aws

Benutzer-Leitfaden

Amazon Elastic Compute Cloud

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Elastic Compute Cloud: Benutzer-Leitfaden

Copyright © 2025 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 ist Amazon EC2? ... 1
Features ... 1
Zugehörige Services ... 2
Zugriff auf EC2 ... 4
Preisgestaltung ... 5
Kostenvoranschläge, Abrechnung und Kostenoptimierung ... 6
Ressourcen ... 7
Erste-Schritte-Tutorial ... 8
Schritt 1: Starten einer Instance ... 10
Schritt 2: Verbindung mit der Instance herstellen ... 12
Schritt 3: Bereinigen Ihrer Instance ... 16
Nächste Schritte ... 17
Bewährte Methoden ... 18
Amazon Machine Images ... 21
AMI-Eigenschaften ... 23
Startberechtigungen ... 23
Root-Volume-Typ ... 24
Den Root-Standardtyp bestimmen ... 25
Virtualisierungstypen ... 27
Suchen eines AMI ... 29
Systems-Manager-Parameter ... 32
Öffentliche Systems-Manager-Parameter ... 37
Gebührenpflichtige AMIs im AWS Marketplace ... 39
Verkaufen Ihres AMI im AWS Marketplace ... 40
Suchen eines gebührenpflichtigen AMI ... 40
Kaufen eines gebührenpflichtigen AMI ... 42
Den Produktcode abrufen ... 43
Verwenden von gebührenpflichtigem Support ... 44
Rechnungen für gebührenpflichtige und unterstützte AMIs ... 45
Verwalten Ihrer -Abonnements ... 45
AMI-Lebenszyklus ... 47
Erstellen eines AMI ... 49
Ein Amazon-S3-gestütztes AMI erstellen ... 58
Ein AMI mit Windows Sysprep erstellen ... 100

Kopieren eines AMI ... 118
Speichern und Wiederherstellen eines AMI ... 137
AMI-Abstammung ... 148
AMI-Nutzung ... 154
AMI als veraltet kennzeichnen ... 179
Deaktivieren eines AMIs ... 185
Aufheben der Registrierung eines AMI ... 192
Startmodi ... 198
Anforderungen für den UEFI-Bootmodus ... 200
AMI-Startmodus-Parameter ... 202
Instance-Typ Startmodus ... 204
Instance Startmodus ... 207
Startmodus des Betriebssystems ... 209
AMI-Startmodus einstellen ... 211
UEFI-Variablen ... 217
UEFI Secure Boot ... 218
AMI-Verschlüsselung ... 236
Instance-startende Szenarien ... 236
Image-kopierende Szenarien ... 240
Geteilt AMIs ... 243
Verifizierter Anbieter ... 243
Suchen Sie nach geteilten AMIs ... 244
Bereiten Sie sich auf die Verwendung von Shared für Linux AMIs vor ... 247
Erlaubt AMIs ... 249
Veröffentlichen Ihres AMI ... 270
Öffentlichen Zugang sperren für AMIs ... 274
Ein AMI für bestimmte Organisationen oder Organisationseinheiten freigeben ... 284
Freigeben eines AMI für bestimmte AWS -Konten ... 297
Aufheben der Freigabe eines AMI für Ihr Konto ... 301
Empfehlungen für die Erstellung von gemeinsam genutztem Linux AMIs ... 303
Überwachen Sie AMI-Ereignisse ... 309
Ereignisdetails ... 310
available-Ereignisse ... 311
failed-Ereignisse ... 311
deregistered-Ereignisse ... 312
disabled-Ereignisse ... 313

Verstehen der AMI-Fakturierung ... 313
Felder für AMI-Fakturierung ... 314
AMI-Fakturierungsdaten finden ... 316
Überprüfen Sie die AMI-Gebühren auf Ihrer Rechnung ... 319
AMI-Kontingente ... 319
Beantragung einer Kontingenterhöhung für AMIs ... 320
Instances ... 322
Instance-Typen ... 323
Verfügbare Instance-Typen ... 324
Hardwarespezifikationen ... 325
Hypervisor-typ ... 325
AMI-Virtualisierungstypen ... 326
Prozessoren ... 326
Suchen eines -Instance-Typs ... 329
EC2-Instance-Typ-Finder ... 337
Empfehlungen zu Compute Optimizer ... 339
Änderungen des Instance-Typs ... 342
Burstable Performance Instances ... 352
GPU-Instances ... 409
Mac-Instances ... 423
EBS-Optimierung ... 474
CPU-Optionen ... 575
AMD SEV-SNP ... 801
Steuerung des Prozessorzustands ... 810
Verwaltete Instances ... 813
Abrechnung für verwaltete Instances ... 813
Ermitteln verwalteter Instances ... 814
Erste Schritte mit verwalteten Instances ... 816
Abrechnungs- und Kaufoptionen ... 816
On-Demand Instances ... 817
Reserved Instances ... 820
Spot Instances ... 893
Dedicated Hosts ... 1003
Dedicated Instances ... 1070
Kapazitätsreservierungen ... 1078
Startvorlagen ... 1229

Einschränkungen ... 1230
Berechtigungen ... 1231
Steuern des Starts von Instances ... 1239
Create ... 1241
Ändern (Versionen verwalten) ... 1258
Delete ... 1262
Starten einer -Instance ... 1265
Tutorials ... 1268
Referenz der Instance-Parameter ... 1295
Starten mit dem Launch Instance Wizard ... 1311
Starten mit einer Startvorlage ... 1315
Von einer vorhandenen Instance starten ... 1322
Von einem AWS Marketplace AMI aus starten ... 1324
Herstellen einer Verbindung zu Ihrer Instance ... 1327
Allgemeine Voraussetzungen für eine Verbindung ... 1328
Herstellen einer Verbindung zu Ihrer Linux-Instance mit SSH ... 1334
Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von RDP ... 1352
Herstellen einer Verbindung über Session Manager ... 1363
Stellen Sie eine Verbindung über eine öffentliche IP und EC2 Instance Connect her ... 1364
Stellen Sie eine Connect über eine private IP und einen EC2 Instance Connect-Endpunkt her ... 1402
Instance-Statusänderungen ... 1437
Abrechnung nach Instance-Status ... 1438
Ausstehende Instances ... 1440
Angehaltene Instances ... 1440
Instances im Ruhezustand ... 1441
Neustarten von Instances ... 1442
Beendete Instances ... 1442
Unterschiede zwischen Instance-Status ... 1443
Anhalten und Starten ... 1446
Hibernate ... 1467
Neustart ... 1499
Beenden ... 1501
Ausmustern ... 1520
Automatische Instance-Wiederherstellung ... 1525
Schlüsselkonzepte der automatischen Instance-Wiederherstellung ... 1527

Unterschiede zwischen vereinfachter automatischer Wiederherstellung und CloudWatch aktionsbasierter Wiederherstellung ... 1529
Ein ausfallsicheres System entwickeln ... 1530
Überprüfen, ob eine automatische Wiederherstellung stattgefunden hat ... 1531
Vereinfachte automatische Wiederherstellung ... 1533
CloudWatch aktionsbasierte Wiederherstellung ... 1538
Instance-Metadaten ... 1543
Instance-Metadatenkategorien ... 1544
Kategorien von dynamischen Daten ... 1562
Auf Instance-Metadaten zugreifen ... 1563
Konfigurieren von IMDS-Optionen ... 1604
Ausführen von Befehlen beim Start ... 1633
Beispiel: AMI-Startindexwert ... 1661
Ermitteln, ob es sich bei einem Host um eine EC2-Instance handelt ... 1666
Untersuchen von Instance-Identitätsdokument ... 1666
Überprüfen des System-UUID ... 1666
Überprüfen der System-ID zur Generierung der virtuellen Maschine ... 1668
Instance-Identitätsdokumente ... 1674
Abrufen des Instance-Identitätsdokuments ... 1675
Verifizieren des Instance-Identitätsdokuments ... 1677
Öffentliche Zertifikate ... 1688
STIG-Compliance ... 1748
STIG-Einstellungen ... 1749
STIG-Skripte herunterladen ... 1769
STIG-Einstellungen mit Systems Manager anwenden ... 1791
Synchronisierung von Uhren ... 1794
Hardware-Paket-Zeitstempel ... 1795
Schaltsekunden ... 1796
Verwenden des lokalen Amazon Time Sync Service ... 1797
Verwenden des öffentlichen Amazon Time Sync Service ... 1810
Vergleichen von Zeitstempeln für Ihre Linux-Instances ... 1812
Ändern der Zeitzone für Ihre Instance ... 1814
EC2 Capacity Manager ... 1816
Wichtigste Funktionen ... 1817
Capacity Manager aktivieren ... 1818
Ihre Daten organisieren ... 1829

Capacity Manager mit der Konsole navigieren ... 1838
Exportieren von Daten ... 1841
Gerätetreiber verwalten ... 1844
Netzwerktreiber ... 1844
Grafiktreiber ... 1845
Speichergerätetreiber ... 1845
AMD-Treiber ... 1846
NVIDIA-Treiber ... 1852
Installieren des NVIDIA-Treibers unter Windows ... 1900
Windows-PV-Treiber ... 1923
AWS NVMe-Treiber ... 1961
Konfigurieren Ihrer Windows-Instance ... 1972
Windows-spezifische Systemeinstellungen ... 1973
AWS-Gerätetreiber für Windows-Instances ... 1974
Windows-Start-Agenten ... 1975
EC2-Schnellstart für Windows ... 2149
Das Windows-Administratorpasswort ändern ... 2175
Windows-Komponenten hinzufügen ... 2176
WSL in Windows installieren ... 2182
Windows-Hilfsprogramme ... 2183
Aktualisieren von Windows-Instances ... 2185
Durchführen eines direkten Upgrades ... 2187
Durchführen eines automatisierten Upgrades ... 2191
Zu einem Nitro-basierten Instance-Typ migrieren ... 2203
Fehlerbehebung bei einem Upgrade ... 2213
Tutorial: Verbinden einer EC2-Instance mit einer RDS-Datenbank ... 2214
Tutorial-Ziel ... 2214
Kontext ... 2214
Architektur ... 2215
Überlegungen ... 2216
Zeit zur Absolvierung des Tutorials ... 2217
Kosten ... 2218
Option 1: Automatisches Verbinden unter Verwendung der EC2-Konsole ... 2218
Option 2: Automatisches Verbinden unter Verwendung der RDS-Konsole ... 2232
Option 3: Manuelles Verbinden ... 2243
Flotten ... 2255

Features und Vorteile ... 2255
Welche Flottenmethode sollte verwendet werden? ... 2256
Konfigurationsoptionen ... 2258
Anforderungstypen ... 2260
Ausgabenlimits ... 2289
Attributbasierte Auswahl des Instance-Typs ... 2292
Instance-Gewichtung ... 2329
Zuweisungsstrategien ... 2332
Kapazitätsausgleich ... 2340
Capacity Reservations ... 2346
Arbeiten Sie mit EC2 Fleet ... 2347
EC2 Status der Flottenanfrage ... 2348
EC2 Voraussetzungen für die Flotte ... 2349
Erstellen Sie eine EC2 Flotte ... 2354
Taggen Sie eine EC2 Flotte ... 2364
Beschreiben Sie eine EC2 Flotte ... 2366
Modifizieren Sie eine EC2 Flotte ... 2370
Löschen Sie eine EC2 Flotte ... 2373
Mit Spot-Flotten arbeiten ... 2378
Status von Spot-Flotten-Anforderungen ... 2379
Spot-Flotten-Berechtigungen ... 2380
Erstellen einer Spot-Flotte ... 2391
Markieren einer Spot-Flotte ... 2401
Spot-Flotte beschreiben ... 2411
Ändern einer Spot-Flotten-Anforderung ... 2412
Spot-Flotten-Anforderung abbrechen (löschen) ... 2414
Automatische Skalierung für Spot-Flotten ... 2417
Überwachen Ihrer Flotte ... 2429
Überwachen Sie Ihre Flotte mit CloudWatch ... 2429
Überwachen Sie Ihre Flotte mit EventBridge ... 2433
Tutorials ... 2452
Tutorial: EC2-Flotte konfigurieren um Instance-Gewichtung zu verwenden ... 2454
Tutorial: EC2-Flotte für die Verwendung von On-Demand Instances als primäre Kapazität konfigurieren ... 2458
Tutorial: EC2 Fleet so konfigurieren, dass On-Demand Instances mit gezielten Kapazitätsreservierungen gestartet werden ... 2460

Tutorial: Ihre EC2-Flotte konfigurieren, um Instances in Kapazitätsblöcken zu starten 2467
CLI-Beispielkonfigurationen für EC2 Fleet 2470
Beispiel 1: Starten von Spot-Instances als Standard-Kaufoption 2471
Beispiel 2: Starten von On-Demand-Instances als Standard-Kaufoption 2471
Beispiel 3: Starten von On-Demand-Instances als primäre Kapazität 2472
Beispiel 4: Starten von On-Demand-Instances unter Verwendung von mehreren Kapazitätsreservierungen 2472
Beispiel 5: Starten von On-Demand-Instances mit Kapazitätsreservierungen, wenn die Gesamtzielkapazität die Anzahl der nicht verwendeten Kapazitätsreservierungen übersteigt 2476
Beispiel 6: Starten von On-Demand-Instances mithilfe von Ziel-Kapazitätsreservierungen . 2480
Beispiel 7: Konfigurieren des Kapazitätsneuausgleichs, um Ersatz-Spot-Instances zu starten 2484
Beispiel 8: Starten von Spot Instances in einer kapazitätsoptimierten Flotte 2485
Beispiel 9: Starten von Spot Instances in einer kapazitätsoptimierten Flotte mit Prioritäten 2487
Beispiel 10: Starten Sie Spot-Instances in einer Flotte price-capacity-optimized 2488
Beispiel 11: Konfigurieren von attributbasierter Auswahl von Instance-Typen 2490
Beispiel für CLI-Konfigurationen der Spot-Flotte 2491
Beispiel 1: Availability Zone mit dem niedrigsten Preis 2492
Beispiel 2: Availability Zone mit dem niedrigsten Preis aus einer Liste 2492
Beispiel 3: Instance-Typ mit dem niedrigsten Preis aus einer Liste 2495
Beispiel 4. Außerkraftsetzen des Preises für die Anforderung 2496
Beispiel 5: Die diversifizierte Zuweisungsstrategie verwenden 2498
Beispiel 6: Instance-Gewichtung verwenden 2501
Beispiel 7: On-Demand-Kapazität verwenden 2503
Beispiel 8: Kapazitätsneuausgleich konfigurieren 2504
Beispiel 9: Eine kapazitätsoptimierte Flotte verwenden 2505
Beispiel 10: Eine kapazitätsoptimierte Flotte mit Prioritäten verwenden 2506
Beispiel 11: Eine priceCapacityOptimized-Flotte verwenden 2508
Beispiel 12: Konfigurieren von attributbasierter Auswahl von Instance-Typen 2509
Flottenkontingente 2510
Anfordern einer Quota-Erhöhung für die Zielkapazität 2512
Netzwerk 2513
Regionen und Zonen 2514
Regionen 2515
Availability Zones 2515

Local Zones ... 2517
Wavelength-Zones ... 2518
AWS Outposts ... 2519
IP-Adressierung von Instances ... 2522
Private IPv4-Adressen ... 2522
Öffentliche IPv4-Adressen ... 2523
Optimierung von öffentlichen IPv4-Adressen ... 2525
IPv6-Adressen ... 2527
Mehrere IP-Adressen ... 2529
Hostnamen der EC2-Instance ... 2530
Link-lokale Adressen ... 2530
IPv4-Adressen ... 2531
IPv6-Adressen ... 2537
Sekundäre IP-Adressen ... 2543
IPv4-Adressen in Windows ... 2547
Hostnamen und Domains der EC2-Instance ... 2554
Hostnamen und Domains der EC2-Instance verstehen ... 2555
Hostnamentypen ... 2555
Bring Your Own IP Addresses ... 2571
BYOIP-Definitionen ... 2573
Voraussetzungen und Kontingente ... 2573
Regionale Verfügbarkeit ... 2575
Verfügbarkeit der Local Zone ... 2575
Voraussetzungen ... 2577
Integrieren Ihres Adressbereichs ... 2585
Ihren Adressbereich verwenden ... 2595
Elastic-IP-Adressen ... 2596
Grundlagen zu Elastic IP-Preisen ... 2597
Grundlagen zu Elastic IP-Adressen ... 2597
Kontingent für Elastic-IP-Adressen ... 2599
So ordnen Sie eine Elastic-IP-Adresse zu ... 2599
Übertragen einer Elastic-IP-Adresse ... 2604
Freigeben einer Elastic-IP-Adresse ... 2611
Verwenden von Reverse DNS für E-Mail-Anwendungen ... 2612
Netzwerkschnittstellen ... 2617
Netzwerkschnittstellen-Konzepte ... 2618

Netzwerkkarten ... 2620
IP-Adressen pro Netzwerkschnittstelle ... 2623
Erstellen einer Netzwerkschnittstelle ... 2625
Netzwerkschnittstellen-Anhänge ... 2631
Verwalten von IP-Adressen ... 2636
Ändern der Netzwerkschnittstellen-Attribute ... 2640
Mehrere Netzwerkschnittstellen ... 2644
Vom Anforderer verwaltete Netzwerkschnittstellen ... 2648
Präfixdelegierung ... 2650
Löschen einer Netzwerkschnittstelle ... 2661
Netzwerkbandbreite ... 2662
Verfügbare Instance-Bandbreite ... 2663
Bandbreitengewichtung ... 2665
Überwachen der Instance-Bandbreite ... 2694
Enhanced Networking ... 2694
Elastic Network Adapter (ENA) ... 2695
ENA Express ... 2762
Intel 82599 VF ... 2792
Überwachen der Netzwerkleistung ... 2806
Verbesserung der Netzwerklatenz in Linux ... 2818
Leistungsaspekte von Nitro ... 2822
Die Netzwerkleistung in Windows optimieren ... 2832
Elastic Fabric Adapter ... 2834
EFA-Grundlagen ... 2835
Unterstützte Schnittstellen und Bibliotheken ... 2838
Unterstützte Instance-Typen ... 2838
Unterstützte Betriebssysteme ... 2857
EFA-Einschränkungen ... 2858
EFA-Preisgestaltung ... 2858
Erste Schritte mit EFA und MPI ... 2859
Erste Schritte mit EFA und NCCL ... 2878
Maximierung der Netzwerkbandbreite ... 2902
Erstellen Sie einen EFA und hängen Sie ihn an ... 2916
Trennen und Löschen eines EFA ... 2922
Überwachen von EFA ... 2922
Prüfen des EFA-Installationsprogramms ... 2930

Versionshinweise ... 2944
EC2 Topologie ... 2965
Funktionsweise ... 2966
Voraussetzungen ... 2974
Beispiele ... 2976
Placement-Gruppen ... 2992
Platzierungsstrategien ... 2993
Erstellen einer Placement-Gruppe ... 2999
Instance-Platzierung ändern ... 3001
Erstellen einer Platzierungsgruppe ... 3003
Freigegebene Platzierungsgruppen ... 3004
Platzierungsgruppen auf AWS Outposts ... 3007
Netzwerk-MTU ... 3008
Jumbo-Frames (9001 MTU) ... 3009
Path MTU Discovery ... 3010
Stellen Sie die MTU für Ihre Instances ein ... 3011
Fehlerbehebung ... 3018
Virtual Private Clouds ... 3018
Ihre Standard-VPCs ... 3018
Nicht standardmäßige VPCs ... 3019
Internetzugang ... 3020
Gemeinsame Subnetze ... 3020
Nur IPv6-Subnetze ... 3021
Sicherheit ... 3022
Datenschutz ... 3023
Datensicherheit bei Amazon EBS ... 3024
Verschlüsselung im Ruhezustand ... 3025
Verschlüsselung während der Übertragung ... 3026
Sicherheit der Infrastruktur ... 3028
Netzwerkisolierung ... 3029
Isolierung auf physischen Hosts ... 3029
Steuern des Netzwerkverkehrs ... 3030
Ausfallsicherheit ... 3032
Compliance-Validierung ... 3033
Identity and Access Management ... 3034
Identitätsbasierte Richtlinien ... 3035

Beispielrichtlinien für die API ... 3047
Beispielrichtlinien für die Konsole ... 3093
AWS verwaltete Richtlinien ... 3107
IAM-Rollen ... 3116
Update-Management ... 3128
Bewährte Methoden für Windows-Instances ... 3129
Bewährte Methoden für die Sicherheit auf hohem Niveau ... 3129
Update-Management ... 3130
Konfigurationsmanagement ... 3132
Änderungsmanagement ... 3134
Prüfung und Rechenschaftspflicht für Amazon EC2 Windows-Instances ... 3134
Schlüsselpaare ... 3135
Erstellen eines Schlüsselpaares ... 3137
Ihre Schlüsselpaare beschreiben ... 3145
Löschen Ihres Schlüsselpaars ... 3150
Einen öffentlichen Schlüssels für Ihre Linux-Instance hinzufügen oder entfernen ... 3151
Fingerabdruck überprüfen ... 3153
Sicherheitsgruppen ... 3156
Übersicht ... 3157
Eine Sicherheitsgruppe erstellen ... 3158
Ändern der Sicherheitsgruppen Ihrer Instance ... 3161
Löschen einer Sicherheitsgruppe ... 3168
Verfolgung von Verbindungen ... 3169
Sicherheitsgruppenregeln für verschiedene Anwendungsfälle ... 3175
NitroTPM ... 3183
Voraussetzungen ... 3184
Linux-AMIs für NitroTPM aktivieren ... 3186
Überprüfen, ob ein AMI für NitroTPM aktiviert ist ... 3187
Aktivieren oder Beenden der Verwendung von NitroTPM ... 3189
Überprüfen, dass eine Instance für NitroTPM aktiviert ist ... 3190
Abrufen des Bestätigungsschlüssels ... 3191
EC2 Bescheinigung der Instanz ... 3193
Integration mit AWS KMS ... 3195
Attestierung isolierter Rechenumgebungen ... 3195
AWS Modell mit geteilter Verantwortung ... 3196
Bescheinigbar AMIs ... 3196

Bereiten Sie sich auf AWS KMS die Bescheinigung vor ... 3206
Das NitroTPM-Attestierungsdokument abrufen ... 3208
Integration mit AWS KMS ... 3216
Isolieren Sie Daten von Ihren eigenen Bedienern ... 3217
Credential Guard für Windows-Instances ... 3218
Voraussetzungen ... 3218
Unterstützte Instance starten ... 3219
Speicherintegrität deaktivieren ... 3221
Credential Guard anschalten ... 3222
Überprüfen, ob Credential Guard ausgeführt wird ... 3223
AWS PrivateLink ... 3224
Erstellen eines Schnittstellen-VPC-Endpunkts ... 3225
Erstellen einer Endpunktrichtlinie ... 3225
Speicher ... 3227
AWS-Speicherpreise ... 3228
Amazon EBS ... 3229
EBS-Volumes-Limits ... 3230
Amazon EC2-Instance-Speicher ... 3233
Datenpersistenz ... 3235
Limits für Instance-Speicher-Volumes ... 3237
Instance-Speicher-Volumes auf SSD ... 3242
Hinzufügen von Instance-Speicher-Volumes ... 3246
Das Swap-Volume für M1- und C1-Instances aktivieren ... 3254
Instance-Speicher-Volumes initialisieren ... 3258
Detaillierte Leistungsstatistiken für Instance-Speicher-Volumes ... 3260
Root-Volume ... 3264
Instances mit einem Amazon-EBS-Root-Volume ... 3265
Instances mit einem Instance-Speicher-Root-Volume (nur Linux-Instances) ... 3266
Behalten Sie das Root-Volume nach Beendigung der Instance ... 3267
Ersetzen eines Stammvolumen ... 3272
Gerätenamen für Volumes ... 3284
Verfügbare Gerätenamen ... 3285
Überlegungen zu Gerätenamen ... 3288
Blockgerät-Zuweisungen ... 3290
Konzepte der Blockgerät-Zuweisung ... 3290
Blockgerät-Zuweisung zu AMI hinzufügen ... 3294

Blockgerät-Zuweisung zu Instance hinzufügen ... 3299
Wie Volumes für Windows-Instances angehängt und zugeordnet werden ... 3308
Zuweisen von NVMe-Festplatten zu Volumes ... 3309
Nicht-NVME-Festplatten zu Volumes zuordnen ... 3314
Torn-Write-Prävention ... 3324
Unterstützte Blockgrößen ... 3325
Voraussetzungen ... 3326
Instance-Unterstützung prüfen ... 3327
Workload konfigurieren ... 3329
Windows-VSS-EBS-Schnappschüsse ... 3330
Was ist -VSS? ... 3331
So funktioniert die VSS-basierte Amazon-EBS-Snapshot-Lösung ... 3332
Voraussetzungen für VSS ... 3333
Erstellen von VSS-Snapshots ... 3347
Problembehandlung von VSS-Snapshots ... 3358
Wiederherstellungsoptionen für die AWS-VSS-Lösung ... 3364
Versionshistorie ... 3365
Objektspeicher, Dateispeicher und Datei-Caching ... 3370
Amazon S3 ... 3371
Amazon EFS ... 3373
Amazon FSx ... 3378
Amazon-Datei-Cache ... 3383
Ressourcen verwalten ... 3385
Eine Region für Ihre Ressourcen wählen ... 3385
Ihre Ressourcen finden ... 3387
Schritte in der Konsole ... 3387
Befehlszeilenbeispiele ... 3397
Globale Ansicht (regionsübergreifend) ... 3400
AWS Globale Ansicht ... 3401
Markieren Ihrer -Ressourcen mit Tags (Markierungen) ... 3405
Grundlagen zu Tags (Markierungen) ... 3405
Markieren Ihrer -Ressourcen mit Tags (Markierungen) ... 3407
Tag (Markierung)-Einschränkungen ... 3408
Tags (Markierungen) und Access Management ... 3409
Markieren von Ressourcen für die Fakturierung ... 3409
Berechtigungen zur Markierung von Ressourcen ... 3410

Tags hinzufügen und entfernen ... 3414
Filtern von Ressourcen nach Tags ... 3418
Tags mithilfe von Instance-Metadaten anzeigen ... 3420
Servicekontingente ... 3427
Anzeigen Ihrer aktuellen Kontingente ... 3427
Beantragen einer Erhöhung ... 3428
Einschränkung für E-Mails, die über Port 25 gesendet werden ... 3428
Überwachung von -Ressourcen ... 3430
Überwachen des Status Ihrer Instances ... 3431
Statusüberprüfungen ... 3432
Statusänderungsereignisse ... 3442
Geplante Ereignisse ... 3444
Überwachen Sie Ihre Instances mit CloudWatch ... 3485
Instance-Alarme ... 3486
Detaillierte Überwachung verwalten ... 3487
CloudWatch Metriken ... 3490
Installieren und konfigurieren Sie den CloudWatch Agenten ... 3513
Statistiken für -Metriken ... 3518
Anzeigen von Überwachungsdiagrammen ... 3528
Alarm erstellen ... 3529
Erstellen von Alarmen, mit denen eine Instance angehalten, beendet, neu gestartet oder wiederhergestellt wird ... 3530
Automatisieren mithilfe von EventBridge ... 3544
Amazon-EC2-Ereignistypen ... 3544
Protokollieren von API-Aufrufen mit CloudTrail ... 3545
Amazon-EC2-API-Verwaltungsereignisse in CloudTrail ... 3547
Amazon-EC2-API-Ereignisbeispiele ... 3547
Prüfung von Verbindungen, die über EC2-Instance-Connect hergestellt wurden ... 3549
Überwachung Ihrer .NET- und SQL Server-Anwendungen ... 3550
Ihre Nutzung des kostenlosen Kontingents nachverfolgen ... 3551
Vorteile des kostenlosen Kontingents vor und nach dem 15. Juli 2025 ... 3552
Die Nutzung des kostenlosen Kontingents für Konten nachverfolgen, die vor dem 15. Juli 2025 erstellt wurden ... 3553
Fakturierungs- und Nutzungsberichte ... 3556
Instances ... 3557
Bare Metal-Instances ... 3558

Dedicated Hosts ... 3558
Dedicated Instances ... 3558
EBS-Optimierung ... 3559
Capacity Reservations ... 3559
Bestandsaufnahme Ihrer EC2-Instances ... 3559
Geografischer Standort ... 3561
Hardwarespezifikationen ... 3562
Bilder ... 3563
IP-Adressen und DNS-Hostnamen ... 3565
Sicherheitsgruppenregeln ... 3566
Benutzerdaten ... 3568
Zugehörige Ressourcen ... 3569
Fehlerbehebung ... 3570
Probleme beim Starten von Instances ... 3570
Ungültiger Gerätename ... 3571
Instance-Limit überschritten ... 3572
Ungenügend Kapazität der Instance ... 3572
Die angefragte Konfiguration wird derzeit nicht unterstützt. Bitte überprüfen Sie die Dokumentation auf unterstützte Konfigurationen. ... 3573
Die Instance wird sofort beendet ... 3574
Unzureichende Berechtigungen ... 3575
Hohe CPU-Auslastung kurz nach dem Windows-Start (Nur Windows-Instances) ... 3576
Probleme beim Anhalten von Instances ... 3577
Erzwingung des Stopps einer Instance ... 3578
(Optional) Eine Ersatz-Instance erstellen ... 3580
Instance-Beendigungsprobleme ... 3583
Die Instance wird sofort beendet ... 3583
Verzögertes Beenden einer Instance ... 3584
Fortdauernde Anzeige einer beendeten Instance ... 3586
Fehler: Die Instance ist möglicherweise nicht beendet worden. Ändern Sie das Instanzattribut 'disableApiTermination' ... 3586
Instances automatisch gestartet oder beendet ... 3587
Unerreichbare Instances ... 3587
Instance-Neustart ... 3587
Instance-Konsolenausgabe ... 3588
Aufnehmen eines Screenshots einer nicht erreichbaren Instance ... 3589

Allgemeine Screenshots für Windows-Instances 3590
Wiederherstellung einer Instance beim Ausfall eines Host-Computers 3600
Die Instance wurde offline angezeigt und unerwartet neu gestartet 3601
SSH-Probleme mit der Linux-Instance 3601
Häufige Ursachen für Verbindungsprobleme 3602
Fehler beim Herstellen der Verbindung mit Ihrer Instance: „Connection timed out“ 3605
Fehler: Schlüssel kann nicht geladen werden ... Erwartend: JEDER PRIVATE SCHLÜSSEL 3608
Fehler: Benutzerschlüssel wird vom Server nicht erkannt 3609
Fehler: Berechtigung verweigert oder Verbindung durch [instance] Port 22 geschlossen ... 3611
Fehler: Ungeschützte private Schlüsseldatei 3614
Fehler: Der private Schlüssel muss mit „-----BEGIN RSA PRIVATE KEY-----“ und mit „-----END RSA PRIVATE KEY-----“ enden 3616
Fehler: Hostschlüssel-Validierung fehlgeschlagen 3616
Fehler: Der Server lehnte unseren Schlüssel ab oder es sind keine unterstützten Authentifizierungsmethoden verfügbar. 3616
Die Instance ist nicht per Ping erreichbar. 3618
Fehler: Der Server hat die Netzwerkverbindung unerwartet geschlossen 3618
Fehler: Hostschlüssel-Validierung fehlgeschlagen für EC2 Instance Connect 3618
Mit EC2 Instance Connect kann keine Verbindung zur Ubuntu-Instance hergestellt werden 3620
Ich habe meinen privaten Schlüssel verloren. Wie kann ich eine Verbindung zu meiner Instance herstellen? 3621
Nicht bestandene Statusprüfungen einer Linux-Instance 3628
Informationen der Statusprüfung durchgehen 3630
Systemprotokolle abrufen 3631
Fehlerbehebung bei Systemprotokollfehlern für Linux-Instances 3631
Out of memory: kill process 3633
ERROR: mmu_update failed (Fehler beim Aktualisieren der Speicherverwaltung) 3634
I/O-Fehler (Blockgerätfehler) 3635
I/O ERROR: neither local nor remote disk (defektes verteiltes Blockgerät) 3637
request_module: runaway loop modprobe (Endlosschleife des modprobe-Programms auf Legacy-Kerneln älterer Linux-Versionen) 3638
"FATAL: kernel too old" und "fsck: No such file or directory while trying to open /dev" (fehlende Übereinstimmung zwischen Kernel und AMI) 3639
„SCHWERWIEGEND: /lib/modules" oder "BusyBox" (Fehlende Kernelmodule) konnten nicht geladen werden 3640

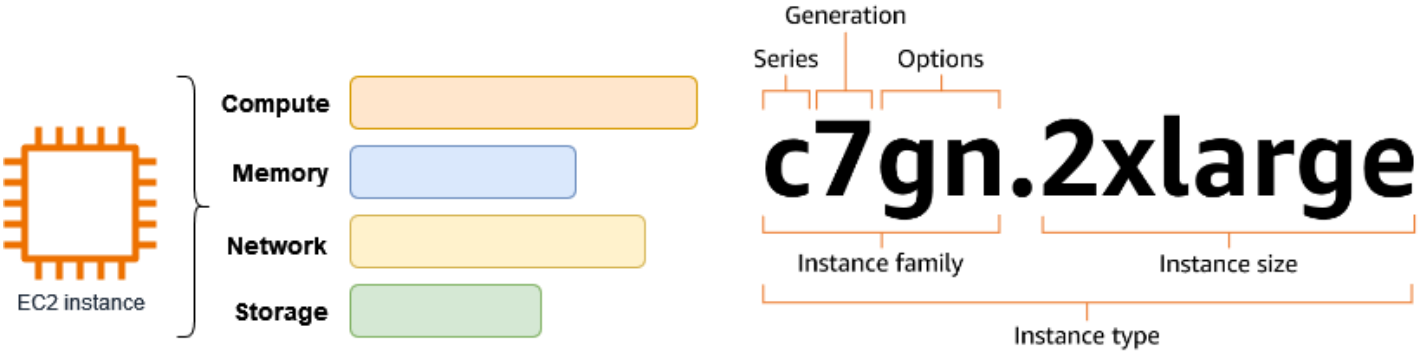
FEHLER Ungültiger Kernel (inkompatibler Kernel) EC2 3642
fsck: No such file or directory while trying to open... (Dateisystem nicht gefunden) 3644
Allgemeiner Fehler beim Mounten von Dateisystemen (Mountfehler) 3646
VFS: Unable to mount root fs on unknown-block (fehlende Übereinstimmung des Stammdateisystems) 3648
Fehler: Die major/minor Anzahl der Root-Geräte konnte nicht ermittelt werden... (Root-Datei system/device stimmt nicht überein) 3650
XENBUS: Device with no driver... 3651
... days without being checked, check forced (Dateisystemprüfung erforderlich) 3653
fsck died with exit status... (fehlendes Gerät) 3653
GRUB prompt (grubdom>) 3655
Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring. (hartcodierte MAC-Adresse) 3658
Die Richtlinie konnte nicht geladen werden SELinux . Machine is in enforcing mode. Wird jetzt angehalten. (SELinux Fehlkonfiguration) 3660
XENBUS: Timeout connecting to devices (Xenbus-Timeout) 3662
Die Linux-Instance wird vom falschen Volume aus gestartet 3663
RDP-Probleme mit der Windows-Instance 3665
Der Remotedesktopdienst kann keine Verbindung zu dem Remotecomputer herstellen 3665
Fehler beim Verwenden des macOS RDP-Clients 3667
RDP zeigt anstelle des Desktops einen schwarzen Bildschirm an 3667
Die Remote-Anmeldung bei einer Instance mit einem Benutzer, der kein Administrator ist, ist nicht möglich 3668
Fehlerbehebung bei Remotedesktop-Problemen mit AWS Systems Manager 3668
Aktivieren von Remotedesktop für eine EC2-Instance mit Remote-Registrierung 3673
Ich habe meinen privaten Schlüssel verloren. Wie kann ich mich mit meiner Windows-Instance verbinden? 3674
Probleme beim Starten der Windows-Instance 3675
Passwort nicht verfügbar 3675
Passwort noch nicht verfügbar 3676
Windows-Passwort kann nicht abgerufen werden 3677
Warten auf Metadaten-Service 3677
Windows kann nicht aktiviert werden 3682
Keine Original-Windows-Version (0x80070005) 3684
Kein Terminal Server License-Server verfügbar, um eine Lizenz bereitzustellen 3685
„Einige Einstellungen werden von Ihrer Organisation verwaltet.“ (Windows 2019) 3685

Probleme bei Windows-Instances 3686
AWS Systems Manager Sessions Manager kann nicht mit einer Windows Server 2025-Instance verbunden werden 3687
EBS-Volumes unter Windows Server 2016 und 2019 werden nicht initialisiert 3687
Starten einer EC2-Windows-Instance in die Verzeichnisdienstwiederherstellung (DSRM) .. 3688
Die Instance verliert die Netzwerkverbindung oder geplante Aufgaben werden nicht zu dem erwarteten Zeitpunkt ausgeführt 3692
Abrufen der Konsoleausgabe nicht möglich 3693
Windows Server 2012 R2 nicht im Netzwerk verfügbar 3693
Kollision der Festplattensignatur 3693
Windows-Administratorpasswort ändern 3695
Passwort mit EC2Launch v2 zurücksetzen 3696
Passwort mit EC2Launch zurücksetzen 3702
Passwort mit EC2Config zurücksetzen 3709
Beheben von Sysprep-Problemen 3715
EC2Rescue für Linux-Instances 3717
EC2Rescue installieren 3718
EC2Rescue-Befehle ausführen 3722
Entwickeln von EC2Rescue-Modulen 3725
EC2Rescue für Windows-Instances 3732
Problembehandlung mithilfe der EC2 Rescue-GUI 3733
Problembehandlung mit EC2 Rescue CLI 3740
Problembehandlung mit EC2 Rescue und Systems Manager 3748
EC2 Serielle Konsole 3752
Voraussetzungen 3753
Konfigurieren Sie den Zugriff auf die EC2 serielle Konsole 3761
Connect zur EC2 seriellen Konsole her 3772
Trennen Sie die Verbindung zur seriellen Konsole EC2 3784
Beheben Sie Probleme mit Ihrer Instance mithilfe der EC2 seriellen Konsole 3785
Senden einer Diagnose-Unterbrechung 3795
Unterstützte Instance-Typen 3796
Voraussetzungen 3796
Senden eines Diagnose-Interrupts 3799
Dokumentverlauf 3800
Verlauf für 2018 und früher 3844
..... mmmdccclxxv

Was ist Amazon EC2?

Amazon Elastic Compute Cloud (Amazon EC2) bietet bedarfsbasiert skalierbare Rechenkapazität in der Amazon Web Services Cloud (AWS Cloud). Mit Amazon EC2 reduzieren Sie die Hardwarekosten, so dass Sie Anwendungen schneller entwickeln und bereitstellen können. Mit Amazon EC2 können Sie so viele oder so wenige virtuelle Server starten, wie Sie benötigen, die Sicherheit und das Netzwerk konfigurieren und den Speicher verwalten. Sie können Kapazität hinzufügen (skalieren), um rechenintensive Aufgaben wie monatliche oder jährliche Prozesse oder Spitzen im Website-Datenverkehr zu bewältigen. Wenn die Nutzung abnimmt, können Sie die Kapazität wieder reduzieren (herunterskalieren).

Eine EC2-Instance ist ein virtueller Server in der AWS-Cloud. Wenn Sie eine EC2-Instance starten, bestimmt der von Ihnen angegebene Instance-Typ die für Ihre Instance verfügbare Hardware. Jeder Instance-Typ bietet eine andere Balancierung in Bezug auf Datenverarbeitung, Arbeitsspeicher, Speicher und Netzwerkfunktionen. Weitere Informationen finden Sie unter Amazon-EC2-Instance-Typen.



Features von Amazon EC2

Amazon EC2 bietet die folgenden allgemeinen Features:

Instances

Virtuelle Server.

Amazon Machine Images (AMIs)

Vorkonfigurierte Vorlagen für Ihre Instances, die die Komponenten enthalten, die Sie für Ihren Server benötigen (einschließlich des Betriebssystems und zusätzlicher Software).

Instance-Typen

Verschiedene Konfigurationen von CPU, Arbeitsspeicher, Speicher, Netzwerkkapazität und Grafikhardware für Ihre Instances.

Amazon EBS-Volumes

Persistente Speicher-Volumes für Ihre Daten mit Amazon Elastic Block Store (Amazon EBS).

Instance-Speicher-Volumes

Speicher-Volumes für temporäre Daten, die gelöscht werden, wenn Sie Ihre Instance anhalten, in den Ruhezustand versetzen oder beenden.

Schlüsselpaare

Sichere Anmeldeinformationen für Ihre Instances. AWS speichert den öffentlichen Schlüssel und Sie speichern den privaten Schlüssel an einem sicheren Ort.

Sicherheitsgruppen

Eine virtuelle Firewall, mit der Sie die Protokolle, Ports und Quell-IP-Bereiche festlegen können, die Ihre Instances erreichen können, sowie die Ziel-IP-Bereiche, mit denen sich Ihre Instances verbinden können.

Amazon EC2 unterstützt die Verarbeitung, Speicherung und Übertragung von Kreditkartendaten durch einen Händler oder Dienstanbieter. Außerdem wurde seine Konformität mit dem Payment Card Industry (PCI) Data Security Standard (DSS) bestätigt. Weitere Informationen über PCI DSS, einschließlich der Anforderung einer Kopie des AWS PCI Compliance Package, finden Sie unter PCI DSS Level 1.

Zugehörige Services

Services zur Verwendung von mit Amazon EC2

Sie können andere AWS-Services mit den Instances verwenden, die Sie mit Amazon EC2 bereitstellen.

Amazon EC2 Auto Scaling

Hilft Ihnen sicherzustellen, dass Sie die richtige Anzahl von Amazon-EC2-Instances zur Verfügung haben, um die Auslastung Ihrer Anwendung zu bewältigen.

AWS Backup

Automatisieren Sie die Sicherung Ihrer Amazon-EC2-Instances und der ihnen angefügten Amazon-EBS-Volumes.

Amazon CloudWatch

Überwachen Sie Ihre Instances und Amazon-EBS-Volumes.

Elastic Load Balancing

Verteilen Sie eingehenden Anwendungsdatenverkehr automatisch auf mehrere Instances.

Amazon GuardDuty

Erkennen Sie die potenziell unbefugte oder schädliche Nutzung Ihrer EC2-Instances.

EC2 Image Builder

Automatisieren Sie die Erstellung, Verwaltung und Bereitstellung von angepassten, sicheren und aktuellen Server-Images.

AWS Launch Wizard

Nehmen Sie die Dimensionierung, Konfiguration und Bereitstellung von AWS-Ressourcen für Anwendungen von Drittanbietern vor, ohne einzelne AWS-Ressourcen manuell zu identifizieren und bereitzustellen.

AWS Systems Manager

Mit dieser sicheren End-to-End-Verwaltungslösung können Sie Operationen auf EC2-Instances in großem Umfang durchführen.

Zusätzliche Datenverarbeitungsservices

Sie können Instances mit einem anderen AWS-Datenverarbeitungsservice starten, anstatt Amazon EC2 zu verwenden.

Amazon Lightsail

Erstellen Sie Websites oder Webanwendungen mit Amazon Lightsail, einer Cloud-Plattform, die Ihnen die Ressourcen zur Verfügung stellt, die Sie benötigen, um Ihr Projekt schnell und zu einem niedrigen, vorhersehbaren monatlichen Preis umzusetzen. Um Amazon EC2 und Lightsail zu vergleichen, siehe Amazon Lightsail oder Amazon EC2.

Amazon Elastic Container Service (Amazon ECS)

Nehmen Sie die Bereitstellung, Verwaltung und Skalierung von containerisierten Anwendungen in einem Cluster von EC2-Instances vor. Weitere Informationen finden Sie unter Einen AWS-Container-Service wählen.

Amazon Elastic Kubernetes Service (Amazon EKS)

Führen Sie Ihre Kubernetes-Anwendungen in AWS aus. Weitere Informationen finden Sie unter Einen AWS-Container-Service wählen.

Zugriff auf Amazon EC2

Sie können Ihre Amazon-EC2-Instances über die folgenden Schnittstellen erstellen und verwalten:

Amazon EC2-Konsole

Eine einfache Weboberfläche zum Erstellen und Verwalten von Amazon-EC2-Instances und -Ressourcen. Nach der Registrierung eines AWS-Kontos können Sie auf die Amazon EC2-Konsole zugreifen, indem Sie sich bei der AWS-Managementkonsole anmelden und auf der Konsolenstartseite EC2 auswählen.

AWS Command Line Interface

Ermöglicht Ihnen die Interaktion mit AWS-Services über Befehle in Ihrer Befehlszeilen-Shell. Es wird auf Windows, Mac und Linux unterstützt. Weitere Informationen zur AWS CLI finden Sie im Benutzerhandbuch zu AWS Command Line Interface. Die Amazon-EC2-Befehle finden Sie in der AWS CLI-Befehlsreferenz.

CloudFormation

Amazon EC2 unterstützt das Erstellen von Ressourcen mit CloudFormation. Sie erstellen eine Vorlage im JSON- oder YAML-Format, die Ihre AWS-Ressourcen beschreibt, und CloudFormation übernimmt die Bereitstellung und Konfiguration dieser Ressourcen für Sie. Sie können Ihre CloudFormation-Vorlagen wiederverwenden, um dieselben Ressourcen mehrmals bereitzustellen, egal ob in derselben Region und in demselben Konto oder in mehreren Regionen und Konten. Weitere Informationen zu unterstützten Ressourcentypen und -eigenschaften für Amazon EC2 finden Sie in der EC2-Ressourcentypreferenz im AWS CloudFormation-Benutzerhandbuch.

AWS SDKs

Wenn Sie es vorziehen, Anwendungen mithilfe sprachspezifischer APIs zu erstellen, anstatt eine Anfrage über HTTP oder HTTPS zu übermitteln, stellt AWS Bibliotheken, Beispiel-Code, Tutorials und andere Ressourcen für Softwareentwickler bereit. Diese Bibliotheken bieten grundlegende Funktionen zur Automatisierung von Aufgaben, z. B. kryptografisches Signieren von Anfragen, Wiederholen von Anfragen und Behandlung von Fehlermeldungen. Dadurch wird Ihnen der Einstieg erleichtert. Weitere Informationen finden Sie unter Tools für AWS.

AWS -Tools für PowerShell

Eine Reihe von PowerShell-Modulen, die auf den vom SDK für .NET bereitgestellten Funktionen aufbauen. Mit den Tools for PowerShell können Sie über die PowerShell-Befehlszeile Skriptvorgänge für Ihre AWS-Ressourcen ausführen. Informationen zu den ersten Schritten finden Sie im AWS -Tools für PowerShell-Benutzerhandbuch. Die Cmdlets für Amazon EC2 finden Sie in der AWS -Tools für PowerShell-Cmdlet-Referenz.

Abfrage-API

Amazon EC2 stellt eine Abfrage-API zur Verfügung. Bei diesen Abfragen handelt es sich um HTTP- oder HTTPS-Abfragen, bei denen das HTTP-Verb GET oder POST sowie der Abfrageparameter verwendet wir `Action`. Weitere Informationen zu den API-Aktionen für Amazon EC2 finden Sie unter Aktionen im Amazon EC2 API Reference.

Preise für Amazon EC2

Amazon EC2 bietet die folgenden Preisoptionen:

Kostenloses Kontingent

Sie können kostenlos mit Amazon EC2 beginnen. Informationen zu den Optionen des kostenlosen Kontingents finden Sie unter Kostenloses AWS-Kontingent.

On-Demand Instances

Bezahlen Sie für die Instances, die Sie nutzen, nach der Sekunde, mit einem Minimum von 60 Sekunden, ohne langfristige Verpflichtungen oder Vorauszahlungen.

Savings Plans

Sie können die Amazon EC2-Kosten reduzieren, indem Sie sich auf eine konsistente Nutzung (in USD/h) für eine Laufzeit von ein oder drei Jahren festlegen.

Reserved Instances

Sie können die Amazon EC2-Kosten reduzieren, indem Sie sich auf eine konsistente Instance-Konfiguration (einschließlich Instance-Typ und Region) für eine Laufzeit von ein oder drei Jahren festlegen.

Spot Instances

Sie können ungenutzte EC2-Instances anfordern, wodurch sich die Amazon EC2-Kosten erheblich verringern lassen.

Dedicated Hosts

Senken Sie die Kosten, indem Sie einen physischen EC2-Server verwenden, der ausschließlich für Sie bestimmt ist, entweder bedarfsbasiert oder im Rahmen eines Savings Plans. Sie können Ihre vorhandenen servergebundenen Softwarelizenzen verwenden und erhalten Unterstützung bei der Erfüllung der Compliance-Anforderungen.

On-Demand Capacity Reservations

Reservieren Sie Rechenkapazität für Ihre EC2-Instances in einer bestimmten Availability Zone für einen beliebigen Zeitraum.

Sekundengenaue Abrechnung

Die Kosten für ungenutzte Minuten und Sekunden werden von Ihrer Rechnung gestrichen.

Eine vollständige Liste der Gebühren und Preise für Amazon EC2 und weitere Informationen zu den Kaufmodellen finden Sie unter Amazon EC2 – Preise.

Kostenvoranschläge, Abrechnung und Kostenoptimierung

Verwenden Sie den AWS -Preisrechner, um Kostenvoranschläge für Ihre AWS-Anwendungsfälle zu erstellen.

Verwenden Sie den AWS Modernization Calculator für Microsoft-Workloads, um die Kosten für die Umstellung von Microsoft-Workloads auf eine moderne Architektur abzuschätzen, die Open-Source und cloudnative Services verwendet, die in AWS bereitgestellt werden.

Um Ihre Rechnung anzuzeigen, navigieren Sie zu Fakturierungs- und Kostenverwaltungs-Dashboard in der AWS Fakturierung und Kostenmanagement-Konsole. Ihre Abrechnung enthält Links zu Nutzungsberichten mit Details zu Ihrer Abrechnung. Weitere Informationen zur Kontoabrechnung AWS finden Sie unter AWS Billing and Cost Management User Guide.

Wenden Sie sich bei Fragen zu AWS-Abrechnungen, -Konten und -Vorfällen an AWS Support.

Informationen zur Berechnung der Kosten einer bereitgestellten Beispielumgebung finden Sie im Cloud Economics Center. Denken Sie bei der Berechnung der Kosten einer bereitgestellten Umgebung daran, Nebenkosten wie Snapshot-Speicher für EBS-Volumes einzubeziehen.

Sie können die Kosten, Sicherheit und Leistung Ihrer AWS-Umgebung mit AWS Trusted Advisor optimieren.

Sie können AWS Cost Explorer verwenden, um die Kosten und Nutzung Ihrer EC2-Instances analysieren. Sie können Daten für die letzten 13 Monate anzeigen und prognostizieren, wie viel Sie wahrscheinlich für die nächsten 12 Monate ausgeben. Weitere Informationen finden Sie unter Analysieren Ihrer Kosten und Nutzung mit AWS Cost Explorer im AWS Cost Management-Benutzerhandbuch.

Ressourcen

- Features von Amazon EC
- AWS re:Post
- AWS Skill Builder
- AWS Unterstützung
- Praktische Tutorials
- Webhosting
- Windows auf AWS

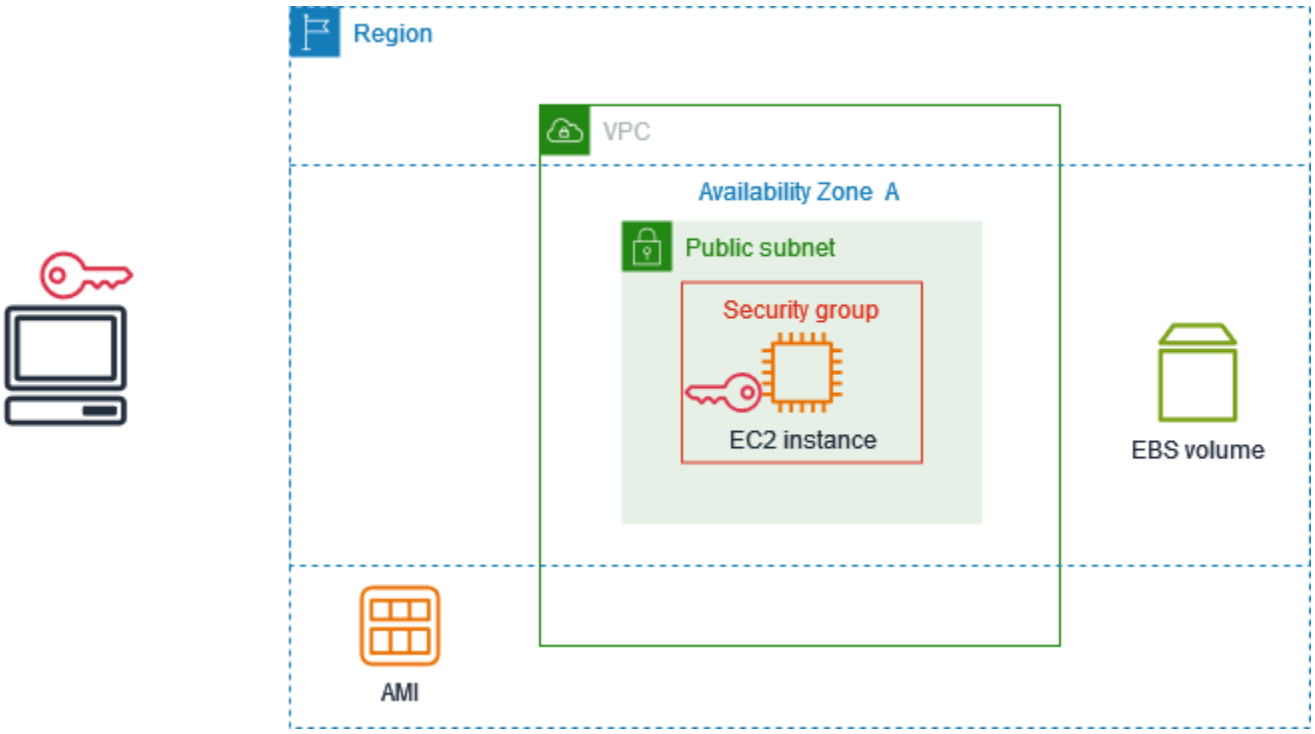
Erste Schritte mit Amazon EC2

Verwenden Sie dieses Tutorial, um mit Amazon Elastic Compute Cloud (Amazon EC2) zu beginnen. Sie erfahren, wie Sie eine EC2-Instance starten und eine Verbindung zu ihr herstellen. Eine Instance ist ein virtueller Server in der AWS-Cloud. Mit Amazon EC2 können Sie das Betriebssystem und die Anwendungen Ihrer Instance einrichten und konfigurieren.

Übersicht

Das folgende Diagramm zeigt die Hauptkomponenten, die Sie in diesem Tutorial verwenden werden:

- Ein Image – Eine Vorlage, die die Software enthält, die auf Ihrer Instance ausgeführt werden soll, z. B. das Betriebssystem.
- Ein Schlüsselpaar – Eine Reihe von Sicherheitsanmeldeinformationen, mit denen Sie Ihre Identität nachweisen, wenn Sie sich mit Ihrer Instance verbinden. Der private Schlüssel ist auf dem lokalen Computer gespeichert und der öffentliche Schlüssel ist in der Instance gespeichert.
- Ein Netzwerk – Eine Virtual Private Cloud (VPC) ist ein virtuelles Netzwerk dediziert für Ihren AWS-Konto. Um Ihnen den schnellen Einstieg zu erleichtern, enthält Ihr Konto eine Standard-VPC in jeder AWS-Region. Jede Standard-VPC hat ein Standardsubnetz in jeder Availability Zone.
- Eine Sicherheitsgruppe – Dient als virtuelle Firewall zur Steuerung von ein- und ausgehendem Datenverkehr.
- Ein EBS-Volume – Wir benötigen ein Root-Volume für das Image. Sie können optional Datenvolumen hinzufügen.



Kosten für dieses Tutorial

Wenn Sie Ihr AWS-Konto erstellen, können Sie kostenlos mit der Verwendung von Amazon EC2 beginnen, indem Sie das Kostenloses AWS-Kontingent nutzen.

Wenn Sie Ihr AWS-Konto vor dem 15. Juli 2025 erstellt haben und das Konto weniger als 12 Monate alt ist, und Sie das kostenlose Kontingent für Amazon EC2 noch nicht ausgeschöpft haben, ist das Absolvieren dieses Tutorials für Sie kostenlos, da wir Ihnen helfen, Optionen auszuwählen, die in das kostenlose Kontingent fallen. Andernfalls fallen die üblichen Amazon-EC2-Nutzungsgebühren an, und zwar ab dem Zeitpunkt, an dem Sie die Instance starten (auch wenn sie im Leerlauf bleibt), bis Sie sie beenden.

Wenn Sie Ihr AWS-Konto vor dem 15. Juli 2025 erstellt haben und das Konto weniger als 6 Monate alt ist, und Sie Ihr Guthaben noch nicht ausgeschöpft haben, ist das Absolvieren dieses Tutorials für Sie kostenlos, da wir Ihnen helfen, Optionen auszuwählen, die in das kostenlose Kontingent fallen.

Informationen darüber, wie Sie feststellen können, ob Sie für das kostenlose Kontingent in Frage kommen, finden Sie unter the section called “Ihre Nutzung des kostenlosen Kontingents nachverfolgen”.

Aufgaben

- Schritt 1: Starten einer Instance

- Schritt 2: Verbindung mit der Instance herstellen
- Schritt 3: Bereinigen Ihrer Instance
- Nächste Schritte

Schritt 1: Starten einer Instance

Sie können eine Amazon-EC2-Instance mit der AWS-Managementkonsole starten, wie in der folgenden Vorgehensweise beschrieben. Da dieses Tutorial für das schnelle Starten Ihrer ersten Instance konzipiert ist, sind nicht alle möglichen Optionen aufgeführt.

So starten Sie eine Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Auf der Navigationsleiste oben im Bildschirm wird die aktuelle AWS-Region angezeigt – beispielsweise Ohio. Sie können die ausgewählte Region verwenden oder optional eine Region auswählen, die Ihnen näher liegt.
3. Wählen Sie auf dem Dashboard der EC2-Konsole im Feld Instance starten die Option Instance starten.
4. Geben Sie unter Name and tags (Name und Tags) bei Name einen beschreibenden Namen für Ihre Instance ein.
5. Führen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) die folgenden Schritte aus:
   a. Wählen Sie Schnellstart und dann das Betriebssystem (OS) für Ihre Instance aus. Für Ihre erste Linux-Instance empfehlen wir Ihnen, Amazon Linux zu verwenden.
   b. Wählen Sie unter Amazon Machine Image (AMI) ein AMI aus, für das das kostenlose Kontingent gilt.
6. Wählen Sie unter Instance-Typ für Instance-Typ einen Instance-Typ aus, der als Für das kostenlose Kontingent berechtigt markiert ist.
7. Unter Schlüsselpaar (Anmelden) wählen Sie für Schlüsselpaarname ein vorhandenes Schlüsselpaar aus oder wählen Sie Neues Schlüsselpaar erstellen, um ein neues zu erstellen.

> **Warning**
>
> Wenn Sie Ohne Schlüsselpaar fortfahren (Nicht empfohlen) auswählen, können Sie mit den in diesem Tutorial beschriebenen Methoden keine Verbindung zu Ihrer Instance herstellen.

8. Beachten Sie, dass wir unter Netzwerkeinstellungen Ihre Standard-VPC ausgewählt haben sowie die Option zur Verwendung des Standardsubnetzes in einer Availability Zone, die wir für Sie ausgewählt haben. Weiters haben wir eine Sicherheitsgruppe mit einer Regel konfiguriert, die Verbindungen zu Ihrer Instance von überall aus ermöglicht (`0.0.0.0/0`).

   > **Warning**
   >
   > Wenn Sie `0.0.0.0/0` angeben, aktivieren Sie den Datenverkehr von allen IP-Adressen auf der ganzen Welt. Dieser Ansatz ist möglicherweise für SSH- und RDP-Protokolle in einer Testumgebung für kurze Zeit zulässig, aber für Produktionsumgebungen sehr unsicher. Achten Sie in Produktionsumgebungen darauf, nur Zugriff von der entsprechenden individuellen IP-Adresse oder vom entsprechenden Adressbereich zu autorisieren.

   Für Ihre erste Instance empfehlen wir Ihnen, die Standardeinstellungen zu verwenden. Andernfalls können Sie Ihre Netzwerkeinstellungen wie folgt aktualisieren:

   - (Optional) Um ein bestimmtes Standardsubnetz zu verwenden, wählen Sie Bearbeiten und dann ein Subnetz aus.
   - (Optional) Um eine andere VPC zu verwenden, wählen Sie Bearbeiten und dann eine vorhandene VPC aus. Wenn die VPC nicht für den öffentlichen Internetzugang konfiguriert ist, können Sie keine Verbindung zu Ihrer Instance herstellen.
   - (Optional) Um den eingehenden Verbindungsverkehr auf ein bestimmtes Netzwerk zu beschränken, wählen Sie Benutzerdefiniert statt Überall und geben Sie den CIDR-Block für Ihr Netzwerk ein.
   - (Optional) Um eine vorhandene Sicherheitsgruppe zu verwenden, wählen Sie Vorhandene Sicherheitsgruppe verwenden und dann die Sicherheitsgruppe. Verfügt die Sicherheitsgruppe nicht über eine Regel zum Zulassen von Verbindungsverkehr aus Ihrem Netzwerk, können Sie keine Verbindung zu Ihrer Instance herstellen. Für eine Linux-

Instance müssen Sie SSH-Verkehr zulassen. Für eine Windows-Instance müssen Sie RDP-Verkehr zulassen.

9. Beachten Sie unter Speicher konfigurieren, dass wir ein Root-Volume, aber keine Datenvolumes konfiguriert haben. Dies ist für Testzwecke ausreichend.
10. Überprüfen Sie Ihre Instance-Konfiguration im Bereich Summary (Übersicht). Wenn alles in Ordnung ist, klicken Sie auf Launch instance (Instance starten).
11. Wenn der Start erfolgreich war, wählen Sie die ID der Instance aus der Erfolgsbenachrichtigung aus, um die Seite Instances zu öffnen und den Status des Starts zu überwachen.
12. Aktivieren Sie das Kontrollkästchen für die Instance. Der anfängliche Status einer Instance ist `pending`. Nach dem Start der Instance ändert sich ihr Zustand in `running`. Wählen Sie den Tab Status und Alarme. Nachdem Ihre Instance die Statusprüfungen bestanden hat, ist sie bereit, Verbindungsanfragen zu empfangen.

Schritt 2: Verbindung mit der Instance herstellen

Welches Verfahren Sie verwenden, hängt vom Betriebssystem der Instance ab. Wenn Sie keine Verbindung mit Ihrer Instance herstellen können, helfen Ihnen die Informationen unter Fehlersuche bei Verbindungsproblemen mit Ihrer Amazon-EC2-Linux-Instance weiter.

Linux-Instances

Sie können sich mit der Linux-Instance über einen SSH-Client verbinden. Wenn Sie Windows auf Ihrem Computer ausführen, öffnen Sie ein Terminal und führen Sie den `ssh`-Befehl aus, um zu überprüfen, ob ein SSH-Client installiert ist. Wenn der Befehl nicht gefunden wird, installieren Sie OpenSSH für Windows.

So stellen Sie per SSH eine Verbindung mit Ihrer Instance her

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und klicken Sie auf Connect (Verbinden).
4. Auf der Seite Verbindung mit Instance herstellen wählen Sie die Registerkarte SSH-Client aus.
5. (Optional) Wenn Sie beim Starten der Instance ein Schlüsselpaar erstellt haben und den privaten Schlüssels (PEM-Datei) auf einen Computer unter Linux oder macOS heruntergeladen haben, führen Sie den chmod-Beispielbefehl aus, um die Berechtigungen für Ihren privaten Schlüssel festzulegen.

6. Kopieren Sie den SSH-Beispielbefehl. Im Folgenden finden Sie ein Beispiel, bei dem *Schlüsselpaarname*.pem der Name Ihrer privaten Schlüsseldatei, *ec2-user* der mit dem Image verknüpfte Benutzername und die Zeichenfolge nach dem @-Symbol der öffentliche DNS-Name der Instance ist.

```
ssh -i key-pair-name.pem ec2-user@ec2-198-51-100-1.us-east-2.compute.amazonaws.com
```

7. Führen Sie in einem Terminalfenster auf Ihrem Computer den ssh-Befehl aus, den Sie im vorherigen Schritt gespeichert haben. Wenn sich die private Schlüsseldatei nicht im aktuellen Verzeichnis befindet, müssen Sie in diesem Befehl den vollqualifizierten Pfad zur Schlüsseldatei angeben.

   Nachfolgend finden Sie eine Beispielantwort:

```
The authenticity of host 'ec2-198-51-100-1.us-east-2.compute.amazonaws.com
 (198-51-100-1)' can't be established.
ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
Are you sure you want to continue connecting (yes/no)?
```

8. (Optional) Vergewissern Sie sich, dass der Fingerabdruck in der Sicherheitswarnung mit dem Instance-Fingerabdruck übereinstimmt, der in der Konsolenausgabe enthalten ist, wenn Sie eine Instance zum ersten Mal starten. Um die Konsolenausgabe abzurufen, wählen Sie Aktionen, Überwachung und Fehlerbehebung, Systemprotokoll abrufen aus. Wenn die Fingerabdrücke nicht übereinstimmen, versucht jemand möglicherweise einen Man-in-the-Middle-Angriff durchzuführen. Falls die Fingerabdrücke übereinstimmen, können Sie mit dem nächsten Schritt fortfahren.
9. Geben Sie ei **yes**.

   Nachfolgend finden Sie eine Beispielantwort:

```
Warning: Permanently added 'ec2-198-51-100-1.us-
east-2.compute.amazonaws.com' (ECDSA) to the list of known hosts.
```

Windows-Instances

Zur Verbindung mit einer Windows-Instance mit RDP müssen Sie das anfängliche Administratorpasswort abrufen und es angeben, wenn Sie per Remote Desktop eine Verbindung mit Ihrer Instance herstellen. (Nach dem Start der Instance dauert es einige Minuten, bis das Passwort

verfügbar ist.) Ihr Konto muss über die Berechtigung zum Aufrufen der Aktion GetPasswordData verfügen. Weitere Informationen finden Sie unter Beispielrichtlinien zur Steuerung des Zugriffs auf die EC2 Amazon-API.

Der Standardbenutzername für das Administratorkonto hängt von der Sprache des Betriebssystems (OS) ab, das im AMI enthalten ist. Um den richtigen Benutzernamen zu ermitteln, identifizieren Sie die Sprache des Betriebssystems und wählen Sie dann den entsprechenden Benutzernamen. Für ein englisches Betriebssystem lautet der Benutzername beispielsweise `Administrator`, für ein französisches Betriebssystem ist es `Administrateur` und für ein portugiesisches Betriebssystem ist es `Administrador`. Wenn eine Sprachversion des Betriebssystems keinen Benutzernamen in derselben Sprache hat, wählen Sie den Benutzernamen `Administrator (Other)`. Weitere Informationen finden Sie unter Lokalisierte Namen für Administratorkonto in Windows auf der Microsoft-Website.

So rufen Sie das Administrator-Passwort ab

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und klicken Sie auf Connect (Verbinden).
4. Auf der Seite Verbindung mit Instance herstellen wählen Sie die Registerkarte RDP-Client aus.
5. Wählen Sie unter Benutzername den Standardbenutzernamen für das Administratorkonto aus. Der von Ihnen gewählte Benutzername muss der Sprache des Betriebssystems (OS) entsprechen, das im AMI enthalten ist, das Sie zum Starten Ihrer Instance verwendet haben. Wenn es keinen Benutzernamen in derselben Sprache wie Ihr Betriebssystem gibt, wählen Sie Administrator (Andere).
6. Wählen Sie Passwort erhalten.
7. Gehen Sie auf der Seite Windows-Passwort erhalten wie folgt vor:

    a. Klicken Sie auf Private Schlüsseldatei hochladen und navigieren Sie zu der privaten Schlüsseldatei (`.pem`), die Sie beim Starten der Instance angegeben haben. Wählen Sie die Datei aus und klicken Sie auf Open (Öffnen), um den gesamten Inhalt der Datei auf dieses Fenster zu kopieren.

    b. Klicken Sie auf Password entschlüsseln. Die Seite Passwort erhalten wird geschlossen und das Standard-Administrator-Passwort für die Instance wird unter Passwort angezeigt. Es ersetzt den zuvor angezeigten Link Passwort erhalten.

c. Bewahren Sie das Passwort an einem sicheren Ort auf. Dieses Passwort wird benötigt, um eine Verbindung mit der Instance herzustellen.

Das folgende Verfahren verwendet den Remote Desktop Connection Client für Windows (MSTSC). Wenn Sie einen anderen RDP-Client verwenden, laden Sie die RDP-Datei herunter und lesen Sie dann in der Dokumentation für den RDP-Client nach, wie Sie die RDP-Verbindung herstellen.

So stellen Sie mithilfe eines RDP-Clients eine Verbindung zu einer Windows-Instance her

1. Wählen Sie auf der Seite Mit Instance verbinden die Option Remote-Desktop-Datei herunterladen aus. Klicken Sie nach dem Herunterladen der Datei auf Abbrechen, um zur Seite Instances zurückzukehren. Die RDP-Datei wurde in Ihren `Downloads`-Ordner heruntergeladen.
2. Führen Sie `mstsc.exe` aus, um den RDP-Client zu öffnen.
3. Erweitern Sie Optionen anzeigen, wählen Sie Öffnen und wählen Sie die RDP-Datei aus Ihrem `Downloads`-Ordner aus.
4. Standardmäßig ist Computer der öffentliche IPv4-DNS-Name der Instance und Benutzername ist das Administratorkonto. Um stattdessen über IPv6 eine Verbindung mit der Instance herzustellen, ersetzen Sie den öffentlichen IPv4-DNS-Namen der Instance durch ihre IPv6-Adresse. Überprüfen und ändern Sie nach Bedarf die folgenden Einstellungen.
5. Wählen Sie Connect aus. Wenn Sie eine Warnmeldung erhalten, dass der Publisher der Remote-Verbindung unbekannt ist, klicken Sie auf Verbinden, um fortzufahren.
6. Geben Sie das Passwort ein, das Sie zuvor gespeichert haben, und klicken Sie dann auf OK.
7. Aufgrund der Art selbst signierter Zertifikate erhalten Sie möglicherweise eine Warnmeldung, dass das Sicherheitszertifikat nicht authentifiziert werden konnte. Führen Sie eine der folgenden Aktionen aus:
   - Wenn Sie dem Zertifikat vertrauen, wählen Sie Ja, um eine Verbindung mit Ihrer Instance herzustellen.
   - [Windows] Bevor Sie fortfahren, vergleichen Sie den Fingerabdruck des Zertifikats mit dem Wert im Systemprotokoll, um die Identität des Remotecomputers zu bestätigen. Wählen Sie Zertifikat anzeigen und dann auf der Registerkarte Details die Option Fingerabdruck. Vergleichen Sie diesen Wert mit dem Wert `RDPCERTIFICATE-THUMBPRINT` in Aktionen, Überwachen und Problembehandlung, Systemprotokoll abrufen.
   - [Mac OS X] Bevor Sie fortfahren, vergleichen Sie den Fingerabdruck des Zertifikats mit dem Wert im Systemprotokoll, um die Identität des Remotecomputers zu bestätigen. Wählen Sie Zertifikat anzeigen, erweitern Sie Details und wählen Sie SHA1-Fingerabdrücke. Vergleichen

Sie diesen Wert mit dem Wert `RDPCERTIFICATE-THUMBPRINT` in Aktionen, Überwachen und Problembehandlung, Systemprotokoll abrufen.

8. Wenn die RDP-Verbindung erfolgreich ist, zeigt der RDP-Client den Windows-Anmeldebildschirm und dann den Windows-Desktop an. Wenn Sie stattdessen eine Fehlermeldung erhalten, finden Sie weitere Informationen unter the section called “Der Remotedesktopdienst kann keine Verbindung zu dem Remotecomputer herstellen”. Wenn Sie mit der RDP-Verbindung fertig sind, können Sie den RDP-Client schließen.

Schritt 3: Bereinigen Ihrer Instance

> **Warning**
>
> Das Beenden einer Instance ist dauerhaft und irreversibel.
> Nachdem Sie eine Instance beendet haben, können Sie keine Verbindung mehr zu ihr herstellen und sie kann nicht wiederhergestellt werden. Alle angehängten Amazon-EBS-Volumes, die so konfiguriert sind, dass sie beim Beenden gelöscht werden, werden ebenfalls dauerhaft gelöscht und können nicht wiederhergestellt werden. Alle auf den Instance-Speicher-Volumes gespeicherten Daten gehen dauerhaft verloren. Weitere Informationen finden Sie unter Wie die Kündigung von Instances funktioniert.
> Bevor Sie eine Instance beenden, stellen Sie sicher, dass Sie alle Daten, die Sie nach der Beendigung behalten müssen, im persistenten Speicher gesichert haben.

Nachdem Sie alle Schritte für die Instance abgeschlossen haben, die Sie für dieses Tutorial erstellt haben, sollten Sie die Bereinigung durchführen, indem Sie die Instance beenden. Falls Sie vor dem Bereinigen für diese Instance noch weitere Schritte ausführen möchten, helfen Ihnen die Informationen unter weite Nächste Schritte.

Sobald sich der Status der Instance auf `shutting down` oder `terminated` ändert, fallen keine Gebühren mehr für die Instance oder die Nutzung an, die auf Ihr kostenloses Kontingent angerechnet werden. Um Ihre Instance zur späteren Verwendung beizubehalten, ohne dass Gebühren anfallen, die auf Ihr kostenloses Kontingent angerechnet werden, können Sie die Instance vorerst anhalten und später wieder starten. Weitere Informationen finden Sie unter Stoppen und starten Sie EC2 Amazon-Instances.

So beenden Sie Ihre Instance

1. Wählen Sie im Navigationsbereich Instances aus. Wählen Sie in der Liste mit den Instances die gewünschte Instance aus.
2. Wählen Sie Instance-Status, Instance beenden (löschen).
3. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Beenden (löschen) aus.

   Amazon EC2 fährt Ihre Instance herunter und beendet sie. Nachdem Ihre Instance beendet wurde, bleibt sie auf der Konsole noch für kurze Zeit sichtbar, bevor der Eintrag automatisch gelöscht wird. Sie können die beendete Instance nicht selbst aus der Konsolenanzeige entfernen.

Nächste Schritte

Nachdem Sie Ihre Instance gestartet haben, sollten Sie sich mit den folgenden Schritten befassen:

- Erkunden Sie die Kernkonzepte von Amazon EC2 mit den einführenden Tutorials. Weitere Informationen finden Sie unter Tutorials zum Starten von EC2-Instances.
- Erfahren Sie, wie Sie Ihre Nutzung des kostenlosen Kontingents für Amazon EC2 mithilfe der Konsole verfolgen können. Weitere Informationen finden Sie unter the section called “Ihre Nutzung des kostenlosen Kontingents nachverfolgen”.
- Konfigurieren Sie einen CloudWatch-Alarm, damit Sie benachrichtigt werden, wenn Ihre Nutzung das kostenlose Kontingent überschreitet (für Konten, die vor dem 15. Juli 2025 erstellt wurden). Weitere Informationen finden Sie unter Nachverfolgen Ihres kostenlosen Kontingents für Kostenloses AWS-Kontingent im Benutzerhandbuch für AWS Billing.
- Fügen Sie ein EBS-Volume hinzu. Weitere Informationen finden Sie unter Amazon-EBS-Volume erstellen im Amazon-EBS-Benutzerhandbuch.
- Informieren Sie sich darüber, wie Sie die Remoteverwaltung für Ihre EC2-Instance mit dem Run-Befehl durchführen können. Weitere Informationen finden Sie unter AWS Systems Manager Run Command im Benutzerhandbuch für AWS Systems Manager.
- Erfahren Sie mehr über Kaufoptionen für Instances. Weitere Informationen finden Sie unter EC2 Abrechnungs- und Kaufoptionen von Amazon.
- Ratschläge zu Instance-Typen einholen. Weitere Informationen finden Sie unter Holen Sie sich Empfehlungen vom EC2-Instance-Typ-Finder.

Bewährte Methoden für Amazon EC2

Um den größtmöglichen Nutzen aus Amazon zu ziehen EC2, empfehlen wir Ihnen, die folgenden bewährten Methoden anzuwenden.

Sicherheit

- Verwalten Sie den Zugriff auf AWS Ressourcen und APIs verwenden Sie, wann immer möglich, einen Identitätsverbund mit einem Identitätsanbieter und IAM-Rollen. Weitere Informationen finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.
- Implementieren Sie Regeln mit den höchsten Einschränkungen für Ihre Sicherheitsgruppe.
- Führen Sie regelmäßig Patches und Aktualisierungen durch; sichern Sie das Betriebssystem und die Anwendungen auf Ihrer Instance. Weitere Informationen finden Sie unter Update-Management. Spezifische Richtlinien für Windows-Betriebssysteme finden Sie unter Bewährte Methoden für die Sicherheit in Windows-Instances.
- Verwenden Sie Amazon Inspector, um EC2 Amazon-Instances automatisch zu erkennen und nach Softwareschwachstellen und unbeabsichtigten Netzwerkbedrohungen zu durchsuchen. Weitere Informationen finden Sie im Benutzerhandbuch für Amazon Inspector.
- Verwenden Sie AWS Security Hub CSPM Kontrollen, um Ihre EC2 Amazon-Ressourcen anhand bewährter Sicherheitsmethoden und Sicherheitsstandards zu überwachen. Weitere Informationen zur Verwendung von Security Hub CSPM finden Sie unter Amazon Elastic Compute Cloud Controls im AWS Security Hub CSPM Benutzerhandbuch.

Speicher

- Erfahren Sie mehr über die Auswirkungen des Root-Volume-Typs auf die Persistenz, Sicherung und Wiederherstellung von Daten. Weitere Informationen finden Sie unter Root-Volume-Typ.
- Verwenden Sie getrennte Amazon EBS-Volumes für das Betriebssystem und Ihre Daten. Stellen Sie sicher, dass das Volume mit Ihren Daten nach Beendigung der Instance erhalten bleibt. Weitere Informationen finden Sie unter Daten beim Beenden einer Instance aufbewahren.
- Nutzen Sie den für Ihre Instance verfügbaren Instance-Speicher zum Speichern von temporären Daten. Denken Sie daran, dass die im Instance-Speicher gespeicherten Daten gelöscht werden, wenn Sie Ihre Instance anhalten, in den Ruhezustand versetzen oder beenden. Wenn Sie Instance-Speicher zur Datenbankspeicherung verwenden, stellen Sie sicher, dass Sie einen Cluster mit einem Replikationsfaktor haben, der Fehlertoleranz gewährleistet.

- Verschlüsseln Sie EBS-Volumes und Snapshots. Weitere Informationen finden Sie unter Amazon-EBS-Verschlüsselung im Amazon-EBS-Benutzerhandbuch.

Ressourcenmanagement

- Nutzen Sie Instance-Metadaten und benutzerdefinierte Ressourcen-Tags zur Nachverfolgung und Identifizierung Ihrer AWS -Ressourcen. Weitere Informationen erhalten Sie unter Verwenden Sie Instanz-Metadaten, um Ihre EC2 Instanz zu verwalten und Kennzeichnen Sie Ihre EC2 Amazon-Ressourcen.
- Sehen Sie sich Ihre aktuellen Limits für Amazon an EC2. Planen Sie Anfragen zur Erhöhung der Limits im Voraus vor dem Zeitpunkt, zu dem Sie sie benötigen. Weitere Informationen finden Sie unter EC2 Amazon-Servicekontingente.
- Verwenden Sie diese Option, AWS Trusted Advisor um Ihre AWS Umgebung zu untersuchen und dann Empfehlungen abzugeben, wenn sich Möglichkeiten bieten, Geld zu sparen, die Systemverfügbarkeit und -leistung zu verbessern oder Sicherheitslücken zu schließen. Weitere Informationen finden Sie unter AWS Trusted Advisor im AWS -Support -Benutzerhandbuch.

Sicherung und Wiederherstellung

- Sichern Sie Ihre EBS-Volumes regelmäßig mit Amazon EBS-Snapshots, und erstellen Sie ein Amazon Machine Image (AMI) aus Ihrer Instance, um die Konfiguration als Vorlage zum Starten zukünftiger Instances zu speichern. Weitere Informationen zu AWS Services, die zur Umsetzung dieses Anwendungsfalls beitragen, finden Sie unter AWS Backupund Amazon Data Lifecycle Manager.
- Stellen Sie kritische Komponenten Ihrer Anwendung in mehreren Availability Zones bereit, und replizieren Sie Ihre Daten entsprechend.
- Entwickeln Sie Ihre Anwendungen so, dass sie dynamische IP-Adressierung beim erneuten Starten Ihrer Instance verwalten können. Weitere Informationen finden Sie unter IP-Adressierung von Amazon EC2-Instances.
- Überwachen von und Reagieren auf Ereignisse. Weitere Informationen finden Sie unter Überwachen Sie die EC2 Amazon-Ressourcen.
- Stellen Sie sicher, dass Sie auf die Bearbeitung von Failover vorbereitet sind. Als einfache Lösung können Sie einer Ersatz-Instance manuell eine Netzwerkschnittstelle oder Elastic IP-Adresse zuordnen. Weitere Informationen finden Sie unter Elastic-Network-Schnittstelle. Für eine

automatisierte Lösung können Sie Amazon EC2 Auto Scaling verwenden. Weitere Informationen finden Sie im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

- Testen Sie regelmäßig den Prozess zur Wiederherstellung Ihrer Instances und Amazon-EBS-Volumes, um sicherzustellen, dass Daten und Services erfolgreich wiederhergestellt werden.

Netzwerk

- Setzen Sie den time-to-live (TTL) -Wert für Ihre Anwendungen auf 255, für IPv4 und IPv6. Wenn Sie einen kleineren Wert verwenden, besteht das Risiko, dass die TTL abläuft, während der Anwendungsdatenverkehr unterwegs ist, was zu Erreichbarkeitsproblemen für Ihre Instances führt.

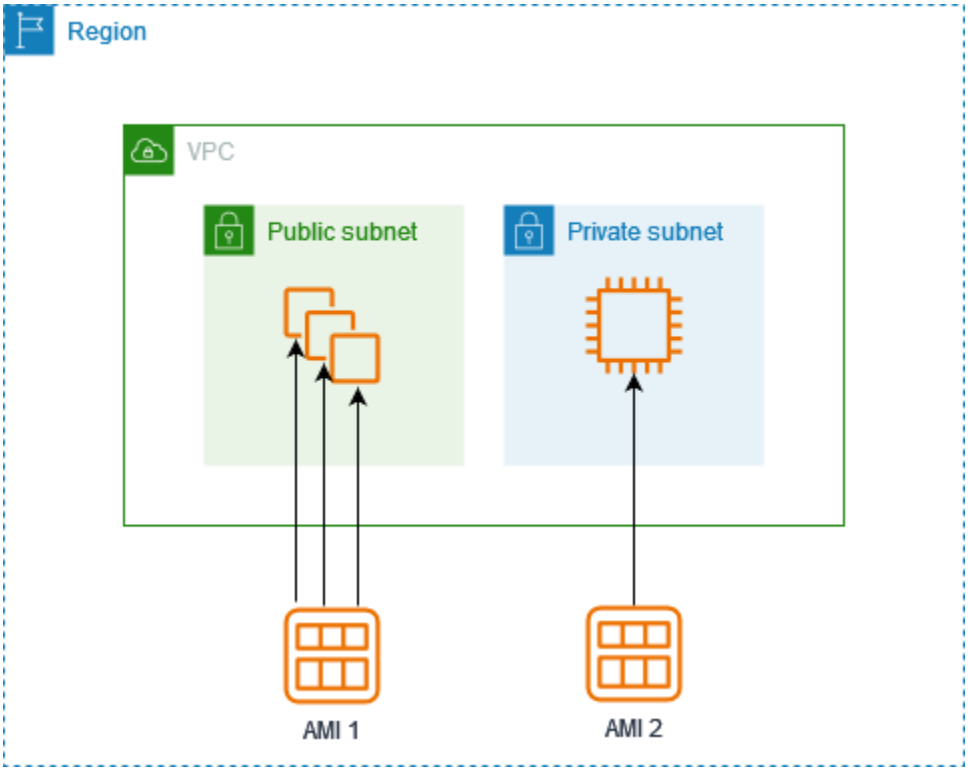
Amazon-Maschinenbilder bei Amazon EC2

Ein Amazon Machine Image (AMI) ist ein Image, das die Software bereitstellt, die zum Einrichten und Starten einer EC2 Amazon-Instance erforderlich ist. Jedes AMI enthält auch eine Blockgerät-Zuweisung, die angibt, welche Blockgeräte an die von Ihnen gestarteten Instances angeschlossen werden sollen. Beim Starten einer Instance müssen Sie ein AMI angeben. Das AMI muss mit dem Instance-Typ kompatibel sein, den Sie für Ihre Instance gewählt haben. Sie können ein von bereitgestelltes AMI AWS, ein öffentliches AMI, ein AMI, das eine andere Person mit Ihnen geteilt hat, oder ein AMI verwenden, das Sie bei der gekauft haben AWS Marketplace.

Ein AMI ist spezifisch für Folgendes:

- Region
- Betriebssystem
- Prozessorarchitektur
- Root-Volume-Typ
- Virtualisierungstyp

Sie können mehrere Instances aus einem einzigen AMI starten, wenn Sie mehrere Instances mit derselben Konfiguration benötigen. Sie können verschiedene Instances verwenden AMIs , um Instances zu starten, wenn Sie Instances mit unterschiedlichen Konfigurationen benötigen, wie in der folgenden Abbildung dargestellt.



Sie können ein AMI aus Ihren EC2 Amazon-Instances erstellen und es dann verwenden, um Instances mit derselben Konfiguration zu starten. Sie können ein AMI in eine andere AWS Region kopieren und es dann verwenden, um Instances in dieser Region zu starten. Sie können ein von Ihnen erstelltes AMI auch mit anderen Konten teilen, sodass diese Instances mit derselben Konfiguration starten können. Sie können Ihr AMI mit dem verkaufen AWS Marketplace.

Inhalt

- AMI-Typen und -Merkmale bei Amazon EC2
- Finden Sie ein AMI, das die Anforderungen für Ihre EC2-Instance erfüllt
- Gebührenpflichtige AMIs im AWS Marketplace für Amazon-EC2-Instances
- Amazon EC2 AMI-Lebenszyklus
- Instance-Startverhalten mit Amazon-EC2-Startmodi
- Verwenden der Verschlüsselung mit EBS-gestützten AMIs
- Verstehen Sie die gemeinsame AMI-Nutzung in Amazon EC2
- Überwachen Sie AMI-Ereignisse mit Amazon EventBridge
- Verstehen von AMI-Fakturierungsdaten
- AMI-Kontingente in Amazon EC2

AMI-Typen und -Merkmale bei Amazon EC2

Wenn Sie eine Instance starten, muss das von Ihnen gewählte AMI mit dem von Ihnen gewählten Instance-Typ kompatibel sein. Sie können ein AMI aufgrund der folgenden Merkmale auswählen:

- Region
- Betriebssystem
- Prozessorarchitektur
- Startberechtigungen
- Root-Volume-Typ
- Virtualisierungstypen

Startberechtigungen

Startberechtigungen legen fest, wer ein AMI zum Starten von Instances verwenden kann. Sie können sich Startberechtigungen wie die gemeinsame Nutzung eines AMI vorstellen – wenn Sie Startberechtigungen erteilen, teilen Sie das AMI mit anderen Benutzern. Nur der Eigentümer eines AMI kann dessen Verfügbarkeit durch Vergabe von Startberechtigungen festlegen. Startberechtigungen lassen sich in die folgenden Kategorien einteilen.

Startberechtigung	Beschreibung
öffentlich	Der Besitzer erteilt allen AWS Konten Startberechtigungen.
explizit	Der Besitzer erteilt bestimmten AWS Konten, Organisationen oder Organisationseinheiten Startberechtigungen (OUs).
implizit	Der Eigentümer hat implizite Startberechtigungen für ein AMI.

Amazon und die EC2 Amazon-Community bieten eine große Auswahl an Zielgruppen AMIs. Weitere Informationen finden Sie unter Verstehen Sie die gemeinsame AMI-Nutzung in Amazon EC2. Entwickler können für ihre Gebühren Gebühren erheben AMIs. Weitere Informationen finden Sie unter Gebührenpflichtige AMIs im AWS Marketplace für Amazon-EC2-Instances.

Root-Volume-Typ

Alle AMIs werden entweder als von Amazon EBS oder von Amazon S3 unterstützt eingestuft.

- Amazon-EBS-gestütztes AMI – Das Root-Volume für eine Instance, die über das AMI gestartet wird, ist ein Amazon Elastic Block Store (Amazon EBS)-Volume, das aus einem Amazon-EBS-Snapshot erstellt wird. Wird sowohl für Linux als auch für Windows AMIs unterstützt.
- Amazon-S3-gestütztes AMI – Das Root-Volume für eine Instance, die über das AMI gestartet wird, ist ein Instance-Speicher-Volume, das aus einer in Amazon S3 gespeicherten Vorlage erstellt wird. Wird AMIs nur für Linux unterstützt. Windows unterstützt AMIs keinen Instance-Speicher für das Root-Volume.

Weitere Informationen finden Sie unter Root-Volumes für Ihre Amazon-EC2-Instances.

> **Note**
>
> Amazon S3-gestützte Produkte AMIs gelten als Ende ihrer Nutzungsdauer und werden nicht für eine neue Verwendung empfohlen. Sie werden nur auf den folgenden älteren Instance-Typen unterstützt: C1, C3, D2, I2, M1, M2, M3, R3 und X1.

In der folgenden Tabelle sind die wichtigen Unterschiede bei der Verwendung der beiden Typen von zusammengefasst. AMIs

Merkmal	Amazon EBS-Backed AMI	Amazon-S3-gestütztes AMI
Root-Volume	EBS-Volume	Instance-Speicher-Volume
Startzeit für eine Instance	Normalerweise unter 1 Minute	Normalerweise unter 5 Minuten
Datenpersistenz	Das Root-Volume wird standardmäßig gelöscht, wenn die Instance beendet wird.* Daten auf alle anderen EBS-Volumes nach Beendigung der Instance erhalten.	Daten auf Instance-Speicher-Volumes bleiben nur während der Lebensdauer der Instance erhalten.

Merkmal	Amazon EBS-Backed AMI	Amazon-S3-gestütztes AMI
Angehaltener Zustand	Kann sich in einem angehaltenen Zustand befinden. Selbst wenn die Instance angehalten ist und nicht ausgeführt wird, wird das Root-Volume in Amazon EBS dauerhaft gespeichert.	Darf nicht im angehaltenen Status sein; Instances werden ausgeführt oder wurden beendet
Modifikationen	Instance-Typ, Kernel, RAM-Daten träger und Benutzerdaten können geändert werden, während die Instance gestoppt ist.	Instance-Attribute sind über die Lebensdauer einer Instance festgelegt.
Gebühren	Ihnen wird die Instance-Nutzung, EBS-Volume-Nutzung und das Speichern Ihres AMI als EBS-Snapshot berechnet.	Ihnen wird die Instance-Nutzung und das Speichern Ihres AMI in Amazon S3 berechnet.
AMI-Erstellung/-Bündelung	Verwendet einen einzelnen Befehl/Aufruf	Erfordert Installation und Verwendung von AMI-Tools

* Standardmäßig ist das Flag `DeleteOnTermination` für EBS-Root-Volumes auf `true` gesetzt. Weitere Informationen zum Ändern dieses Flags, so dass das Volume nach der Beendigung erhalten bleibt, finden Sie unter Behalten Sie ein Amazon-EBS-Root-Volume nach dem Beenden einer Amazon-EC2-Instance.

** Nur unterstützt mit `io2`-EBS Block Express. Weitere Informationen finden Sie unter Bereitgestellte-IOPS-SSD-Block-Express-Volumes im Amazon-EBS-Benutzerhandbuch.

Identifizieren Sie den Root-Volume-Typ, der von Ihrem AMI bestimmt wird

Das AMI, das Sie zum Starten einer EC2 Instance verwenden, bestimmt den Typ des Root-Volumes. Das Root-Volume einer EC2 Instance ist entweder ein EBS-Volume oder ein Instance-Speicher-Volume.

Nitro-basierte Instances unterstützen nur EBS-Root-Volumes. Die folgenden Instance-Typen der vorherigen Generation sind die einzigen, die Instance-Speicher Root-Volumes unterstützen: C1, C3, D2, I2, M1, M2, M3, R3 und X1.

Console

So identifizieren Sie den Root-Volume-Typ, der von einem AMI bestimmt wird

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich das AMI aus AMIs, und wählen Sie es aus.
3. Prüfen Sie auf der Registerkarte Details den Wert unter Root-Gerätetyp wie folgt:
   - `ebs` – Instances, die über dieses AMI gestartet werden, erhalten ein EBS-Root-Volume
   - `instance store` – Instances, die über dieses AMI gestartet werden, erhalten ein Instance-Speicher-Root-Volume

AWS CLI

So identifizieren Sie den Root-Volume-Typ, der von einem AMI bestimmt wird

Verwenden Sie den Befehl describe-images.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[].RootDeviceType
```

Es folgt eine Beispielausgabe.

```
ebs
```

PowerShell

So identifizieren Sie den Root-Volume-Typ, der von einem AMI bestimmt wird

Verwenden Sie das cmdlet Get-EC2Image.

```
(Get-EC2Image `
    -ImageId ami-0abcdef1234567890).RootDeviceType.Value
```

Es folgt eine Beispielausgabe.

```
ebs
```

Virtualisierungstypen

Amazon Machine Images verwenden einen von zwei Virtualisierungstypen: Paravirtual (PV) oder Hardware Virtual Machine (HVM). Die Hauptunterschiede zwischen PV und HVM AMIs bestehen in der Art und Weise, wie sie booten und ob sie spezielle Hardwareerweiterungen (CPU, Netzwerk und Speicher) für eine bessere Leistung nutzen können. Windows AMIs ist HVM AMIs.

In der folgenden Tabelle werden HVM und PV verglichen. AMIs

Merkmal	HVM (Hardwaregestützte virtuelle Maschine)	PV
Description	HVM AMIs verfügen über einen vollständig virtualisierten Hardwaresatz und starten, indem der Master-Boot-Record des Root-Block-Geräts Ihres Images ausgeführt wird. Dieser Virtualisierungstyp kann ein Betriebssystem direkt auf einer virtuellen Maschine ausführen, ohne dass diese modifiziert werden muss – ganz so, als würde es sich um Bare-Metal-Hardware handeln. Das EC2 Amazon-Hostsystem emuliert einen Teil oder die gesamte zugrunde liegende Hardware, die dem Gast präsentiert wird.	PV AMIs bootet mit einem speziellen Bootloader namens PV-GRUB, der den Boot-Zykl us startet und anschließend den in der `menu.lst` Datei auf Ihrem Image angegeben en Kernel kettenweise lädt. Paravirtual-Gäste können auf Host-Hardware ausgeführt werden, die keine explizite Unterstützung für Virtualis ierung hat. Weitere Informati onen zu PV-GRUB und seiner Verwendung in Amazon finden Sie unter Vom Benutzer EC2 bereitgestellte Kernel.
Unterstützte Instance-Typen	Alle Instance-Typen der aktuellen Generation unterstüt zen HVM. AMIs	Die folgenden Instance-Typen der vorherigen Generation unterstützen PV AMIs: C1, C3,

Merkmal	HVM (Hardwaregestützte virtuelle Maschine)	PV
		M1, M3, M2 und T1. Instance-Typen der aktuellen Generation unterstützen PV nicht AMIs.
Unterstützung für Hardware-Erweiterungen	HVM-Gäste können den Vorteil von Hardware-Erweiterungen nutzen, die einen schnellen Zugriff auf die zugrunde liegende Hardware des Hostsystems ermöglichen. Sie müssen erweiterte Netzwerke und GPU-Verarbeitung nutzen. Um Anweisungen an spezialisierte Netzwerk- und GPU-Geräte weiterleiten zu können, muss das Betriebssystem Zugriff auf die native Hardwareplattform haben und HVM-Virtualisierung stellt den erforderlichen Zugriff bereit. Weitere Informationen finden Sie unter Erweitertes Netzwerk in Amazon-EC2-Instances.	Nein, sie können keine speziellen Hardwareerweiterungen wie erweiterte Netzwerk- oder GPU-Verarbeitung nutzen.
Such-Anleitung	Stellen Sie sicher, dass der Virtualisierungstyp des AMI auf `hvm` festgelegt ist. Verwenden Sie hierzu die Konsole oder den Befehl describe-images.	Stellen Sie sicher, dass der Virtualisierungstyp des AMI auf `paravirtual` festgelegt ist. Verwenden Sie hierzu die Konsole oder den Befehl describe-images.

PV auf HVM

Paravirtuelle Gäste schnitten beim Speicher- und Netzwerkbetrieb traditionell besser ab als HVM-Gäste, da sie spezielle Treiber nutzen konnten, wodurch der Aufwand für I/O die Emulation von Netzwerk- und Festplattenhardware vermieden wurde, wohingegen HVM-Gäste diese Anweisungen auf emulierte Hardware übersetzen mussten. Jetzt sind PV-Treiber für HVM-Gäste verfügbar, sodass Betriebssysteme, die nicht für den Betrieb in einer paravirtualisierten Umgebung portiert werden können, dennoch Leistungsvorteile bei Speicher und Netzwerk erzielen können, wenn sie verwendet werden. I/O Mit diesen PV auf HVM-Treibern können HVM-Gäste die gleiche oder eine bessere Leistung als paravirtuelle Gäste erzielen.

Finden Sie ein AMI, das die Anforderungen für Ihre EC2-Instance erfüllt

Ein AMI umfasst die Komponenten und Anwendungen, wie das Betriebssystem und den Typ des Root-Volumes, die zum Starten einer Instance erforderlich sind. Um eine Instance zu starten, müssen Sie ein AMI finden, das Ihren Anforderungen entspricht.

Bei der Auswahl eines AMI müssen Sie die folgenden möglichen Anforderungen an die zu startenden Instances beachten:

- Die AWS-Region der AMI, da die AMI-IDs für jede Region eindeutig sind.
- Das Betriebssystem (z. B. Windows oder Linux).
- Die Architektur: (z. B. 32-Bit, 64-Bit oder 64-Bit-ARM).
- Der Root-Volume-Typ (z. B. Amazon EBS oder Instance-Speicher).
- Der Anbieter (z. B. Amazon Web Services).
- Zusätzliche Software (z. B. SQL Server).

Console

Sie können in der Liste der AMIs auswählen, wenn Sie den Launch Instance Wizard verwenden, oder Sie können alle verfügbaren AMIs über die Seite Images durchsuchen.

So suchen Sie ein Quick-Start-AMI mit dem Launch Instance Wizard

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste die Region aus, in der Sie Ihre Instances starten möchten. Sie können unabhängig von Ihrem Standort jede verfügbare Region auswählen. AMI-IDs sind für jede AWS-Region eindeutig.

3. Wählen Sie im Dashboard der Konsole die Option Launch Instance aus.
4. Wählen Sie unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image) die Option Schnellstart, wählen Sie das Betriebssystem (OS) für Ihre Instance und wählen Sie dann unter Amazon Machine Image (AMI) eines der häufig verwendeten AMIs aus der Liste. Wenn das richtige AMI nicht angezeigt wird, können Sie Browser more AMIs (Weitere AMIs durchsuchen) auswählen, um den vollständigen AMI-Katalog zu durchsuchen. Weitere Informationen finden Sie unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image).

So finden Sie ein AMI über die Seite für AMIs

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste die Region aus, in der Sie Ihre Instances starten möchten. Sie können unabhängig von Ihrem Standort jede verfügbare Region auswählen. AMI-IDs sind für jede AWS-Region eindeutig.
3. Wählen Sie im Navigationsbereich die Option AMIs.
4. Mit den Optionen Filter und Search (Suche) können Sie die angezeigten AMIs so eingrenzen, dass nur die angezeigt werden, die Ihren Kriterien entsprechen.

   Wählen Sie beispielsweise Öffentliche Images aus, um alle AMIs von AWS aufzulisten. Nutzen Sie dann die Optionen von Search (Suche), um die Liste der angezeigten AMIs weiter anzupassen. Wählen Sie die Suchleiste aus und anschließend im Menü Owner alias (Besitzeralias), dann den Operator = und den Wert amazon. Um AMIs zu finden, die einer bestimmten Plattform entsprechen, z. B. Linux oder Windows, wählen Sie erneut in der Suchleiste Plattform, dann den Operator = und dann das Betriebssystem aus der bereitgestellten Liste.
5. (Optional) Wählen Sie das Symbol Einstellungen, um auszuwählen, welche Image-Attribute angezeigt werden sollen, z. B. der Root-Volume-Typ. Alternativ können Sie ein AMI in der Liste auswählen und seine Eigenschaften auf der Registerkarte Details anzeigen.
6. Bevor Sie ein AMI auswählen, müssen Sie Folgendes beachten: Sie müssen wissen, ob das AMI durch Instance-Speicher oder Amazon EBS gestützt ist, und die Auswirkungen dieses Unterschieds kennen. Weitere Informationen finden Sie unter Root-Volume-Typ.
7. Um eine Instance von diesem AMI zu starten, wählen Sie sie aus und wählen Sie dann Instance von Image starten. Informationen zum Starten einer Instance über die Konsole

finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten. Wenn Sie die Instance nicht sofort starten möchten, notieren Sie sich die AMI-ID für später.

AWS CLI

Verwenden Sie den Befehl describe-images, um ein AMI zu suchen, das Ihren Anforderungen entspricht. Standardmäßig gibt dieser Befehl alle öffentlichen AMIs zurück, die Sie besitzen und die für Sie freigegeben sind.

So suchen Sie ein AMI, das Amazon gehört

Verwenden Sie den Befehl describe-images mit der Option `--owners`.

```
aws ec2 describe-images --owners amazon
```

So suchen Sie ein Windows-AMI

Verwenden Sie den folgenden Filter, um nur Windows-AMIs anzuzeigen.

```
--filters "Name=platform,Values=windows"
```

So suchen Sie ein EBS-gestütztes AMI

Fügen Sie den folgenden Filter hinzu, um nur AMIs anzuzeigen, die von Amazon EBS gestützt sind.

```
--filters "Name=root-device-type,Values=ebs"
```

PowerShell

Verwenden Sie das cmdlet Get-EC2Image, um ein AMI zu suchen, das Ihren Anforderungen entspricht. Standardmäßig gibt dieses cmdlet alle öffentlichen AMIs zurück, die Sie besitzen oder die für Sie freigegeben sind.

So suchen Sie ein AMI, das Amazon gehört

Verwenden Sie den Befehl Get-EC2Image mit dem Parameter `-Owner`.

```
Get-EC2Image -Owner amazon
```

So suchen Sie ein Windows-AMI

Verwenden Sie den folgenden Filter, um nur Windows-AMIs anzuzeigen.

```
-Filter @{Name="platform"; Values="windows"}
```

Weitere Informationen und Beispiele finden Sie unter Ein Amazon Machine Image mit Windows PowerShell suchen im Benutzerhandbuch für AWS -Tools für PowerShell.

Zugehörige Ressourcen

Weitere Informationen über AMIs für ein bestimmtes Betriebssystemen finden Sie im Folgenden:

- Amazon Linux 2023 – AL2023 in Amazon EC2 im Benutzerhandbuch für Amazon Linux 2023
- Ubuntu – Amazon EC2 AMI Locator auf der Canonical-Ubuntu-Website.
- RHEL – Red Hat Enterprise Linux Images (AMI) verfügbar in Amazon Web Services (AWS) auf der Red Hat Website.
- Windows Server – AMI-Referenz für AWS Windows

Informationen zu AMIs, die Sie im AWS Marketplace abonnieren können, finden Sie unter Gebührenpflichtige AMIs im AWS Marketplace für Amazon-EC2-Instances.

Informationen zur Verwendung von Systems Manager, um Ihren Benutzern zu helfen, das neueste AMI zu finden, das sie beim Starten einer Instance verwenden sollten, finden Sie im Folgenden:

- Referenz-AMIs mithilfe von Systems-Manager-Parametern
- Mithilfe von öffentlichen Systems-Manager-Parametern auf die neuesten AMIs verweisen

Referenz-AMIs mithilfe von Systems-Manager-Parametern

Wenn Sie eine Instance mit dem EC2 Launch Instance Wizard in der Amazon-EC2-Konsole starten, können Sie entweder ein AMI aus der Liste auswählen oder einen AWS Systems Manager-Parameter auswählen, der auf eine AMI-ID verweist (beschrieben in diesem Abschnitt). Wenn Sie Automatisierungscode zum Starten Ihrer Instances verwenden, können Sie den Systems Manager-Parameter anstelle der AMI-ID angeben.

Ein Systems Manager-Parameter ist ein vom Kunden definiertes Schlüssel-Wert-Paar, das Sie in Systems Manager Parameterspeicher erstellen können. Der Parameterspeicher bietet einen zentralen Speicher zur Auslagerung Ihrer Anwendungskonfigurationswerte. Weitere

Informationen finden Sie unter AWS Systems Manager Parameter Store im AWS Systems ManagerBenutzerhandbuch zu .

Wenn Sie einen Parameter erstellen, der auf eine AMI-ID verweist, stellen Sie sicher, dass Sie den Datentyp als angebe `aws:ec2:image`. Die Angabe dieses Datentyps stellt sicher, dass beim Erstellen oder Ändern des Parameters der Parameterwert als AMI-ID validiert wird. Weitere Informationen finden Sie unter Unterstützung für native Parameter für Amazon Machine Image-IDs im Benutzerhandbuch zu AWS Systems Manager.

Inhalt

- Anwendungsfälle
- Berechtigungen
- Einschränkungen
- Starten einer Instance mit einem Systems Manager-Parameter

Anwendungsfälle

Wenn Sie Systems-Manager-Parameter verwenden, die auf AMI-IDs zu verweisen, können Ihre Benutzer beim Starten von Instances das richtige AMI einfacher auswählen. System-Manager-Parameter können auch die Verwaltung von Automatisierungscode vereinfachen.

Benutzerfreundlicher

Wenn Instances unter Verwendung eines bestimmten AMI gestartet werden müssen und dieses AMI regelmäßig aktualisiert wird, empfehlen wir, dass Ihre Benutzer einen Systems-Manager-Parameter auswählen müssen, um das AMI zu finden. Indem Sie erforderlich machen, dass Ihre Benutzer einen Systems-Manager-Parameter auswählen, wird sichergestellt, dass beim Starten von Instances das neueste AMI verwendet wird.

Beispielsweise könnten Sie in Ihrer Organisation jeden Monat eine neue Version Ihres AMIs erstellen, das die neuesten Betriebssystem- und Anwendungs-Patches enthält. Außerdem müssen Ihre Benutzer Instances mit der neuesten Version Ihres AMIs starten. Um sicherzustellen, dass Ihre Benutzer die neueste Version verwenden, können Sie einen Systems Manager-Parameter (z. B. `golden-ami`) erstellen, der auf die korrekte AMI-ID verweist. Jedes Mal, wenn eine neue Version des AMIs erstellt wird, aktualisieren Sie den AMI-ID-Wert im Parameter, sodass er immer auf das neueste AMI verweist. Ihre Benutzer brauchen nichts von den regelmäßigen Updates des AMI zu wissen, da sie weiterhin jedes Mal denselben Systems-Manager-Parameter auswählen. Die

Verwendung eines Systems-Manager-Parameters für Ihr AMI erleichtert ihnen die Auswahl des richtigen AMI für den Start einer Instance.

Vereinfachen Sie die automatisierte Codepflege

Wenn Sie Automatisierungscode zum Starten Ihrer Instances verwenden, können Sie den Systems Manager-Parameter anstelle der AMI-ID angeben. Wenn eine neue Version des AMI erstellt wird, können Sie den AMI-ID-Wert im Parameter so ändern, dass er auf das neueste AMI verweist. Der Automatisierungscode, der auf den Parameter verweist, muss nicht jedes Mal geändert werden, wenn eine neue Version des AMI erstellt wird. Das vereinfacht die Wartung der Automatisierung und trägt zur Senkung der Bereitstellungskosten bei.

> **Note**
>
> Laufende Instances sind nicht betroffen, wenn Sie die AMI-ID ändern, auf die der Systems-Manager-Parameter verweist.

Berechtigungen

Wenn Sie Systems-Manager-Parameter verwenden, die im Launch Instance Wizard auf AMI-IDs zu verweisen, müssen Sie die folgenden Berechtigungen zu Ihrer IAM-Richtlinie hinzufügen:

- `ssm:DescribeParameters` – Gewährt die Berechtigung, Systems-Manager-Parameter anzuzeigen und auszuwählen.
- `ssm:GetParameters` – Gewährt die Berechtigung zum Abrufen der Werte der Systems-Manager-Parameter.

Sie können auch den Zugriff auf bestimmte Systems Manager-Parameter beschränken. Weitere Informationen und Beispiele für IAM-Richtlinien finden Sie unter Beispiel: Verwenden Sie den EC2 Launch-Instance-Assistenten.

Einschränkungen

AMIs und Systems Manager-Parameter sind regionsspezifisch. Um denselben Systems Manager-Parameternamen in allen Regionen zu verwenden, erstellen Sie in jeder Region einen Systems Manager-Parameter mit demselben Namen (z. B, `golden-ami`). Verweisen Sie in jeder Region mit dem Parameter Systems Manager auf ein AMI in dieser Region.

Bei Parameternamen muss die Groß- und Kleinschreibung beachtet werden. Umgekehrte Schrägstriche für den Parameternamen sind nur erforderlich, wenn der Parameter Teil einer Hierarchie ist, z. B, `/amis/production/golden-ami`. Sie können den umgekehrten Schrägstrich weglassen, wenn der Parameter nicht Teil einer Hierarchie ist.

Starten einer Instance mit einem Systems Manager-Parameter

Anstatt eine AMI-ID anzugeben, wenn Sie eine Instance starten, können Sie einen Systems-Manager-Parameter angeben, der auf eine AMI-ID verweist.

Um den Parameter programmgesteuert anzugeben, verwenden Sie die folgende Syntax, wobei `resolve:ssm` das Standardpräfix und `parameter-name` der eindeutige Parametername ist.

```
resolve:ssm:parameter-name
```

Systems Manager-Parameter bieten Versionsunterstützung. Jeder Iteration eines Parameters wird eine eindeutige Versionsnummer zugewiesen. Sie können die Version des Parameters wie folgt referenzieren, wobei `version` die eindeutige Versionsnummer ist. Standardmäßig wird die neueste Version des Parameters verwendet, wenn keine Version angegeben ist.

```
resolve:ssm:parameter-name:version
```

Informationen zum Starten einer Instance mit einem öffentlichen Parameter, der von AWS bereitgestellt wird, finden Sie unter Mithilfe von öffentlichen Systems-Manager-Parametern auf die neuesten AMIs verweisen.

Console

So suchen Sie ein AMI mithilfe eines Systems-Manager-Parameters

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste die Region aus, in der Sie Ihre Instances starten möchten. Sie können unabhängig von Ihrem Standort jede verfügbare Region auswählen.
3. Wählen Sie im Dashboard der Konsole die Option Launch Instance aus.
4. Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) die Option Browse more AMIs (Weitere AMIs durchsuchen) aus.

5. Wählen Sie die Pfeilschaltfläche rechts neben der Suchleiste und dann Search by Systems Manager parameter (Nach Systems-Manager-Parameter suchen) aus.
6. Wählen Sie für Systems Manager-Parameter einen Parameter aus. Die entsprechende AMI-ID wird unter Currently resolves to (Wird derzeit aufgelöst in) angezeigt.
7. Wählen Sie Search (Suchen) aus. Die AMIs, die der AMI-ID entsprechen, erscheinen in der Liste.
8. Wählen Sie die AMI aus der Liste und wählen Sie Select (Auswählen).

Weitere Informationen über das Starten einer Instance mithilfe des Launch Instance Wizard finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten.

AWS CLI

So starten Sie eine Instance mit einem Systems-Manager-Parameter

Verwenden den Befehl run-instances mit der Option `--image-id`. In diesem Beispiel wird ein Systems-Manager-Parameter mit dem Namen **`golden-ami`** verwendet, der eine AMI-ID angibt.

```
--image-id resolve:ssm:/golden-ami
```

Sie können Versionen eines Systems-Manager-Parameters erstellen. Das folgende Beispiel gibt Version 2 des Parameters **`golden-ami`** an.

```
--image-id resolve:ssm:/golden-ami:2
```

PowerShell

So starten Sie eine Instance mit einem Systems-Manager-Parameter

Verwenden Sie das Cmdlet New-EC2Instance mit dem `-ImageId`-Parameter. In diesem Beispiel wird ein Systems-Manager-Parameter mit dem Namen **`golden-ami`** verwendet, der eine AMI-ID angibt.

```
-ImageId "resolve:ssm:/golden-ami"
```

Sie können Versionen eines Systems-Manager-Parameters erstellen. Das folgende Beispiel gibt Version 2 des Parameters **`golden-ami`** an.

```
-ImageId "resolve:ssm:/golden-ami:2"
```

Mithilfe von öffentlichen Systems-Manager-Parametern auf die neuesten AMIs verweisen

AWS Systems Manager stellt öffentliche -Parameter für öffentliche AMIs bereit, die von AWS gewartet werden. Sie können beim Starten von Instances die öffentlichen Parameter verwenden, um sicherzustellen, dass Sie die neuesten AMIs verwenden. Beispielsweise ist der öffentliche Parameter `/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-arm64` in allen Regionen verfügbar und verweist immer auf die neueste Version des Amazon Linux 2023 AMI für die arm64-Architektur in einer bestimmten Region.

Die öffentlichen Parameter sind über die folgenden Pfade verfügbar:

- Linux – `/aws/service/ami-amazon-linux-latest`
- Windows – `/aws/service/ami-windows-latest`

Weitere Informationen finden Sie unter Arbeiten mit öffentlichen Parametern im AWS Systems Manager-Benutzerhandbuch.

Amazon-Linux-AMIs auflisten

AWS CLI

So listen Sie die Linux-AMIs in der aktuellen AWS-Region auf

Verwenden Sie den Befehl get-parameters-by-path. Der Wert für den `--path`-Parameter ist spezifisch für Linux-AMIs.

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-amazon-linux-latest \
    --query "Parameters[].Name"
```

PowerShell

So listen Sie die Linux-AMIs in der aktuellen AWS-Region auf

Verwenden Sie das cmdlet Get-SSMParametersByPath.

```
Get-SSMParametersByPath `
    -Path "/aws/service/ami-amazon-linux-latest" | `
    Sort-Object Name | Format-Table Name
```

Windows-AMIs auflisten

AWS CLI

So listen Sie die Windows-AMIs in der aktuellen AWS-Region auf

Verwenden Sie den Befehl get-parameters-by-path. Der Wert für den `--path`-Parameter ist spezifisch für Windows-AMIs.

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-windows-latest \
    --query "Parameters[].Name"
```

PowerShell

So listen Sie die Windows-AMIs in der aktuellen AWS-Region auf

Verwenden Sie das cmdlet Get-SSMParametersByPath.

```
Get-SSMParametersByPath `
    -Path "/aws/service/ami-windows-latest" | `
    Sort-Object Name | Format-Table Name
```

Eine Instance mit einem öffentlichen Parameter starten

Um den öffentlichen Parameter beim Starten einer Instance anzugeben, verwenden Sie die folgende Syntax: `resolve:ssm:`*`public-parameter`*, wobei `resolve:ssm` das Standardpräfix und *`public-parameter`* der Pfad und Name des öffentlichen Parameters ist.

AWS CLI

So starten Sie eine Instance mit einem öffentlichen Parameter:

Verwenden den Befehl run-instances mit der Option `--image-id`. Das folgende Beispiel gibt einen öffentlichen Systems-Manager-Parameter für die Image-ID an, um eine Instance mit dem neuesten Amazon-Linux-2023-AMI zu starten.

```
--image-id resolve:ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-
default-x86_64
```

PowerShell

So starten Sie eine Instance mit einem öffentlichen Parameter:

Verwenden Sie das Cmdlet New-EC2Instance mit dem `-ImageId`-Parameter. Das folgende Beispiel gibt einen öffentlichen Systems-Manager-Parameter für die Image-ID an, um eine Instance mit dem neuesten AMI für Windows Server 2022 zu starten.

```
-ImageId "resolve:ssm:/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-Base"
```

Beispiele für die Verwendung von Systems-Manager-Parametern finden Sie unter Abfrage der neuesten Amazon-Linux-AMI-IDs mithilfe des AWS Systems Manager-Parameterspeichers und Abfrage der neuesten Windows AMI mithilfe des AWS Systems Manager-Parameterspeichers.

Gebührenpflichtige AMIs im AWS Marketplace für Amazon-EC2-Instances

Ein gebührenpflichtiges AMI ist ein AMI, das im AWS Marketplace zum Verkauf angeboten wird. Der AWS Marketplace ist ein Online-Shop, in dem Sie Software kaufen können, die in AWS ausgeführt wird; dazu gehören auch AMIs, mit denen Sie Ihre EC2-Instance starten können. Die AWS Marketplace AMIs sind in Kategorien zusammengefasst (z. B. Developer Tools), so dass es einfacher ist, die Produkte zu finden, die Ihre Anforderungen am besten erfüllen. Weitere Informationen über AWS Marketplace finden Sie auf der AWS Marketplace-Website.

Sie können AMIs auch von Drittanbietern im AWS Marketplace erwerben, einschließlich solcher AMIs, die mit Serviceverträgen von Organisationen wie zum Beispiel Red Hat bereitgestellt werden. Sie können auch ein AMI erstellen und es im AWS Marketplace an andere Amazon-EC2-Benutzer verkaufen. Der Aufbau eines sicheren, nutzbaren AMI zum öffentlichen Gebrauch ist ein relativ einfacher Prozess, wenn Sie ein paar simple Richtlinien befolgen. Weitere Informationen zum Erstellen und Verwenden gemeinsamer AMIs finden Sie unter Verstehen Sie die gemeinsame AMI-Nutzung in Amazon EC2.

Der Start einer Instance aus einem gebührenpflichtigen AMI erfolgt auf die gleiche Weise wie der Start aus jedem anderen AMI. Es sind keine zusätzlichen Parameter erforderlich. Die Kosten für die Instance werden auf Basis der von dem Eigentümer des AMI festgelegten Gebühren sowie der Standard-Nutzungsgebühren für die jeweiligen Webservices berechnet; dazu gehört z. B. der

Stundensatz für die Ausführung einer m5.small-Instance in Amazon EC2. Gegebenenfalls fallen zusätzliche Steuern an. Der Eigentümer eines gebührenpflichtigen AMI kann nachvollziehen, ob eine bestimmte Instance mithilfe dieses gebührenpflichtigen AMI gestartet wurde.

> **Important**
>
> Amazon DevPay akzeptiert keine neuen Verkäufer oder Produkte mehr. AWS Marketplace ist jetzt die einzige einheitliche E-Commerce-Plattform für den Verkauf von Software und Services über AWS. Weitere Informationen dazu, wie Sie Software über AWS Marketplace bereitstellen und verkaufen können, finden Sie unter Verkaufen im AWS Marketplace. AWS Marketplace unterstützt alle Amazon-EBS-gestützten AMIs.

Inhalt

- Verkaufen Ihres AMI im AWS Marketplace
- Suchen eines gebührenpflichtigen AMI
- Gebührenpflichtiges AMI im AWS Marketplace erwerben
- Den AWS Marketplace-Produktcode von Ihrer Instance abrufen
- Gebührenpflichtigen Support für unterstützte AWS Marketplace-Angebote verwenden
- Rechnungen für gebührenpflichtige und unterstützte AMIs
- Verwalten Ihrer AWS Marketplace-Abonnements

Verkaufen Ihres AMI im AWS Marketplace

Sie können Ihr AMI mithilfe AWS Marketplace. AWS Marketplace bietet ein strukturiertes Einkaufserlebnis. Darüber hinaus unterstützt AWS Marketplace auch AWS-Features wie Amazon-EBS-gestützte AMIs, Reserved Instances und Spot-Instances.

Weitere Informationen dazu, wie Sie Ihre AMI über AWS Marketplace verkaufen können, finden Sie unter Verkaufen im AWS Marketplace.

Suchen eines gebührenpflichtigen AMI

Ein kostenpflichtiges AMI ist ein Amazon Machine Image (AMI), das käuflich erworben werden kann. Ein kostenpflichtiges AMI hat auch einen Produktcode. Sie finden AMIs, die Sie kaufen können, unter AWS Marketplace.

Console

So suchen Sie ein gebührenpflichtiges AMI

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie im ersten Filterfeld Public images aus.
4. Führen Sie eine der folgenden Aktionen aus:
   - Wenn Sie den Produktcode kennen, wählen Sie Product Code, dann = und geben Sie dann den Produktcode ein.
   - Wenn Sie den Produktcode nicht kennen, geben Sie in der Suchleiste den folgenden Filter an: Owner alias=aws-marketplace. Geben Sie zusätzliche Filter wie erforderlich an.
5. Speichern Sie die ID des AMI.

AWS CLI

So suchen Sie ein gebührenpflichtiges AMI

Verwenden Sie den Befehl describe-images.

```
aws ec2 describe-images --owners aws-marketplace
```

Die Ausgabe umfasst eine große Anzahl von Images. Sie können Filter angeben, mit deren Hilfe Sie bestimmen können, welches AMI Sie benötigen. Nachdem Sie ein AMI gefunden haben, geben Sie dessen ID im folgenden Befehl an, um seinen Produktcode zu erhalten.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[*].ProductCodes[].ProductCodeId
```

Es folgt eine Beispielausgabe.

```
[
    "cdef1234abc567def8EXAMPLE"
]
```

Wenn Sie den Produktcode kennen, können Sie die Ergebnisse nach Produktcode filtern. Dieses Beispiel gibt das neueste AMI mit dem angegebenen Produktcode zurück.

```
aws ec2 describe-images \
    --filters "Name=product-code,Values=cdef1234abc567def8EXAMPLE" \
    --query "sort_by(Images, &CreationDate)[-1].[ImageId]"
```

PowerShell

So suchen Sie ein gebührenpflichtiges AMI

Verwenden Sie das cmdlet Get-EC2Image.

```
Get-EC2Image -Owner aws-marketplace
```

Die Ausgabe umfasst eine große Anzahl von Images. Sie können Filter angeben, mit deren Hilfe Sie bestimmen können, welches AMI Sie benötigen. Nachdem Sie ein AMI gefunden haben, geben Sie dessen ID im folgenden Befehl an, um seinen Produktcode zu erhalten.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).ProductCodes
```

Es folgt eine Beispielausgabe.

```
ProductCodeId             ProductCodeType
-------------             ---------------
cdef1234abc567def8EXAMPLE marketplace
```

Wenn Sie den Produktcode kennen, können Sie die Ergebnisse nach Produktcode filtern. Dieses Beispiel gibt das neueste AMI mit dem angegebenen Produktcode zurück.

```
(Get-EC2Image -Owner aws-marketplace -Filter @{"Name"="product-
code";"Value"="cdef1234abc567def8EXAMPLE"} | sort CreationDate -Descending | Select-
Object -First 1).ImageId
```

Gebührenpflichtiges AMI im AWS Marketplace erwerben

Sie müssen sich für ein gebührenpflichtiges AMI (Erwerb) registrieren, bevor Sie eine Amazon-EC2-Instance mit dem AMI starten können.

In der Regel erhalten Sie vom Verkäufer des gebührenpflichtigen AMI alle erforderlichen Informationen, z. B. den Preis und den Link, unter dem Sie es kaufen können. Wenn Sie auf den

Link klicken, werden Sie zuerst aufgefordert, sich bei AWS anzumelden; danach können Sie das AMI kaufen.

Kaufen eines gebührenpflichtigen AMI mit der Konsole

Sie können ein gebührenpflichtiges AMI kaufen, indem Sie den Amazon EC2-Launch Wizard verwenden. Weitere Informationen finden Sie unter Starten einer Amazon-EC2-Instance von einem AWS Marketplace-AMI.

Abonnieren eines Produkts mit AWS Marketplace

Zur Nutzung des AWS Marketplace benötigen Sie AWS-Konto. Um Instances von AWS Marketplace-Produkten starten zu können, müssen Sie sich für die Verwendung des Amazon-EC2-Service registrieren sowie das Produkt abonnieren, vom dem aus Sie die Instance starten möchten. Sie können eine der folgenden Methoden verwenden, um Produkte im AWS Marketplace zu abonnieren:

- Die AWS Marketplace-Website: Sie können vorkonfigurierte Software schnell über das Feature „Bereitstellung mit 1-Click” starten. Weitere Informationen finden Sie unter AMI-basierte Produkte im AWS Marketplace.
- Der Amazon EC2-Launch Wizard: Sie können nach einer AMI suchen und eine Instance direkt aus dem Launch Wizard starten. Weitere Informationen finden Sie unter Starten einer Amazon-EC2-Instance von einem AWS Marketplace-AMI.

Den AWS Marketplace-Produktcode von Ihrer Instance abrufen

Sie können den AWS Marketplace-Produkt-Code für Ihre Instance abrufen, indem Sie die Metadaten der Instance verwenden. Wenn ein Produkt-Code für die Instance vorhanden ist, wird er von Amazon EC2 ausgegeben. Weitere Informationen zum Abrufen von Metadaten finden Sie unter Auf Instanz-Metadaten für eine EC2 Instanz zugreifen.

IMDSv2

Linux

Führen Sie den folgenden Befehl in Ihrer Linux-Instance aus.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
```

```
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/product-codes
```

Windows

Führen Sie die folgenden cmdlets in Ihrer Windows-Instance aus.

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/product-codes
```

IMDSv1

Linux

Führen Sie den folgenden Befehl in Ihrer Linux-Instance aus.

```
curl http://169.254.169.254/latest/meta-data/product-codes
```

Windows

Führen Sie den folgenden Befehl in Ihrer Windows-Instance aus.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/product-codes
```

Gebührenpflichtigen Support für unterstützte AWS Marketplace-Angebote verwenden

Mit Amazon EC2 können Developer auch Support für Software (oder abgeleitete AMIs) anbieten. Developer können Produkte für den Support erstellen, und Sie können sich für deren Verwendung registrieren. Bei der Registrierung für das Support-Produkt erhalten Sie von dem Developer einen Produkt-Code, den Sie anschließend mit Ihrem eigenen AMI verknüpfen müssen. Auf diese Weise kann der Developer sicherstellen, dass Ihre Instance berechtigt ist, den Support zu erhalten. Außerdem wird so sichergestellt, dass die Gebühren für das Produkt gemäß der Nutzungsbedingungen des Developers in Rechnung gestellt werden können, wenn Sie diesem Produkt zugeordnete Instances ausführen.

Einschränkungen

- Wenn Sie das Attribut für den Produktcode gesetzt haben, kann es nicht mehr geändert oder entfernt werden.
- Sie können ein Support-Produkt nicht mit Reserved Instances verwenden. Es wird immer der Preis berechnet, der vom Verkäufer des jeweiligen Support-Produkts angegeben wurde.

AWS CLI

So ordnen Sie dem AMI einen Produktcode zu

Verwenden Sie den Befehl modify-image-attribute.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --product-codes "cdef1234abc567def8EXAMPLE"
```

PowerShell

So ordnen Sie dem AMI einen Produktcode zu

Verwenden Sie das cmdlet Edit-EC2ImageAttribute.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -ProductCode "cdef1234abc567def8EXAMPLE"
```

Rechnungen für gebührenpflichtige und unterstützte AMIs

Am Monatsende werden Sie per E-Mail benachrichtigt, mit welchem Betrag Ihre Kreditkarte für die Verwendung gebührenpflichtiger oder unterstützter AMIs in diesem Monat belastet wurde. Diese Rechnung wird separat von Ihrer regulären Amazon EC2-Rechnung erstellt. Weitere Informationen finden Sie unter Bezahlen für Produkte im AWS Marketplace-Käuferhandbuch.

Verwalten Ihrer AWS Marketplace-Abonnements

Auf der AWS Marketplace-Website können Sie z B. Ihre Abonnementdaten prüfen, die Nutzungsinformationen des Anbieters anzeigen und Ihre Abonnements verwalten.

-Abonnementdetails prüfen

So prüfen Sie Ihre Abonnementdaten

1. Melden Sie sich bei den an AWS Marketplace.
2. Wählen Sie Your Marketplace Account.
3. Wählen Sie Manage Your Software Subscriptions.
4. Alle aktuellen Abonnements werden aufgelistet. Wählen Sie die Verwendungsanleitung, um spezielle Informationen für die Nutzung des Products anzuzeigen, z. B. den Benutzernamen für die Verbindung mit Ihrer ausgeführten Instance.

Abonnement kündigen

> **Note**
>
> - Durch die Kündigung eines Abonnements werden die mit diesem AMI gestarteten Instances nicht beendet. Wir stellen Ihnen weiterhin Ihre laufenden Instances in Rechnung, bis sie beendet werden. Sie müssen alle mit dem AMI gestarteten Instances beenden, um die Fakturierung für das Abonnement zu beenden.
> - Wenn Sie Ihr Abonnement gekündigt haben, ist es nicht mehr möglich, Instances aus diesem AMI zu starten. Sie können dieses AMI wieder verwenden, wenn Sie es auf der AWS Marketplace-Website oder über den Startassistenten in der Amazon-EC2-Konsole erneut abonnieren.

So kündigen Sie ein AWS Marketplace-Abonnement

1. Um die Fakturierung für das Abonnement anzuhalten, vergewissern Sie sich, dass Sie alle Instances beendet haben, die in dem Abonnement ausgeführt wurden.

   > **Warning**
   >
   > Das Beenden einer Instance ist dauerhaft und irreversibel.
   > Nachdem Sie eine Instance beendet haben, können Sie keine Verbindung mehr zu ihr herstellen und sie kann nicht wiederhergestellt werden. Alle angehängten Amazon-EBS-Volumes, die so konfiguriert sind, dass sie beim Beenden gelöscht werden, werden ebenfalls dauerhaft gelöscht und können nicht wiederhergestellt werden. Alle auf den

Instance-Speicher-Volumes gespeicherten Daten gehen dauerhaft verloren. Weitere Informationen finden Sie unter Wie die Kündigung von Instances funktioniert.
Bevor Sie eine Instance beenden, stellen Sie sicher, dass Sie alle Daten, die Sie nach der Beendigung behalten müssen, im persistenten Speicher gesichert haben.

a. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
b. Wählen Sie im Navigationsbereich Instances aus.
c. Wählen Sie die Instance und dann Instance-Status und Instance beenden (löschen) aus.
d. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Beenden (löschen) aus.

2. Melden Sie sich bei AWS Marketplace an, klicken Sie auf Your Marketplace Account (Ihr Marketplace-Konto) und danach auf Manage Your Software Subscriptions (Software-Abonnements verwalten).
3. Wählen Sie Cancel subscription. Sie werden aufgefordert, die Kündigung zu bestätigen.

Amazon EC2 AMI-Lebenszyklus

Ein Amazon Machine Image (AMI) ist ein Image, das die Softwarekonfiguration enthält, die zum Einrichten und Hochfahren einer Instance erforderlich ist. Beim Starten einer Instance müssen Sie ein AMI angeben. Sie können die von Amazon AMIs bereitgestellten Produkte verwenden oder Ihre eigenen erstellen AMIs. Das AMI muss sich in dem befinden, AWS-Region in dem Sie Ihre Instance starten möchten.

Der Lebenszyklus eines AMI umfasst das Erstellen, Kopieren, Verwerfen, Deaktivieren und Löschen (Abmelden) des AMI.

Erstellen AMIs. Amazon stellt zwar bereit AMIs , dass Sie Ihre Instances starten können, Sie können jedoch auch maßgeschneiderte Instances erstellen, die auf Ihre Bedürfnisse AMIs zugeschnitten sind. Um ein benutzerdefiniertes AMI zu erstellen, starten Sie eine Instance aus einem vorhandenen AMI, passen Sie die Instance an (zum Beispiel Software installieren und Betriebssystemeinstellungen konfigurieren) und erstellen Sie dann ein AMI aus der Instance. Alle Instance-Anpassungen werden im neuen AMI gespeichert, sodass die Instances, die Sie von Ihrem neuen AMI aus starten, diese Anpassungen enthalten.

Beglaubigbar AMIs. Informationen zum Erstellen eines AMI, das den EC2 Instanznachweis unterstützt, finden Sie unter. Bescheinigbar AMIs

Kopieren. AMIs Sie können ein AMI verwenden, um eine Instance nur in dem zu starten, AWS-Region in dem sich das AMI befindet. Wenn Sie Instances mit derselben Konfiguration in mehreren Regionen starten müssen, kopieren Sie das AMI in die anderen Regionen.

Veraltet AMIs. Um ein AMI als überholt oder veraltet zu kennzeichnen, können Sie ein sofortiges oder zukünftiges Datum für die Außerbetriebnahme festlegen. Veraltete Versionen AMIs werden in den AMI-Listen ausgeblendet, aber Benutzer und Dienste können veraltete Versionen weiterhin verwenden, AMIs wenn sie die AMI-ID kennen.

Deaktivieren. AMIs Um vorübergehend zu verhindern, dass ein AMI verwendet wird, können Sie es deaktivieren. Wenn ein AMI deaktiviert ist, können Sie es nicht verwenden, um neue Instances zu starten. Wenn Sie das AMI jedoch erneut aktivieren, können Sie es erneut verwenden, um Instances zu starten. Beachten Sie, dass die Deaktivierung eines AMI keine Auswirkungen auf bestehende Instances hat, die bereits von diesem aus gestartet wurden.

Abmelden (löschen). AMIs Wenn Sie ein AMI nicht mehr benötigen, können Sie es abmelden, um zu verhindern, dass es zum Starten neuer Instances verwendet wird. Wenn das AMI einer Aufbewahrungsregel entspricht, wird es in den Papierkorb verschoben, wo es wiederhergestellt werden kann, bevor die Aufbewahrungsfrist abläuft. Danach wird es dauerhaft gelöscht. Wenn es keiner Aufbewahrungsregel entspricht, wird es sofort dauerhaft gelöscht. Beachten Sie, dass die Abmeldung eines AMI keine Auswirkungen auf die Instances hat, die bereits aus dem AMI gestartet wurden.

Automatisieren Sie den AMI-Lebenszyklus. Sie können Amazon Data Lifecycle Manager verwenden, um die Erstellung, Aufbewahrung, Kopie, Einstellung und Abmeldung von Amazon AMIs EBS-gestützten Snapshots und deren Backing-Snapshots zu automatisieren. Sie können EC2 Image Builder auch verwenden, um die Erstellung, Verwaltung und Bereitstellung benutzerdefinierter Dateien zu automatisieren AMIs. Weitere Informationen finden Sie unter Automatisieren von Backups mit Amazon Data Lifecycle Manager im Amazon EBS-Benutzerhandbuch und im EC2Image Builder Builder-Benutzerhandbuch.

Inhalt

- Ein Amazon-EBS-gestütztes AMI erstellen
- Ein Amazon-S3-gestütztes AMI erstellen
- Ein Amazon-EC2-AMI mit Windows Sysprep erstellen
- Ein EC2 Amazon-AMI kopieren
- Speichern und Wiederherstellen eines AMI mit S3

- Verwenden Sie AMI-Abstammung, um den Ursprung eines AMI nachzuverfolgen
- Verwaltung und Überwachung der AMI-Nutzung
- Ein Amazon-AMI als veraltet kennzeichnen EC2
- Ein Amazon EC2 AMI deaktivieren
- Aufheben der Registrierung eines Amazon-EC2-AMI

Ein Amazon-EBS-gestütztes AMI erstellen

Sie können Ihr eigenes Amazon-EBS-gestütztes AMI aus einer Amazon-EC2-Instance oder aus einem Snapshot des Root-Volumes einer Amazon-EC2-Instance erstellen.

Um ein Amazon-EBS-gestütztes AMI aus einer Instance zu erstellen, starten Sie zunächst eine Instance mit einem bestehenden Amazon-EBS-gestütztes AMI. Dies kann ein AMI sein, das Sie über denAWS Marketplace erhalten haben, ein per oder VM Import/Export erstelltes AMI oder jedes andere AMI sein, auf das Sie Zugriff haben. Nachdem Sie die Instance an Ihre spezifischen Anforderungen angepasst haben, erstellen und registrieren Sie ein neues AMI. Sie können dann das neue AMI verwenden, um neue Instances mit Ihren Anpassungen zu starten.

> **Note**
>
> Informationen zum Erstellen eines AMI, das die EC2-Instance-Attestierung unterstützt, finden Sie unter Bescheinigbar AMIs.

Die unten beschriebenen Verfahren funktionieren für Amazon EC2-Instances mit verschlüsselten Volumes Amazon Elastic Block Store (Amazon EBS) (einschließlich Stamm-Volume) und für unverschlüsselte Volumes.

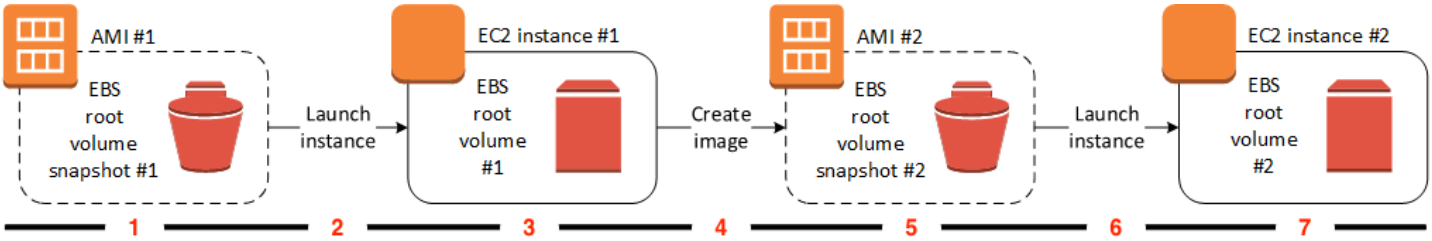
Der Prozess zum Erstellen eines AMI ist anders, als bei Amazon-S3-gestützten AMIs. Weitere Informationen finden Sie unter Ein Amazon-S3-gestütztes AMI erstellen.

Inhalt

- Überblick über die AMI-Erstellung aus einer Instance
- Ein AMI aus einer Instance erstellen
- Ein AMI aus einem Snapshot erstellen

Überblick über die AMI-Erstellung aus einer Instance

Das folgende Diagramm fasst den Prozess zum Erstellen eines Amazon-EBS-gestützten AMI in einer laufenden EC2-Instance zusammen: Beginnen Sie mit einem vorhandenen AMI, starten Sie eine Instance, passen Sie sie an, erstellen Sie daraus ein neues AMI und starten Sie schließlich eine Instance Ihres neuen AMI. Die Zahlen im Diagramm stimmen mit den Zahlen in der folgenden Beschreibung überein.



1 – AMI Nr. 1: Beginnen Sie mit einem vorhandenen AMI

Finden Sie ein vorhandenes AMI, das dem zu erstellenden AMI ähnelt. Dies kann ein AMI sein, das Sie über den AWS Marketplace erhalten haben, ein über VM Import/Export erstelltes AMI oder ein beliebiges anderes AMI sein, auf das Sie Zugriff haben. Sie passen dieses AMI an Ihre Bedürfnisse an.

Im Diagramm gibt EBS root volume snapshot #1 (EBS-Root-Volume-Snapshot Nr. 1) an, dass das AMI ein Amazon-EBS-gestütztes AMI ist und dass Informationen über das Root-Volume in diesem Snapshot gespeichert sind.

2 – Starten Sie eine Instance über ein vorhandenes AMI

Um ein AMI zu konfigurieren, starten Sie eine Instance über das AMI, auf dem Ihr neues AMI basieren soll, und passen Sie die Instance an (im Diagramm mit 3 gekennzeichnet). Dann erstellen Sie ein neues AMI, das die Anpassungen enthält (4 im Diagramm).

3 – EC2-Instance Nr. 1: Passen Sie die Instance an

Stellen Sie eine Verbindung mit Ihrer Instance her und passen Sie sie an Ihre Bedürfnisse an. Ihr neues AMI wird diese Anpassungen enthalten.

Sie können die folgenden Aktionen für Ihre Instance durchführen, um sie anzupassen:

- Installieren von Software und Anwendungen
- Kopieren von Daten
- Reduzieren der Startzeit durch Löschen von temporären Dateien und Defragmentieren Ihrer Festplatte

- Anfügen zusätzlicher EBS-Volumes

4 – Erstellen Sie ein Image

Wenn Sie ein AMI aus einer Instance erstellen, fährt Amazon EC2 die Instance vor dem Erstellen des AMI herunter, um sicherzustellen, dass alle Vorgänge auf der Instance angehalten werden und sich während des Erstellungsprozesses in einem einheitlichen Zustand befinden. Wenn Sie sicher sind, dass sich die Instance in einem einheitlichen und für die AMI-Erstellung geeigneten Zustand befindet, können Sie Amazon EC2 anweisen, die Instance nicht herunterzufahren und neu zu starten. Bei einigen Dateisystemen, z. B. XFS, können Aktivitäten vorübergehend eingefroren werden, damit das Image ohne Neustart der Instance auf sichere Weise erstellt werden kann.

Während der AMI-Erstellung erstellt Amazon EC2 Snapshots des Stamm-Volumes Ihrer Instance und von allen anderen EBS-Volumes, die an Ihre Instance angefügt sind. Ihnen werden Gebühren für die Snapshots in Rechnung gestellt, bis Sie die Registrierung des AMI aufheben und die Snapshots löschen. Wenn an die Instance angefügte Volumes verschlüsselt sind, wird das neue AMI nur auf den Instances erfolgreich gestartet, die Amazon-EBS-Verschlüsselung unterstützen.

Je nach der Größe des Volumes kann die Erstellung des AMI mehrere Minuten in Anspruch nehmen (manchmal sogar bis zu 24 Stunden). Es kann deutlich effizienter sein, vor der Erstellung eines AMI Snapshots der Volumes zu erstellen. Auf diese Weise müssen bei der AMI-Erstellung nur kleine, inkrementelle Snapshots erstellt werden und der Prozess ist schneller abgeschlossen (die Gesamtzeit der Snapshoterstellung bleibt gleich).

5 – AMI Nr. 2: Neues AMI

Nach Abschluss des Prozesses verfügen Sie über ein neues AMI und einen Snapshot Snapshot Nr. 2, der für das Root-Volume der Instance erstellt wurde. Wenn Sie der Instance zusätzlich zum Root-Volume Instance-Speicher-Volumes oder EBS-Volumes hinzugefügt haben, enthält die Blockgerät-Zuweisung für das neue AMI Informationen zu diesen Volumes.

Amazon EC2 registriert das AMI automatisch für Sie.

6 – Starten Sie eine Instance über das neue AMI

Sie können das neue AMI verwenden, um eine Instance zu starten.

7 – EC2-Instance Nr. 2: Neue Instance

Wenn Sie eine Instance mit dem neuen AMI starten, erstellt Amazon EC2 wir mithilfe des Snapshots ein neues EBS-Volume für das Root-Volume der Instance. Wenn Sie beim Anpassen der Instance Instance-Speicher-Volumes oder EBS-Volumes hinzugefügt haben, enthält die

Blockgerät-Zuweisung für das neue AMI Informationen zu diesen Volumes. Außerdem enthalten die Blockgerät-Zuweisungen für Instances, die Sie über das neue AMI starten, automatisch Informationen zu diesen Volumes. Die Instance-Speicher-Volumes, die in der Blockgerät-Zuweisung für die neue Instance angegeben sind, sind neu und enthalten keine Daten von den Instance-Speicher-Volumes der Instance, die Sie zum Erstellen des AMI verwendet haben. Die Daten auf den EBS-Volumes werden beibehalten. Weitere Informationen finden Sie unter Blockgerät-Zuweisungen auf Amazon-EC2-Instances blockieren.

Wenn Sie eine neue Instance aus einem EBS-gestützten AMI erstellen, sollten Sie sowohl das Root-Volume als auch den zusätzlichen EBS-Speicher initialisieren, bevor Sie die Instance in Betrieb nehmen. Weitere Informationen finden Sie unter Amazon-EBS-Volume-Typen initialisieren im Amazon-EBS-Benutzerhandbuch.

Ein AMI aus einer Instance erstellen

Wenn Sie eine bestehende Instance haben, können Sie ein AMI von dieser Instance erstellen.

Console

So erstellen Sie ein AMI

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance, von der aus Sie das AMI erstellen möchten, und wählen Sie Actions (Aktionen), dann Image and templates (Image und Vorlagen) und dann Create image (Image erstellen).

   > **Tip**
   >
   > Wenn diese Option deaktiviert ist, handelt es sich bei Ihrer Instance nicht um eine Amazon EBS-gestützte Instance.

4. Geben Sie auf der Seite Create image (Image erstellen) die folgenden Informationen an:

   a. Geben Sie für Image name (Image-Name) einen eindeutigen Namen für das Image ein, der bis zu 127 Zeichen lang sein kann.

   b. Für Image description (Image-Beschreibung), geben Sie eine optionale Beschreibung des Images mit einer Länge von maximal 255 Zeichen ein.

c. Bei Instance neu starten lassen Sie das Kontrollkästchen entweder aktiviert (Standardeinstellung) oder deaktivieren es.

- Wenn Instance neu starten ausgewählt ist, startet Amazon EC2 bei der Erstellung des neuen AMI die Instance neu, damit Snapshots der angefügten Volumes erstellt werden können, während sich die Daten im Ruhezustand befinden, um einen konsistenten Zustand zu gewährleisten.
- Ist Instance neu starten nicht ausgewählt wenn Amazon EC2 das neue AMI erstellt, wird es nicht heruntergefahren und startet die Instance nicht neu.

> **Warning**
>
> Wenn Sie Instance neu starten abwählen, können wir die Dateisystemintegrität des erstellten Abbilds nicht garantieren.

d. Instance volumes (Instance-Volumes) – Sie können wie folgt das Stamm-Volume ändern sowie weitere Amazon-EBS- und Instance-Speicher-Volumes hinzufügen:

i. Das Stamm-Volume wird in der ersten Zeile definiert.

- Um die Größe des Stamm-Volumes zu ändern, geben Sie für Size (Größe) den erforderlichen Wert ein.
- Wenn Sie Delete on termination (Bei Beenden löschen) auswählen, wird das EBS-Volume gelöscht, sobald Sie die Instance beenden, die aus diesem AMI erstellt wurde. Wenn Sie Delete on termination (Bei Beenden löschen) nicht auswählen, wird das EBS-Volume nicht gelöscht, sobald Sie die Instance beenden. Weitere Informationen finden Sie unter Daten beim Beenden einer Instance aufbewahren.

ii. Wählen Sie zum Hinzufügen eines EBS-Volumes die Option Add volume (Volume hinzufügen) (dadurch wird eine neue Zeile hinzugefügt). Wählen Sie als Speichertyp die Option EBS und füllen Sie die Felder in der Zeile aus. Wenn Sie eine Instance aus Ihrem neuen AMI starten, werden diese zusätzlichen Volumes automatisch der Instance zugeordnet. Leere Volumes müssen formatiert und „gemountet“ werden. Volumes, die auf einem Snapshot basieren, müssen „gemountet“ werden.

iii. Informationen zum Hinzufügen eines Instance-Speicher-Volumes finden Sie unter Instance-Speicher-Volumes zu einem Amazon-EC2-AMI hinzufügen. Wenn Sie eine Instance aus Ihrem neuen AMI starten, werden zusätzliche Volumes automatisch

initialisiert und gemountet. Diese Volumes enthalten keine Daten aus den Instance-Speicher-Volumes der ausgeführten Instance, auf der Ihr AMI basiert.

e. Snapshot-Ziel – Wenn sich Ihre Instance-Volumes in einer Local Zone befinden, die lokale EBS-Snapshots unterstützt, wählen Sie aus, wo die AMI-Snapshots erstellt werden sollen:

- AWS-Region: Erstellen Sie Snapshots in der übergeordneten Region der Local Zone Ihrer Volumes.
- AWS Local Zone: Erstellen Sie Snapshots in derselben Local Zone wie Ihre Volumes.

> **Note**
>
> Diese Option wird nur in Local Zonen angezeigt, die lokale EBS-Snapshots unterstützen, und nur, wenn Ihre Instance in einer Local Zone erstellt wurde. Wenn sich das Volume in einer Region befindet, wird diese Option nicht angezeigt, und der Snapshot wird automatisch in derselben Region wie das Volume erstellt. Weitere Informationen finden Sie unter Lokale Snapshots in Local Zones im Amazon-EBS-Benutzerhandbuch.

> **Important**
>
> Alle Snapshots der Volumes der Instance müssen sich am selben Speicherort befinden. Überprüfen Sie den Speicherort vorhandener Snapshots. Wenn sich vorhandene Snapshots an einem anderen Speicherort als dem ausgewählten Ziel befinden, schlägt die AMI-Erstellung fehl.

f. Tags (Markierungen) – Sie können das AMI und die Snapshots mit denselben Tags (Markierungen) oder mit unterschiedlichen Tags (Markierungen) markieren.

- Um das AMI und die Snapshots mit den gleichen Tags (Markierungen) zu markieren, wählen Sie Tag image and snapshots together (Image und Snapshots zusammen markieren). Die gleichen Tags (Markierungen) werden auf das AMI und jeden erstellten Snapshot angewendet.
- Um das AMI und die Snapshots mit verschiedenen Tags (Markierungen) zu markieren, wählen Sie Tag image and snapshots separately (Image und Snapshots separat

markieren). Verschiedene Tags (Markierungen) werden auf das AMI und die erstellten Snapshots angewendet. Alle Snapshots erhalten jedoch die gleichen Tags (Markierungen). Sie können nicht jeden Snapshot mit einem anderen Tags (Markierungen) versehen.

Sie fügen ein Tag (Markierung) hinzu, indem Sie Add Tags (Tag (Markierung) hinzufügen) auswählen und den Schlüssel und den Wert für das Tags (Markierungen) eingeben. Wiederholen Sie diesen Schritt für jeden Tag (Markierung).

g. Wenn Sie bereit sind, Ihr AMI zu erstellen, wählen Sie Create image (Image erstellen).

5. Sehen Sie den Status Ihres AMI während der Erstellung ein wie folgt:

   a. Wählen Sie im Navigationsbereich die Option AMIs.

   b. Legen Sie den Filter auf Owned by me (Eigentum von mir) fest, um Ihr AMI in der entsprechenden Liste zu finden.

      Am Anfang wird als Status `pending` angezeigt; nach einigen Minuten sollte sich der Status jedoch in `available` ändern.

6. (Optional) Wie Sie den Snapshot anzeigen, der für das neue AMI erstellt wurde:

   a. Notieren Sie die ID des AMIs, das Sie im vorherigen Schritt ausfindig gemacht haben.

   b. Wählen Sie im Navigationsbereich die Option Snapshots.

   c. Stellen Sie den Filter auf Owned by me (Eigentum von mir) ein, und suchen Sie dann den Snapshot mit der neuen AMI-ID in der Spalte Description (Beschreibung).

      Wenn Sie eine Instance über dieses AMI starten, verwendet Amazon EC2 diesen Snapshot, um das Root-Volume der Instance zu erstellen.

AWS CLI

So erstellen Sie ein AMI

Verwenden Sie den Befehl create-image.

```
aws ec2 create-image \
    --instance-id i-1234567890abcdef0 \
    --name "my-web-server" \
    --description "My web server image" \
```

```
    --no-reboot
```

PowerShell

So erstellen Sie ein AMI

Verwenden Sie das cmdlet New-EC2Image.

```
New-EC2Image `
    -InstanceId i-1234567890abcdef0 `
    -Name "my-web-server" `
    -Description "My web server image" `
    -NoReboot $true
```

Ein AMI aus einem Snapshot erstellen

Wenn Sie über einen Snapshot des Root-Volumes einer Instance verfügen, können Sie ein AMI aus diesem Snapshot erstellen.

> **Note**
>
> In den meisten Fällen benötigen AMIs für Windows, Red Hat, SUSE und SQL Server korrekte Lizenzinformationen, um auf dem AMI vorhanden zu sein. Weitere Informationen finden Sie unter Verstehen von AMI-Fakturierungsdaten. Beim Erstellen eines AMI aus einem Snapshot leitet der `RegisterImage`-Vorgang die korrekten Fakturierungsinformationen aus den Metadaten des Snapshots ab. Dazu müssen jedoch die entsprechenden Metadaten vorhanden sein. Um zu überprüfen, ob die richtigen Rechnungsinformationen verwendet wurden, überprüfen Sie das Feld Plattformdetails auf dem neuen AMI. Wenn das Feld leer ist oder nicht dem erwarteten Betriebssystemcode entspricht (z. B. Windows, Red Hat, SUSE oder SQL), war die AMI-Erstellung nicht erfolgreich. Sie sollten das AMI verwerfen und den Anweisungen unter Ein AMI aus einer Instance erstellen folgen.

Console

Ein AMI aus einem Snapshot erstellen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.

3. Wählen Sie den Snapshot aus, aus dem das AMI erstellt werden soll, und wählen Sie dann Actions (Aktionen), Create image from snapshot (Image aus Snapshot erstellen) aus.
4. Geben Sie auf der Seite Image von Snapshot erstellen die folgenden Informationen an:

   a. Geben Sie unter Image-Name einen beschreibenden Namen für das Image ein.

   b. Geben Sie unter Beschreibung eine kurze Beschreibung für das Image ein.

   c. Wählen Sie unter Architektur die Image-Architektur aus. Wählen Sie i386 für 32Bbit, x86_64 für 64-Bit, arm64 für 64-Bit-ARM oder x86_64 für 64-Bit-macOS.

   d. Geben Sie für Root-Gerätename den Gerätenamen ein, der für das Root-Volume verwendet werden soll. Weitere Informationen finden Sie unter Gerätenamen für Volumes auf Amazon-EC2-Instances.

   e. Wählen Sie für Virtualisierungstyp den Virtualisierungstyp aus, der von Instances verwendet werden soll, die von diesem AMI gestartet werden. Weitere Informationen finden Sie unter Virtualisierungstypen.

   f. (Nur zur paravirtuellen Virtualisierung) Für Kernel-ID, wählen Sie den Betriebssystem-Kernel für das Image aus. Wenn Sie einen Snapshot des Root-Volumes einer Instance verwenden, wählen Sie dieselbe Kernel-ID wie die ursprüngliche Instance aus. Wenn Sie sich nicht sicher sind, verwenden Sie den Standardkernel.

   g. (Nur für Paravirtualisierung) Wählen Sie für RAM-Festplatten-ID die RAM-Festplatte für das Image aus. Wenn Sie einen bestimmten Kernel ausgewählt haben, müssen Sie möglicherweise einen bestimmten RAM-Datenträger mit den Treibern auswählen, die ihn unterstützen.

   h. Wählen Sie für den Startmodus den Startmodus für das Image aus, oder wählen Sie Standard verwenden, sodass eine Instance, wenn sie mit diesem AMI gestartet wird, mit dem vom Instance-Typ unterstützten Startmodus gestartet wird. Weitere Informationen finden Sie unter Den Bootmodus eines Amazon-EC2-AMIs festlegen.

   i. (Optional) Passen Sie im Abschnitt Blockgerät-Zuweisungen das Root-Volume an und fügen Sie zusätzliche Daten-Volumes hinzu.

      Für jedes Volume können Sie Größe, Typ, Leistungsmerkmale, das Verhalten des Löschens beim Beenden und den Verschlüsselungsstatus angeben. Für das Stamm-Volume darf die Größe nicht kleiner sein als die Größe des Snapshots. Für den Volume-Typ ist standardmäßig die Allzweck-SSD gp3 ausgewählt.

   j. (Optional) Unter Tags können Sie dem neuen AMI ein oder mehrere Tags hinzufügen. Sie fügen ein Tag (Markierung) hinzu, indem Sie Add Tags (Tag (Markierung)

hinzufügen) auswählen und den Schlüssel und den Wert für das Tags (Markierungen) eingeben. Wiederholen Sie diesen Schritt für jeden Tag (Markierung).

k. Wenn Sie bereit sind, Ihr AMI zu erstellen, wählen Sie Create image (Image erstellen).

5. (Nur Windows, Red Hat, SUSE und SQL Server) Um zu überprüfen, ob die richtigen Fakturierungsinformationen verwendet wurden, überprüfen Sie das Feld Plattformdetails auf dem neuen AMI. Wenn das Feld leer ist oder nicht dem erwarteten Betriebssystemcode entspricht (z. B. Windows oder Red Hat), war die AMI-Erstellung nicht erfolgreich. Sie sollten das AMI verwerfen und den Anweisungen unter Ein AMI aus einer Instance erstellen folgen.

AWS CLI

So erstellen Sie ein AMI aus einem Snapshot mit der AWS CLI

Verwenden Sie den Befehl register-image.

```
aws ec2 register-image \
    --name my-image \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/
xvda,Ebs={SnapshotId=snap-0db2cf683925d191f}
```

PowerShell

So erstellen Sie ein AMI aus einem Snapshot mit PowerShell

Verwenden Sie das cmdlet Register-EC2Image.

```
$block = @{SnapshotId=snap-0db2cf683925d191f}
Register-EC2Image `
    -Name my-image `
    -RootDeviceName /dev/xvda `
    -BlockDeviceMapping @{DeviceName="/dev/xvda";Ebs=$block}
```

Ein Amazon-S3-gestütztes AMI erstellen

Anhand des AMI, das Sie beim Starten Ihrer Instance angeben, wird der Typ des Root-Volumes ermittelt.

Beginnen Sie auf einer Instance, die Sie über ein vorhandenes Amazon-S3-gestütztes Linux-AMI gestartet haben, um ein Amazon-S3-gestütztes Linux-AMI zu erstellen. Nachdem Sie die Instance an Ihre Anforderungen angepasst haben, können Sie das Volume als Paket bündeln (Bundle) und ein neues AMI erstellen und registrieren, um es zum Starten von neuen Instances mit diesen Anpassungen zu verwenden.

Sie können kein Amazon-S3-gestütztes Windows-AMI erstellen, da Windows-AMIs Instance-Speicher für das Root-Volume nicht unterstützen.

> **Important**
>
> Nur die folgenden Instance-Typen unterstützen ein Instance-Speicher-Volume als Root-Volume und erfordern ein Amazon-S3-gestütztes AMI: C1, C3, D2, I2, M1, M2, M3, R3 und X1.

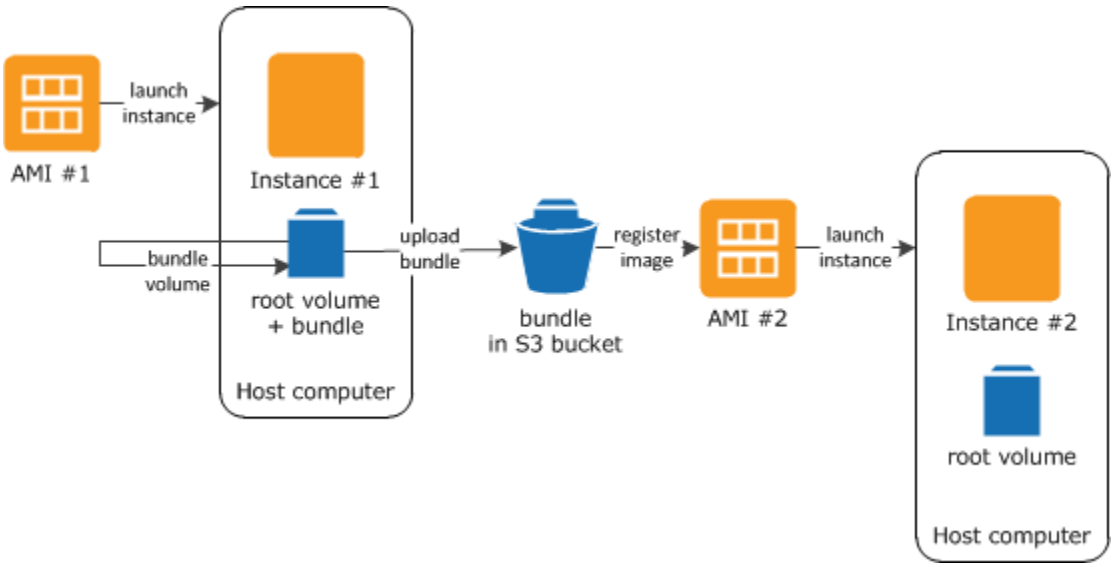
Für das Erstellen von Amazon EBS-backed AMIs wird ein anderer Prozess verwendet. Weitere Informationen finden Sie unter Ein Amazon-EBS-gestütztes AMI erstellen.

Inhalt

- Übersicht über die Erstellung von AMI
- Voraussetzungen
- Erstellen eines AMI aus einer Amazon-Linux-Instance
- Die Amazon-EC2-AMI-Tools einrichten
- AMI-Tools-Referenz für Amazon EC2
- Konvertieren Sie Ihre Amazon-S3-gestütztes AMI in ein Amazon EBS-gestütztes AMI

Übersicht über die Erstellung von AMI

Im folgenden Diagramm ist der Prozess zum Erstellen eines AMI aus einer Instance mit einem Instance-Speicher-Root-Volume dargestellt.



Starten Sie zuerst eine Instance über ein AMI, das dem zu erstellenden AMI ähnelt. Sie können eine Verbindung mit Ihrer Instance herstellen und sie anpassen. Wenn die Instance nach Ihren Vorstellungen konfiguriert ist, können Sie dafür ein Paket (Bundle) erstellen. Es dauert mehrere Minuten, bis die Paketerstellung abgeschlossen ist. Nach Abschluss des Prozesses verfügen Sie über ein Paket, das aus einem Image-Manifest (`image.manifest.xml`) und Dateien (`image.part.xx`) besteht, die eine Vorlage für das Stamm-Volume enthalten. Als Nächstes laden Sie das Paket in Ihren Amazon S3-Bucket hoch und registrieren anschließend Ihr AMI.

> **Note**
>
> Um Objekte für Ihr Amazon-S3-gestütztes Linux-AMI in einen S3-Bucket hochzuladen, müssen ACLs für den Bucket aktiviert sein. Andernfalls kann Amazon EC2 keine ACLs für die hochzuladenden Objekte festlegen. Wenn Ihr Ziel-Bucket die erzwungene Einstellung für den Bucket-Eigentümer für S3 Object Ownership verwendet, funktioniert dies nicht, da ACLs deaktiviert sind. Weitere Informationen finden Sie unter Steuern des Eigentums an Objekten und Deaktivieren von ACLs für Ihren Bucket.

Beim Starten einer Instance mit dem neuen AMI erstellen wir das Stamm-Volume für die Instance mithilfe des Pakets, das Sie in Amazon S3 hochgeladen haben. Für den Speicherplatz, der von dem Paket in Amazon S3 verwendet wird, werden Ihrem Konto Kosten berechnet, bis Sie es löschen. Weitere Informationen finden Sie unter Aufheben der Registrierung eines Amazon-EC2-AMI.

Wenn Sie Ihrer Instance zusätzlich zum Root-Volume Instance-Speicher-Volumes hinzufügen, enthält die Blockgerät-Zuweisung für das neue AMI Informationen zu diesen Volumes. Außerdem

enthalten die Blockgerät-Zuweisungen für Instances, die Sie über das neue AMI starten, automatisch Informationen zu diesen Volumes. Weitere Informationen finden Sie unter Blockgerät-Zuweisungen auf Amazon-EC2-Instances blockieren.

Voraussetzungen

Bevor Sie ein AMI erstellen können, müssen Sie die folgenden Aufgaben durchführen:

- Installieren Sie die AMI-Tools. Weitere Informationen finden Sie unter Die Amazon-EC2-AMI-Tools einrichten.
- Installieren Sie den AWS CLI. Weitere Informationen finden Sie unter Erste Schritte mit AWS CLI.
- Stellen Sie sicher, dass Sie über einen S3-Bucket für das Bundle verfügen und dass für Ihren Bucket ACLs aktiviert sind. Weitere Informationen zur Konfiguration von ACLs finden Sie unter Konfigurieren von ACLs.
  - Öffnen Sie zum Erstellen eines S3-Buckets mit der AWS-Managementkonsole die Amazon-S3-Konsole unter https://console.aws.amazon.com/s3/ und wählen Sie Bucket erstellen aus.
  - Zum Erstellen eines S3-Buckets mit der AWS CLI, können Sie den Befehl mb verwenden. Wenn Ihre installierte Version der AMI-Tools 1.5.18 oder höher ist, können Sie auch den `ec2-upload-bundle`-Befehl verwenden, um den S3-Bucket zu erstellen. Weitere Informationen finden Sie unter ec2-upload-bundle.
- Stellen Sie sicher, dass die Dateien in Ihrem Paket nicht im S3-Bucket verschlüsselt sind. Wenn Sie Verschlüsselung für Ihr AMI benötigen, können Sie stattdessen ein EBS-gestütztes AMI verwenden. Weitere Informationen finden Sie unter Verwenden der Verschlüsselung mit EBS-gestützten AMIs.
- Stellen Sie sicher, dass Sie über Ihre AWS-Konto-ID verfügen. Weitere Informationen finden Sie unter Anzeigen von AWS-Konto-Identifikatoren im AWS-Referenzhandbuch zur Kontoverwaltung.
- Stellen Sie sicher, dass Sie über Anmeldeinformationen zur Verwendung von AWS CLI verfügen. Weitere Informationen finden Sie unter Authentifizierung und Zugriffs-Anmeldeinformationen für die AWS CLI im Benutzerhandbuch für AWS Command Line Interface.
- Stellen Sie sicher, dass Sie über ein X.509-Zertifikat und den entsprechenden privaten Schlüssel verfügen.
  - Informationen zur Erstellung eines X.509-Zertifikats erhalten Sie unter Verwalten von Signaturzertifikaten. Das X.509-Zertifikat und der private Schlüssel werden verwendet, um Ihr AMI zu verschlüsseln und zu entschlüsseln.
  - [China (Peking)] Verwenden Sie das Zertifikat `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-cn-north-1.pem`.

- [AWS GovCloud (US-West)] Verwenden Sie das `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-gov.pem`-Zertifikat.
- Stellen Sie eine Verbindung mit Ihrer Instance her und passen Sie sie an. Sie können beispielsweise Software und Anwendungen installieren, Daten kopieren, temporäre Dateien löschen und die Linux-Konfiguration ändern.

Erstellen eines AMI aus einer Amazon-Linux-Instance

Die folgenden Verfahren beschreiben, wie Sie ein AMI aus einer Instance mit einem Instance-Speicher-Root-Volume erstellen, auf der Amazon Linux 1 ausgeführt wird. Sie funktionieren unter Umständen nicht für Instances, auf denen andere Linux-Verteilungen ausgeführt werden.

So bereiten Sie die Verwendung der AMI-Tools vor (nur HVM-Instances)

1. Für die AMI-Tools ist das richtige Starten von GRUB Legacy-System erforderlich. Verwenden Sie den folgenden Befehl, um GRUB zu installieren:

   ```
   [ec2-user ~]$ sudo yum install -y grub
   ```

2. Installieren Sie die Pakete für die Partitionsverwaltung mit dem folgenden Befehl:

   ```
   [ec2-user ~]$ sudo yum install -y gdisk kpartx parted
   ```

So erstellen Sie ein AMI aus einer Amazon-Linux-Instance mit einem Instance-Speicher-Root-Volume

Hierbei wird vorausgesetzt, dass Sie die Voraussetzungen unter erfüllt habe Voraussetzungen.

Ersetzen Sie in den folgenden Befehlen jeden *Platzhalter für Benutzereingaben* durch Ihre eigenen Informationen.

1. Laden Sie Ihre Anmeldeinformationen auf Ihre Instance hoch. Wir verwenden diese Anmeldeinformationen, um sicherzustellen, dass nur Sie und Amazon EC2 Zugriff auf Ihr AMI haben.

   a. Erstellen Sie auf Ihrer Instance wie folgt ein temporäres Verzeichnis für Ihre Anmeldeinformationen:

      ```
      [ec2-user ~]$ mkdir /tmp/cert
      ```

Auf diese Weise können Sie Ihre Anmeldeinformationen aus der Image-Erstellung ausschließen.

b. Kopieren Sie Ihr X.509-Zertifikat und den dazugehörigen privaten Schlüssel von Ihrem Computer in das Verzeichnis `/tmp/cert` auf Ihrer Instance, indem Sie ein Secure Copy-Tool nutzen, z. B. scp. Die Option `-i` *`my-private-key`*`.pem` im folgenden scp-Befehl ist der private Schlüssel, den Sie zum Herstellen der Verbindung für Ihre Instance mit SSH verwenden, und nicht der private X.509-Schlüssel. Beispiel:

```
you@your_computer:~ $ scp -i my-private-key.pem /
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /
path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  685     0.7KB/s   00:00
```

Da dies reine Textdateien sind, können Sie das Zertifikat und den Schlüssel in einem Text-Editor öffnen und den Inhalt jeweils in neue Dateien unter kopiere `/tmp/cert`.

2. Bereiten Sie das Paket für den Upload in Amazon S3 vor, indem Sie den Befehl ec2-bundle-vol über Ihre Instance ausführen. Achten Sie darauf, die Option `-e` anzugeben, um das Verzeichnis auszuschließen, in dem Ihre Anmeldeinformationen gespeichert sind. Während des Paketprozesses werden standardmäßig Dateien ausgeschlossen, die ggf. vertrauliche Informationen enthalten. Dies sind beispielsweise die Dateien `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` und `*/.bash_history`. Verwenden Sie die Option `--no-filter`, wenn Sie alle diese Dateien einbinden möchten. Mit der Option `--include` können Sie einzelne Dateien einbinden.

> **Important**
>
> Standardmäßig wird beim Prozess zur Erstellung des AMI-Pakets eine komprimierte, verschlüsselte Sammlung von Dateien im Verzeichnis `/tmp` erstellt, das als Ihr Stamm-Volume dient. Falls unter `/tmp` nicht genügend freier Speicherplatz zum Speichern des Pakets vorhanden ist, müssen Sie mit der Option `-d` *`/path/to/bundle/storage`* einen anderen Speicherort für das Paket angeben. Einige Instances verfügen über unter `/mnt` oder `/media/ephemeral0` bereitgestellten flüchtigen Speicher, den Sie verwenden können. Alternativ können Sie auch ein neues Amazon-EBS-Volume

erstellen, anfügen und bereitstellen, um das Paket zu speichern. Weitere Informationen finden Sie unter Amazon-EBS-Volume erstellen im Amazon-EBS-Benutzerhandbuch.

a. Sie müssen den ec2-bundle-vol-Befehl als Root-Benutzer ausführen. Für die meisten Befehle können Sie sudo verwenden, um erhöhte Berechtigungen zu erhalten. In diesem Fall sollten Sie aber sudo -E su ausführen, um Ihre Umgebungsvariablen beizubehalten.

```
[ec2-user ~]$ sudo -E su
```

Beachten Sie, dass Sie in der bash-Eingabeaufforderung nun als root-Benutzer identifiziert werden und dass das Dollarzeichen durch einen Hashtag ersetzt wurde. Hiermit wird angegeben, dass Sie sich in einer root-Shell befinden:

```
[root ec2-user]#
```

b. Führen Sie den Befehl ec2-bundle-vol wie folgt aus, um das AMI-Paket zu erstellen:

```
[root ec2-user]# ec2-bundle-vol -k /tmp/cert/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 123456789012 -r x86_64 -e /tmp/cert --
partition gpt
```

> **Note**
>
> Für die Regionen China (Peking) und AWS GovCloud (US-West) verwenden Sie die Parameter `--ec2cert` und geben Sie die Zertifikate gemäß den Voraussetzungen an.

Die Image-Erstellung kann einige Minuten dauern. Nach Abschluss dieses Befehls enthält Ihr Verzeichnis `/tmp` (bzw. das nicht standardmäßige Verzeichnis) das Paket (`image.manifest.xml` sowie mehrere `image.part.xx`-Dateien).

c. Beenden Sie die root-Shell.

```
[root ec2-user]# exit
```

3. (Optional) Bearbeiten Sie die Blockgerät-Zuweisungen in der Datei `image.manifest.xml` für Ihr AMI, um mehr Instance-Speicher-Volumes hinzuzufügen. Weitere Informationen finden Sie unter Blockgerät-Zuweisungen auf Amazon-EC2-Instances blockieren.

   a. Erstellen Sie ein Backup der Datei `image.manifest.xml`.

   ```
   [ec2-user ~]$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
   ```

   b. Formatieren Sie die Datei `image.manifest.xml` neu, damit sie leichter gelesen und bearbeitet werden kann.

   ```
   [ec2-user ~]$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/
   image.manifest.xml
   ```

   c. Bearbeiten Sie die Blockgerät-Zuweisungen in `image.manifest.xml` mit einem Text-Editor. Das Beispiel unten enthält einen neuen Eintrag für das Instance-Speicher-Volume `ephemeral1`.

   > **Note**
   >
   > Eine Liste der ausgeschlossenen Dateien finden Sie unter ec2-bundle-vol.

   ```
   <block_device_mapping>
     <mapping>
       <virtual>ami</virtual>
       <device>sda</device>
     </mapping>
     <mapping>
       <virtual>ephemeral0</virtual>
       <device>sdb</device>
     </mapping>
     <mapping>
       <virtual>ephemeral1</virtual>
       <device>sdc</device>
     </mapping>
     <mapping>
       <virtual>root</virtual>
       <device>/dev/sda1</device>
     </mapping>
   ```

```
    </block_device_mapping>
```

d. Speichern Sie die Datei `image.manifest.xml` und beenden Sie den Text-Editor.

4. Führen Sie den Befehl ec2-upload-bundle wie folgt aus, um Ihr Paket in Amazon S3 hochzuladen:

```
[ec2-user ~]$ ec2-upload-bundle -b amzn-s3-demo-bucket/bundle_folder/bundle_name -
m /tmp/image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

> **Important**
>
> Wenn Sie Ihr AMI in einer anderen Region als US East (N. Virginia) registrieren möchten, müssen Sie sowohl die Zielregion mit der Option `--region` als auch einen Bucket-Pfad angeben, der in der Zielregion bereits vorhanden ist (bzw. einen eindeutigen Bucket-Pfad, der in der Zielregion erstellt werden kann).

5. (Optional) Nach dem Upload des Pakets in Amazon S3 können Sie das Paket mit dem folgenden `/tmp`-Befehl aus dem Verzeichnis rm auf der Instance entfernen:

```
[ec2-user ~]$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

> **Important**
>
> Wenn Sie mit der Option `-d` */path/to/bundle/storage* einen Pfad in Step 2 angegeben haben, sollten Sie diesen Pfad anstelle von `/tmp` verwenden.

6. Führen Sie den Befehl register-image wie folgt aus, um Ihr AMI zu registrieren:

```
[ec2-user ~]$ aws ec2 register-image --image-location amzn-s3-demo-
bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --
virtualization-type hvm
```

> **Important**
>
> Wenn Sie zuvor für den Befehl ec2-upload-bundle eine Region angegeben haben, müssen Sie die entsprechende Region für diesen Befehl noch einmal angeben.

Die Amazon-EC2-AMI-Tools einrichten

Sie können die AMI-Tools verwenden, um Amazon-S3-gestützte Linux-AMIs zu erstellen und zu verwalten. Um die Tools verwenden zu können, müssen Sie sie auf Ihrer Linux-Instance installieren. Die AMI-Tools sind als RPM-Paket und für Linux-Distributionen, die RPM nicht unterstützen, auch als ZIP-Datei verfügbar.

So richten Sie die AMI-Tools per RPM ein

1. Installieren Sie Ruby mithilfe des Paket-Managers für Ihre Linux-Veteilung, z. B. yum. Beispiel:

   ```
   [ec2-user ~]$ sudo yum install -y ruby
   ```

2. Laden Sie die RPM-Datei mit einem Tool wie wget oder curl herunter. Beispiel:

   ```
   [ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.noarch.rpm
   ```

3. Überprüfen Sie die Signatur der RPM-Datei, indem Sie den folgenden Befehl eingeben:

   ```
   [ec2-user ~]$ rpm -K ec2-ami-tools.noarch.rpm
   ```

   Der obige Befehl sollte ergeben, dass die SHA1- und MD5-Hashes der Datei `OK.` sind. Wenn der Befehl ergibt, dass die Hashes `NOT OK` sind, verwenden Sie den folgenden Befehl, um die Header SHA1- und MD5-Hashes der Datei anzuzeigen:

   ```
   [ec2-user ~]$ rpm -Kv ec2-ami-tools.noarch.rpm
   ```

   Vergleichen Sie dann die Header SHA1- und MD5-Hashes Ihrer Datei mit den folgenden verifizierten AMI-Tools-Hashes, um die Authentizität der Datei zu bestätigen:

   - Header SHA1: a1f662d6f25f69871104e6a62187fa4df508f880
   - MD5: 9faff05258064e2f7909b66142de6782

   Wenn die Header SHA1- und MD5-Hashes Ihrer Datei mit den verifizierten AMI-Tools-Hashes übereinstimmen, fahren Sie mit dem nächsten Schritt fort.

4. Installieren Sie RPM mit dem folgenden Befehl:

   ```
   [ec2-user ~]$ sudo yum install ec2-ami-tools.noarch.rpm
   ```

5. Überprüfen Sie die Installation der AMI-Tools mit dem Befehl ec2-ami-tools-version.

```
[ec2-user ~]$ ec2-ami-tools-version
```

> **Note**
>
> Gehen Sie wie folgt vor, wenn Sie einen Ladefehler erhalten, z. B. „cannot load such file -- ec2/amitools/version (LoadError)“: Führen Sie den nächsten Schritt aus, um dem RUBYLIB-Pfad den Speicherort Ihrer Installation der AMI-Tools hinzuzufügen.

6. (Optional) Wenn Sie im vorherigen Schritt einen Fehler erhalten haben, ist es ratsam, dem RUBYLIB-Pfad den Installationsspeicherort Ihrer AMI-Tools hinzuzufügen.

   a. Führen Sie den folgenden Befehl aus, um die hinzuzufügenden Pfade zu ermitteln.

```
[ec2-user ~]$ rpm -qil ec2-ami-tools | grep ec2/amitools/version
/usr/lib/ruby/site_ruby/ec2/amitools/version.rb
/usr/lib64/ruby/site_ruby/ec2/amitools/version.rb
```

   Im obigen Beispiel befindet sich die fehlende Datei aus dem vorherigen Ladefehler unter /usr/lib/ruby/site_ruby und /usr/lib64/ruby/site_ruby.

   b. Fügen Sie die Speicherorte aus dem vorherigen Schritt Ihrem RUBYLIB-Pfad hinzu.

```
[ec2-user ~]$ export RUBYLIB=$RUBYLIB:/usr/lib/ruby/site_ruby:/usr/lib64/ruby/
site_ruby
```

   c. Überprüfen Sie die Installation der AMI-Tools mit dem Befehl ec2-ami-tools-version.

```
[ec2-user ~]$ ec2-ami-tools-version
```

So richten Sie die AMI-Tools per ZIP-Datei ein

1. Führen Sie die Ruby-Installation und das Entzippen mithilfe des Paket-Managers für Ihre Linux-Distribution durch, z. B. apt-get. Beispiel:

```
[ec2-user ~]$ sudo apt-get update -y && sudo apt-get install -y ruby unzip
```

2. Laden Sie die ZIP-Datei mit einem Tool wie wget oder curl herunter. Beispiel:

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.zip
```

3. Entzippen Sie die Dateien in ein geeignetes Installationsverzeichnis, z. B. `/usr/local/ec2`.

```
[ec2-user ~]$ sudo mkdir -p /usr/local/ec2
$ sudo unzip ec2-ami-tools.zip -d /usr/local/ec2
```

   Beachten Sie, dass die ZIP-Datei den Ordner "ec2-ami-tools-*x.x.x*", wobei *x.x.x* die Versionsnummer der Tools ist (z. B. `ec2-ami-tools-1.5.7`).

4. Legen Sie die Umgebungsvariable `EC2_AMITOOL_HOME` auf das Installationsverzeichnis für die Tools fest. Beispiel:

```
[ec2-user ~]$ export EC2_AMITOOL_HOME=/usr/local/ec2/ec2-ami-tools-x.x.x
```

5. Fügen Sie die Tools Ihrer Umgebungsvariablen `PATH` hinzu. Beispiel:

```
[ec2-user ~]$ export PATH=$EC2_AMITOOL_HOME/bin:$PATH
```

6. Sie können die Installation der AMI-Tools mit dem Befehl ec2-ami-tools-version überprüfen.

```
[ec2-user ~]$ ec2-ami-tools-version
```

Verwalten von Signaturzertifikaten

Für bestimmte Befehle in den AMI-Tools ist ein Signaturzertifikat erforderlich (auch als X.509-Zertifikat bezeichnet). Sie müssen das Zertifikat erstellen und anschließend in hochlade AWS. Beispielsweise können Sie zum Erstellen des Zertifikats ein Drittanbieter-Tool wie OpenSSL verwenden.

So erstellen Sie ein Signaturzertifikat

1. Installieren und konfigurieren Sie OpenSSL.
2. Erstellen Sie mit dem Befehl `openssl genrsa` einen privaten Schlüssel und speichern Sie die Ausgabe in einer `.pem`-Datei. Wir empfehlen Ihnen, einen RSA-Schlüssel mit 2 048 oder 4 096 Bit zu erstellen.

```
openssl genrsa 2048 > private-key.pem
```

3. Generieren Sie mit dem Befehl `openssl req` ein Zertifikat.

```
openssl req -new -x509 -nodes -sha256 -days 365 -key private-key.pem -outform PEM -
out certificate.pem
```

Verwenden Sie zum Hochladen des Zertifikats in AWS den Befehl upload-signing-certificate.

```
aws iam upload-signing-certificate --user-name user-name --certificate-body
 file://path/to/certificate.pem
```

Verwenden Sie den Befehl list-signing-certificates, um die Zertifikate für einen Benutzer aufzulisten:

```
aws iam list-signing-certificates --user-name user-name
```

Verwenden Sie den Befehl update-signing-certificate, um ein Signaturzertifikat für einen Benutzer zu deaktivieren oder wieder zu aktivieren. Mit dem folgenden Befehl wird das Zertifikat deaktiviert:

```
aws iam update-signing-certificate --certificate-id OFHPLP4ZULTHYPMSYEX704BEXAMPLE --
status Inactive --user-name user-name
```

Verwenden Sie den Befehl delete-signing-certificate, um ein Zertifikat zu löschen:

```
aws iam delete-signing-certificate --user-name user-name --certificate-
id OFHPLP4ZULTHYPMSYEX704BEXAMPLE
```

AMI-Tools-Referenz für Amazon EC2

Sie können die AMI-Tools-Befehle verwenden, um Amazon-S3-gestützte Linux-AMIs zu erstellen und zu verwalten. Weitere Informationen über das Einrichten der Tools finden Sie unter Die Amazon-EC2-AMI-Tools einrichten.

Weitere Information über Zugriffsschlüssel finden Sie unter Verwalten von Zugriffsschlüsseln für IAM-Benutzer im IAM-Benutzerhandbuch.

Befehle

- ec2-ami-tools-version
- ec2-bundle-image
- ec2-bundle-vol

- ec2-delete-bundle
- ec2-download-bundle
- ec2-migrate-manifest
- ec2-unbundle
- ec2-upload-bundle
- Allgemeine Optionen für AMI-Tools

ec2-ami-tools-version

Beschreibung

Beschreibt die Version der AMI-Tools.

Syntax

ec2-ami-tools-version

Output

Die Versionsinformationen

Beispiel

Dieser Beispielbefehl zeigt die Versionsinformationen für die AMI-Tools an, die Sie verwenden.

```
[ec2-user ~]$ ec2-ami-tools-version
1.5.2 20071010
```

ec2-bundle-image

Beschreibung

Erstellt ein Amazon-S3-gestütztes Linux-AMI aus einem Betriebssystem-Image, das in einer Loopback-Datei erstellt wurde.

Syntax

ec2-bundle-image -c *path* -k *path* -u *account* -i *path* [-d *path*] [--ec2cert *path*] [-r *architecture*] [--productcodes *code1*,*code2*,...] [-B *mapping*] [-p *prefix*]

Optionen

`-c, --cert` path

Die PEM-kodierte öffentliche RSA-Schlüsselzertifikatsdatei des Benutzers

Erforderlich: Ja

`-k, --privatekey` path

Der Pfad zu einer PEM-kodierten RSA-Schlüsseldatei. Sie müssen diesen Schlüssel zum Entpacken dieses Pakets angeben, bewahren Sie ihn daher gut auf. Dieser Schlüssel muss nicht in Ihrem AWS-Konto registriert sein.

Erforderlich: Ja

`-u, --user` account

Die AWS-Konto-ID des Benutzers ohne Bindestriche

Erforderlich: Ja

`-i, --image` path

Der Pfad zum Image, das gebündelt werden soll

Erforderlich: Ja

`-d, --destination` path

Das Verzeichnis, in dem das Paket erstellt wird

Standard: `/tmp`

Erforderlich: Nein

`--ec2cert` path

Der Pfad zum öffentlichen Amazon EC2 X.509-Schlüsselzertifikat, das zum Verschlüsseln des Image-Manifests verwendet wird.

Die Regionen `us-gov-west-1` und `cn-north-1` verwenden ein nicht standardmäßiges öffentliches Schlüsselzertifikat, und der Pfad zu diesem Zertifikat muss mit dieser Option angegeben werden. Der Pfad zum Zertifikat variiert ausgehend von der Installationsmethode

der AMI-Tools. Für Amazon Linux befinden sich die Zertifikate unter `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Wenn Sie die AMI-Tools aus der RPM- oder ZIP-Datei in Die Amazon-EC2-AMI-Tools einrichten installiert haben, befinden sich die Zertifikate unter `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Erforderlich: Nur für die Regionen `us-gov-west-1` und `cn-north-1`.

`-r, --arch` architecture

Image-Architektur. Wenn Sie die Architektur nicht in der Befehlszeile angeben, werden Sie dazu aufgefordert, sobald das Bündeln beginnt.

Zulässige Werte: `i386` | `x86_64`

Erforderlich: Nein

`--productcodes` code1,code2,...

Produkt-Codes, die dem Image zum Zeitpunkt der Registrierung angefügt werden, durch Kommas getrennt

Erforderlich: Nein

`-B, --block-device-mapping` mapping

Definiert, wie Blockgeräte für eine Instance dieses AMI bereitgestellt werden, wenn der Instance-Typ das angegebene Gerät unterstützt.

Geben Sie eine durch Komma getrennte Liste von Schlüssel-Wert-Paaren an, wobei jeder Schlüssel ein virtueller Name und jeder Wert der entsprechende Gerätename ist. Virtuelle Namen umfassen Folgendes:

- `ami` — Das Stammdateisystemgerät, wie es von der Instance erfasst wird
- `root` — Das Stammdateisystemgerät, wie es vom Kernel erfasst wird
- `swap` — Das Swap-Gerät, wie es von der Instance erfasst wird
- `ephemeralN` — Das n-te Instance-Speicher-Volume

Erforderlich: Nein

`-p, --prefix` prefix

Das Dateinamenpräfix für gebündelte AMI-Dateien

Standard: Der Name der Imagedatei. Wenn der Pfad des Images beispielsweise `/var/spool/my-image/version-2/debian.img` ist, dann ist das Standardpräfix `debian.img`.

Erforderlich: Nein

`--kernel` kernel_id

Veraltet. Verwenden Sie zum Festlegen des Kernels register-image.

Erforderlich: Nein

`--ramdisk` ramdisk_id

Veraltet. Verwenden Sie zum Festlegen des RAM-Datenträgers (sofern erforderlich) register-image.

Erforderlich: Nein

Output

Statusmeldung, die die Phasen und Status des Bündelungsprozesses beschreibt

Beispiel

Dieses Beispiel erstellt ein gebündeltes AMI aus einem Betriebssystem-Image, das in einer Loopback-Datei erstellt wurde.

```
[ec2-user ~]$ ec2-bundle-image -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -i image.img -d bundled/ -r x86_64
Please specify a value for arch [i386]:
Bundling image file...
Splitting bundled/image.gz.crypt...
Created image.part.00
Created image.part.01
Created image.part.02
Created image.part.03
Created image.part.04
Created image.part.05
Created image.part.06
Created image.part.07
Created image.part.08
Created image.part.09
Created image.part.10
```

```
Created image.part.11
Created image.part.12
Created image.part.13
Created image.part.14
Generating digests for each part...
Digests generated.
Creating bundle manifest...
ec2-bundle-image complete.
```

ec2-bundle-vol

Beschreibung

Erstellt ein Amazon-S3-gestütztes Linux-AMI durch Komprimieren, Verschlüsseln und Signieren einer Kopie des Root-Volumes für die Instance.

Amazon EC2 versucht, Produkt-Codes, Kernel-Einstellungen, RAM-Datenträgereinstellungen und Blockgerät-Zuweisungen von der Instance zu erben.

Während des Paketprozesses werden standardmäßig Dateien ausgeschlossen, die ggf. vertrauliche Informationen enthalten. Dies sind beispielsweise die Dateien `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` und `*/.bash_history`. Verwenden Sie die Option `--no-filter`, wenn Sie alle diese Dateien einbinden möchten. Mit der Option `--include` können Sie einzelne Dateien einbinden.

Weitere Informationen finden Sie unter Ein Amazon-S3-gestütztes AMI erstellen.

Syntax

ec2-bundle-vol -c *path* -k *path* -u *account* [-d *path*] [--ec2cert *path*] [-r *architecture*] [--productcodes *code1*,*code2*,...] [-B *mapping*] [--all] [-e *directory1*,*directory2*,...] [-i *file1*,*file2*,...] [--no-filter] [-p *prefix*] [-s *size*] [--[no-]inherit] [-v *volume*] [-P *type*] [-S *script*] [--fstab *path*] [--generate-fstab] [--grub-config *path*]

Optionen

`-c, --cert` path

Die PEM-kodierte öffentliche RSA-Schlüsselzertifikatsdatei des Benutzers

Erforderlich: Ja

`-k, --privatekey` path

Der Pfad zur PEM-kodierten RSA-Schlüsseldatei des Benutzers

Erforderlich: Ja

`-u, --user` account

Die AWS-Konto-ID des Benutzers ohne Bindestriche

Erforderlich: Ja

`-d, --destination` destination

Das Verzeichnis, in dem das Paket erstellt wird

Standard: `/tmp`

Erforderlich: Nein

`--ec2cert` path

Der Pfad zum öffentlichen Amazon EC2 X.509-Schlüsselzertifikat, das zum Verschlüsseln des Image-Manifests verwendet wird.

Die Regionen `us-gov-west-1` und `cn-north-1` verwenden ein nicht standardmäßiges öffentliches Schlüsselzertifikat, und der Pfad zu diesem Zertifikat muss mit dieser Option angegeben werden. Der Pfad zum Zertifikat variiert ausgehend von der Installationsmethode der AMI-Tools. Für Amazon Linux befinden sich die Zertifikate unter `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Wenn Sie die AMI-Tools aus der RPM- oder ZIP-Datei in Die Amazon-EC2-AMI-Tools einrichten installiert haben, befinden sich die Zertifikate unter `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Erforderlich: Nur für die Regionen `us-gov-west-1` und `cn-north-1`.

`-r, --arch` architecture

Die Architektur des Images. Wenn Sie sie nicht in der Befehlszeile angeben, werden Sie dazu aufgefordert, sobald das Bündeln beginnt.

Zulässige Werte: `i386` | `x86_64`

Erforderlich: Nein

`--productcodes` code1,code2,...

Produkt-Codes, die dem Image zum Zeitpunkt der Registrierung angefügt werden, durch Kommas getrennt

Erforderlich: Nein

`-B, --block-device-mapping` mapping

Definiert, wie Blockgeräte für eine Instance dieses AMI bereitgestellt werden, wenn der Instance-Typ das angegebene Gerät unterstützt.

Geben Sie eine durch Komma getrennte Liste von Schlüssel-Wert-Paaren an, wobei jeder Schlüssel ein virtueller Name und jeder Wert der entsprechende Gerätename ist. Virtuelle Namen umfassen Folgendes:

- `ami` — Das Stammdateisystemgerät, wie es von der Instance erfasst wird
- `root` — Das Stammdateisystemgerät, wie es vom Kernel erfasst wird
- `swap` — Das Swap-Gerät, wie es von der Instance erfasst wird
- `ephemeralN` — Das n-te Instance-Speicher-Volume

Erforderlich: Nein

`-a, --all`

Bündeln Sie alle Verzeichnisse, einschließlich derer, die sich auf remote bereitgestellten Dateisystemen befinden.

Erforderlich: Nein

`-e, --exclude` directory1,directory2,...

Eine Liste absoluter Verzeichnispfade und Dateien, die aus dem Bündelungsvorgang ausgeschlossen werden sollen. Dieser Parameter überschreibt die Option `--all`. Wenn ein Ausschließen festgelegt ist, werden die mit dem Parameter aufgeführten Verzeichnisse und Unterverzeichnisse nicht mit dem Volume gebündelt.

Erforderlich: Nein

`-i, --include` file1,file2,...

Eine Liste von Dateien, die in den Bündelungsvorgang einbezogen werden sollen. Die angegeben Dateien werden ansonsten aus dem AMI ausgeschlossen, da sie möglicherweise vertrauliche Informationen enthalten.

Erforderlich: Nein

`--no-filter`

Wenn dies angegeben ist werden wir die Dateien nicht aus dem AMI ausschließen, da sie möglicherweise vertrauliche Informationen enthalten.

Erforderlich: Nein

`-p, --prefix` prefix

Das Dateinamenpräfix für gebündelte AMI-Dateien

Standard: `image`

Erforderlich: Nein

`-s, --size` size

Die Größe der zu erstellenden Image-Datei in MB (1024 * 1024 Bytes). Die maximale Größe ist 10240 MB.

Standard: 10240

Erforderlich: Nein

`--[no-]inherit`

Gibt an, ob das Image die Metadaten der Instance erben soll (standardmäßig werden sie geerbt). Das Bündeln schlägt fehl, wenn Sie `--inherit` aktivieren, auf die Instance-Metadaten aber nicht zugegriffen werden kann.

Erforderlich: Nein

`-v, --volume` volume

Der absolute Pfad zum bereitgestellten Volume, aus dem das Bündel erstellt werden soll

Standard: Das Stammverzeichnis (/)

Erforderlich: Nein

`-P, --partition` type

Gibt an, ob das DatenträgerImage eine Partitionstabelle verwenden soll. Wenn Sie keinen Partitionstabellentyp angeben, wird standardmäßig der Typ festgelegt, der im übergeordneten Blockgerät des Volumes verwendet wird (sofern zutreffend), andernfalls ist der Standard `gpt`.

Zulässige Werte: `mbr` | `gpt` | `none`

Erforderlich: Nein

`-S, --script` script

Ein vor dem Bündeln auszuführendes Anpassungsskript. Das Skript muss ein einzelnes Argument, den Mountingpoint des Volumes, erwarten.

Erforderlich: Nein

`--fstab` path

Der Pfad zum fstab, das im Image gebündelt werden soll. Wenn das nicht festgelegt ist, bündelt Amazon EC2 /etc/fstab.

Erforderlich: Nein

`--generate-fstab`

Bündelt das Volume mit einem von Amazon EC2 bereitgestellten fstab.

Erforderlich: Nein

`--grub-config`

Der Pfad zu einer alternativen Grub-Konfigurationsdatei, die im Image gebündelt werden soll. Standardmäßig erwartet `ec2-bundle-vol`, dass entweder `/boot/grub/menu.lst` oder `/boot/grub/grub.conf` auf dem geklonten Image vorhanden ist. Mit dieser Option können Sie einen Pfad zu einer alternativen Grub-Konfigurationsdatei festlegen, der dann in die Standardeinstellungen (wenn vorhanden) kopiert wird.

Erforderlich: Nein

`--kernel` kernel_id

Veraltet. Verwenden Sie zum Festlegen des Kernels register-image.

Erforderlich: Nein

`--ramdisk`ramdisk_id

Veraltet. Verwenden Sie zum Festlegen des RAM-Datenträgers (sofern erforderlich) register-image.

Erforderlich: Nein

Output

Statusmeldung, die die Phasen und Status der Bündelung beschreibt

Beispiel

Dieses Beispiel erstellt eine gebündeltes AMI durch Komprimieren, Verschlüsseln und Signieren eines Snapshots des Stammdateisystems des lokalen Computers.

```
[ec2-user ~]$ ec2-bundle-vol -d /mnt -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c
 cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -r x86_64
  Copying / into the image file /mnt/image...
  Excluding:
       sys
       dev/shm
       proc
       dev/pts
       proc/sys/fs/binfmt_misc
       dev
       media
       mnt
       proc
       sys
       tmp/image
       mnt/img-mnt
  1+0 records in
  1+0 records out
  mke2fs 1.38 (30-Jun-2005)
  warning: 256 blocks unused.

  Splitting /mnt/image.gz.crypt...
  Created image.part.00
  Created image.part.01
  Created image.part.02
  Created image.part.03
  ...
  Created image.part.22
  Created image.part.23
  Generating digests for each part...
  Digests generated.
  Creating bundle manifest...
```

```
Bundle Volume complete.
```

ec2-delete-bundle

Beschreibung

Löscht das festgelegte Paket aus dem Amazon S3-Speicher. Wenn Sie ein Paket löschen, können Sie aus dem entsprechenden AMI keine Instances starten.

Syntax

ec2-delete-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* [-t *token*] [--url *url*] [--region *region*] [--sigv *version*] [-m *path*] [-p *prefix*] [--clear] [--retry] [-y]

Optionen

`-b, --bucket` bucket

Der Name des Amazon S3-Buckets, der das gebündelte AMI enthält, gefolgt von einem optionalen, durch "/" getrennten Pfadpräfix

Erforderlich: Ja

`-a, --access-key` access_key_id

Die AWS-Zugriffsschlüssel-ID

Erforderlich: Ja

`-s, --secret-key` secret_access_key

Der geheime AWS-Zugriffsschlüssel

Erforderlich: Ja

`-t, --delegation-token` token

Das Delegierungstoken, das an die AWS-Anforderung übergeben wird. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen im IAM-Benutzerhandbuch.

Erforderlich: Nur wenn Sie temporäre Sicherheitsanmeldeinformationen verwenden.

Standard: Der Wert der AWS_DELEGATION_TOKEN-Umgebungsvariablen (wenn festgelegt)

--regionregion

Die in der Anforderungssignatur zu verwendende Region.

Standard: us-east-1

Erforderlich: Ist erforderlich, wenn Signaturversion 4 verwendet wird

--sigvVersion

Die beim Signieren der Anforderung zu verwendende Signaturversion

Zulässige Werte: 2 | 4

Standard: 4

Erforderlich: Nein

-m, --manifestpath

Der Pfad zur Manifestdatei

Erforderlich: Sie müssen --prefix oder --manifest angeben.

-p, --prefix prefix

Das gebündelte AMI-Dateinamenpräfix. Geben Sie das gesamte Präfix an. Verwenden Sie beim Präfix "image.img" beispielsweise -p image.img und nicht -p image.

Erforderlich: Sie müssen --prefix oder --manifest angeben.

--clear

Löscht nach dem Löschen des angegebenen Pakets den Amazon S3-Bucket, wenn er leer ist.

Erforderlich: Nein

--retry

Versucht bei allen Amazon S3-Fehlern den Vorgang automatisch erneut, bis zu fünfmal pro Vorgang.

Erforderlich: Nein

`-y, --yes`

Es wird automatisch davon ausgegangen, dass die Antwort auf alle Eingabeaufforderungen "ja" ist.

Erforderlich: Nein

Output

Amazon EC2 zeigt Statusmeldungen an, die die Phasen und Status des Löschvorgangs angeben.

Beispiel

Dieses Beispiel löscht ein Paket aus Amazon S3.

```
[ec2-user ~]$ ec2-delete-bundle -b amzn-s3-demo-bucket -a your_access_key_id -
s your_secret_access_key
Deleting files:
amzn-s3-demo-bucket/image.manifest.xml
amzn-s3-demo-bucket/image.part.00
amzn-s3-demo-bucket/image.part.01
amzn-s3-demo-bucket/image.part.02
amzn-s3-demo-bucket/image.part.03
amzn-s3-demo-bucket/image.part.04
amzn-s3-demo-bucket/image.part.05
amzn-s3-demo-bucket/image.part.06
Continue? [y/n]
y
Deleted amzn-s3-demo-bucket/image.manifest.xml
Deleted amzn-s3-demo-bucket/image.part.00
Deleted amzn-s3-demo-bucket/image.part.01
Deleted amzn-s3-demo-bucket/image.part.02
Deleted amzn-s3-demo-bucket/image.part.03
Deleted amzn-s3-demo-bucket/image.part.04
Deleted amzn-s3-demo-bucket/image.part.05
Deleted amzn-s3-demo-bucket/image.part.06
ec2-delete-bundle complete.
```

ec2-download-bundle

Beschreibung

Lädt die angegebenen Amazon-S3-gestützten Linux-AMIs vom Amazon-S3-Speicher herunter.

Syntax

ec2-download-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* -k *path* [--url *url*] [--region *region*] [--sigv *version*] [-m *file*] [-p *prefix*] [-d *directory*] [--retry]

Optionen

`-b, --bucket` bucket

Der Name des Amazon S3-Buckets, in dem sich das Paket befindet, gefolgt von einem optionalen, durch "/" getrennten Pfadpräfix

Erforderlich: Ja

`-a, --access-key` access_key_id

Die AWS-Zugriffsschlüssel-ID

Erforderlich: Ja

`-s, --secret-key` secret_access_key

Der geheime AWS-Zugriffsschlüssel

Erforderlich: Ja

`-k, --privatekey` path

Der private Schlüssel, der zum Entschlüsseln des Manifests verwendet wird

Erforderlich: Ja

`--url` url

Die Amazon S3-Service-URL

Standard: `https://s3.amazonaws.com/`

Erforderlich: Nein

`--region` region

Die in der Anforderungssignatur zu verwendende Region.

Standard: `us-east-1`

Erforderlich: Ist erforderlich, wenn Signaturversion 4 verwendet wird

`--sigv` version

Die beim Signieren der Anforderung zu verwendende Signaturversion

Zulässige Werte: `2` | `4`

Standard: `4`

Erforderlich: Nein

`-m, --manifest` file

Der Name der Manifestdatei (ohne den Pfad). Wir empfehlen Ihnen, dass Sie entweder das Manifest (`-m`) oder ein Präfix (`-p`) angeben.

Erforderlich: Nein

`-p, --prefix` prefix

Das Dateinamenpräfix für gebündelte AMI-Dateien

Standard: `image`

Erforderlich: Nein

`-d, --directory` directory

Das Verzeichnis, in dem das heruntergeladene Paket gespeichert wird. Das Verzeichnis muss vorhanden sein.

Standard: Das aktuelle Arbeitsverzeichnis

Erforderlich: Nein

`--retry`

Versucht bei allen Amazon S3-Fehlern den Vorgang automatisch erneut, bis zu fünfmal pro Vorgang.

Erforderlich: Nein

Output

Statusmeldungen werden angezeigt, die die unterschiedlichen Phasen und Status des Download-Vorgangs angeben.

Beispiel

Dieses Beispiel erstellt das `bundled`-Verzeichnis (mithilfe des Linux-Befehls mkdir) und lädt das Paket vom Amazon S3-Bucket `amzn-s3-demo-bucket` herunter.

```
[ec2-user ~]$ mkdir bundled
[ec2-user ~]$ ec2-download-bundle -b amzn-s3-demo-bucket/bundles/bundle_name
 -m image.manifest.xml -a your_access_key_id -s your_secret_access_key -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d mybundle
Downloading manifest image.manifest.xml from amzn-s3-demo-bucket to mybundle/
image.manifest.xml ...
Downloading part image.part.00 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.00 ...
Downloaded image.part.00 from amzn-s3-demo-bucket
Downloading part image.part.01 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.01 ...
Downloaded image.part.01 from amzn-s3-demo-bucket
Downloading part image.part.02 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.02 ...
Downloaded image.part.02 from amzn-s3-demo-bucket
Downloading part image.part.03 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.03 ...
Downloaded image.part.03 from amzn-s3-demo-bucket
Downloading part image.part.04 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.04 ...
Downloaded image.part.04 from amzn-s3-demo-bucket
Downloading part image.part.05 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.05 ...
Downloaded image.part.05 from amzn-s3-demo-bucket
Downloading part image.part.06 from amzn-s3-demo-bucket/bundles/bundle_name to
 mybundle/image.part.06 ...
Downloaded image.part.06 from amzn-s3-demo-bucket
```

ec2-migrate-manifest

Beschreibung

Verändert ein Amazon-S3-gestütztes Linux-AMI (z. B. das Zertifikat, den Kernel und den RAM-Datenträger) so, dass es eine andere Region unterstützt.

Syntax

```
ec2-migrate-manifest -c path -k path -m path {(-a access_key_id -
s secret_access_key --region region) | (--no-mapping)} [--ec2cert
ec2_cert_path] [--kernel kernel-id] [--ramdisk ramdisk_id]
```

Optionen

`-c, --cert` path

Die PEM-kodierte öffentliche RSA-Schlüsselzertifikatsdatei des Benutzers

Erforderlich: Ja

`-k, --privatekey` path

Der Pfad zur PEM-kodierten RSA-Schlüsseldatei des Benutzers

Erforderlich: Ja

`--manifest` path

Der Pfad zur Manifestdatei

Erforderlich: Ja

`-a, --access-key` access_key_id

Die AWS-Zugriffsschlüssel-ID

Erforderlich: Ist erforderlich, wenn das automatische Mapping verwendet wird.

`-s, --secret-key` secret_access_key

Der geheime AWS-Zugriffsschlüssel

Erforderlich: Ist erforderlich, wenn das automatische Mapping verwendet wird.

`--region` region

Die in der Mapping-Datei zu suchende Region

Erforderlich: Ist erforderlich, wenn das automatische Mapping verwendet wird.

`--no-mapping`

Deaktiviert das automatische Mapping von Kernels und RAM-Datenträgern.

Während der Migration ersetzt Amazon EC2 den Kernel und den RAM-Datenträger in der Manifestdatei durch einen Kernel und einen RAM-Datenträger, die für die Zielregion erstellt wurden. Sofern der Parameter `--no-mapping` nicht angeben wurde, verwendet `ec2-migrate-bundle` unter Umständen die Vorgänge `DescribeRegions` und `DescribeImages` für automatisierte Zuweisungen.

Erforderlich: Ist erforderlich, wenn Sie die Optionen `-a`, `-s` und `--region` nicht angeben, die für das automatische Mapping verwendet werden.

`--ec2cert` path

Der Pfad zum öffentlichen Amazon EC2 X.509-Schlüsselzertifikat, das zum Verschlüsseln des Image-Manifests verwendet wird.

Die Regionen `us-gov-west-1` und `cn-north-1` verwenden ein nicht standardmäßiges öffentliches Schlüsselzertifikat, und der Pfad zu diesem Zertifikat muss mit dieser Option angegeben werden. Der Pfad zum Zertifikat variiert ausgehend von der Installationsmethode der AMI-Tools. Für Amazon Linux befinden sich die Zertifikate unter `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Wenn Sie die AMI-Tools aus der ZIP-Datei in Die Amazon-EC2-AMI-Tools einrichten installiert haben, befinden sich die Zertifikate unter `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Erforderlich: Nur für die Regionen `us-gov-west-1` und `cn-north-1`.

`--kernel` kernel_id

Die ID des Kernels, der ausgewählt werden soll

> **Important**
>
> Wir empfehlen Ihnen die Verwendung von PV-GRUB anstelle von Kernels und RAM-Datenträgern. Weitere Informationen finden Sie unter Vom Benutzer bereitgestellte Kernel im Benutzerhandbuch für Amazon Linux 2.

Erforderlich: Nein

`--ramdisk` ramdisk_id

Die ID des RAM-Datenträgers, der ausgewählt werden soll

> **Important**
>
> Wir empfehlen Ihnen die Verwendung von PV-GRUB anstelle von Kernels und RAM-Datenträgern. Weitere Informationen finden Sie unter Vom Benutzer bereitgestellte Kernel im Benutzerhandbuch für Amazon Linux 2.

Erforderlich: Nein

Output

Statusmeldung, die die Phasen und Status des Bündelungsprozesses beschreibt

Beispiel

Dieses Beispiel kopiert das im `my-ami.manifest.xml`-Manifest angegebene AMI aus den USA in die EU.

```
[ec2-user ~]$ ec2-migrate-manifest --manifest my-ami.manifest.xml
 --cert cert-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --privatekey pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --region eu-west-1

Backing up manifest...
Successfully migrated my-ami.manifest.xml It is now suitable for use in eu-west-1.
```

ec2-unbundle

Beschreibung

Erstellt das Paket neu aus einem Amazon-S3-gestützten AMI für Linux.

Syntax

ec2-unbundle -k *path* -m *path* [-s *source_directory*] [-d *destination_directory*]

Optionen

`-k, --privatekey` path

Der Pfad zu Ihrer PEM-kodierten RSA-Schlüsseldatei

Erforderlich: Ja

`-m, --manifest` path

Der Pfad zur Manifestdatei

Erforderlich: Ja

`-s, --source` source_directory

Das Verzeichnis, das das Paket enthält

Standard: Das aktuelle Verzeichnis

Erforderlich: Nein

`-d, --destination` destination_directory

Das Verzeichnis, in dem das AMI entpackt wird. Das Zielverzeichnis muss vorhanden sein.

Standard: Das aktuelle Verzeichnis

Erforderlich: Nein

Beispiel

Dieses Linux- und UNIX-Beispiel entpackt das AMI, das in der `image.manifest.xml`-Datei angegeben ist.

```
[ec2-user ~]$ mkdir unbundled
$ ec2-unbundle -m mybundle/image.manifest.xml -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -s mybundle -d unbundled
$ ls -l unbundled
total 1025008
-rw-r--r-- 1 root root 1048578048 Aug 25 23:46 image.img
```

Output

Statusmeldungen werden angezeigt, die die unterschiedlichen Phasen und Status des Entpackvorgangs angeben.

ec2-upload-bundle

Beschreibung

Lädt das Paket für ein Amazon-S3-gestütztes Linux-AMI in Amazon S3 hoch und legt die entsprechenden Zugriffssteuerungslisten (ACLs) für die hochgeladenen Objekte fest. Weitere Informationen finden Sie unter Ein Amazon-S3-gestütztes AMI erstellen.

> **Note**
>
> Um Objekte für Ihr Amazon-S3-gestütztes Linux-AMI in einen S3-Bucket hochzuladen, müssen ACLs für den Bucket aktiviert sein. Andernfalls kann Amazon EC2 keine ACLs für die hochzuladenden Objekte festlegen. Wenn Ihr Ziel-Bucket die erzwungene Einstellung für den Bucket-Eigentümer für S3 Object Ownership verwendet, funktioniert dies nicht, da ACLs deaktiviert sind. Weitere Informationen finden Sie unter Steuern des Eigentums an Objekten und Deaktivieren von ACLs für Ihren Bucket.

Syntax

```
ec2-upload-bundle -b bucket -a access_key_id -s secret_access_key [-t
token] -m path [--url url] [--region region] [--sigv version] [--acl acl]
[-d directory] [--part part] [--retry] [--skipmanifest]
```

Optionen

`-b, --bucket` bucket

Der Name des Amazon S3-Buckets, in dem das Paket gespeichert werden soll, gefolgt von einem optionalen durch "/" getrennten Pfadpräfix. Wenn der Bucket nicht vorhanden ist, wird er erstellt, sofern der Bucket-Name verfügbar ist. Wenn der Bucket nicht vorhanden ist und die Version der AMI-Tools 1.5.18 oder höher ist, legt dieser Befehl außerdem die ACLs für den Bucket fest.

Erforderlich: Ja

`-a, --access-key` access_key_id

Ihre AWS-Zugriffsschlüssel-ID

Erforderlich: Ja

`-s, --secret-key` secret_access_key

Ihr geheimer AWS-Zugriffsschlüssel

Erforderlich: Ja

`-t, --delegation-token` token

Das Delegierungstoken, das an die AWS-Anforderung übergeben wird. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen im IAM-Benutzerhandbuch.

Erforderlich: Nur wenn Sie temporäre Sicherheitsanmeldeinformationen verwenden.

Standard: Der Wert der `AWS_DELEGATION_TOKEN`-Umgebungsvariablen (wenn festgelegt)

`-m, --manifest` path

Der Pfad zur Manifestdatei Die Manifestdatei wird während des Bündelungsvorgangs erstellt. Sie finden sie in dem Verzeichnis, das das Paket enthält.

Erforderlich: Ja

`--url` url

Veraltet. Verwenden Sie die Option `--region`, wenn Ihr Bucket nicht auf den Standort `EU` (nicht `eu-west-1`) beschränkt ist. Das Flag `--location` ist die einzige Möglichkeit, um auf diese spezifische Standortbeschränkung einzugehen.

Die Amazon S3-Endpunkt-Service-URL

Standard: `https://s3.amazonaws.com/`

Erforderlich: Nein

`--region` region

Die Region, die in der Anforderungssignatur für den S3-Ziel-Bucket verwendet werden soll

- Wenn der Bucket nicht vorhanden ist und Sie keine Region angeben, erstellt das Tool den Bucket ohne eine Standortbeschränkung (in `us-east-1`).
- Wenn der Bucket nicht vorhanden ist und Sie eine Region angeben, erstellt das Tool den Bucket in der angegebenen Region.
- Wenn der Bucket vorhanden ist und Sie keine Region angeben, verwendet das Tool den Standort des Buckets.

- Wenn der Bucket vorhanden ist und Sie `us-east-1` als Region angeben, verwendet das Tool den tatsächlichen Standort des Buckets, ohne eine Fehlermeldung auszugeben, und vorhandene übereinstimmende Dateien werden überschrieben.
- Wenn der Bucket vorhanden ist und Sie eine Region angeben, die nicht `us-east-1` ist und nicht mit dem tatsächlichen Standort des Buckets übereinstimmt, wird das Tool mit einem Fehler beendet.

Wenn Ihr Bucket auf den Standort `EU` (nicht `eu-west-1`) beschränkt ist, verwenden Sie das Flag `--location`. Das Flag `--location` ist die einzige Möglichkeit, um auf diese spezifische Standortbeschränkung einzugehen.

Standard: `us-east-1`

Erforderlich: Ist erforderlich, wenn Signaturversion 4 verwendet wird

`--sigv` version

Die beim Signieren der Anforderung zu verwendende Signaturversion

Zulässige Werte: `2` | `4`

Standard: `4`

Erforderlich: Nein

`--acl` acl

Die Richtlinie für die Access Control List des gebündelten Images

Zulässige Werte: `public-read` | `aws-exec-read`

Standard: `aws-exec-read`

Erforderlich: Nein

`-d, --directory` directory

Das Verzeichnis, das die gebündelten AMI-Teile enthält

Standard: Das Verzeichnis, das die Manifestdatei enthält (siehe die Option `-m`)

Erforderlich: Nein

`--part` part

Beginnt mit dem Hochladen des angegebenen Teils und aller folgenden Teile. Beispiel, `--part 04`.

Erforderlich: Nein

`--retry`

Versucht bei allen Amazon S3-Fehlern den Vorgang automatisch erneut, bis zu fünfmal pro Vorgang.

Erforderlich: Nein

`--skipmanifest`

Lädt das Manifest nicht hoch.

Erforderlich: Nein

`--location` location

Veraltet. Verwenden Sie die Option `--region`, wenn Ihr Bucket nicht auf den Standort EU (nicht `eu-west-1`) beschränkt ist. Das Flag `--location` ist die einzige Möglichkeit, um auf diese spezifische Standortbeschränkung einzugehen.

Die Standortbeschränkung des Amazon S3-Ziel-Buckets. Wenn der Bucket vorhanden ist und Sie einen Standort angegeben haben, der nicht mit dem tatsächlichen Standort des Buckets übereinstimmt, wird das Tool mit einem Fehler beendet. Wenn der Bucket vorhanden ist und Sie keinen Standort angeben, verwendet das Tool den Standort des Buckets. Wenn der Bucket nicht vorhanden ist und Sie einen Standort angeben, erstellt das Tool den Bucket am angegebenen Standort. Wenn der Bucket nicht vorhanden ist und Sie keinen Standort angeben, erstellt das Tool den Bucket ohne eine Standortbeschränkung (in `us-east-1`).

Standard: Wenn `--region` angegeben ist, wird der Standort auf die angegebene Region festgelegt. Wenn `--region` nicht angegeben ist, ist der Standort standardmäßig `us-east-1`.

Erforderlich: Nein

Output

Amazon EC2 zeigt Statusmeldungen an, die die Phasen und Status des Upload-Vorgangs angeben.

Beispiel

Dieses Beispiel lädt das Paket hoch, das vom `image.manifest.xml`-Manifest festgelegt wurde.

```
[ec2-user ~]$ ec2-upload-bundle -b amzn-s3-demo-bucket/bundles/bundle_name -m
 image.manifest.xml -a your_access_key_id -s your_secret_access_key
Creating bucket...
Uploading bundled image parts to the S3 bucket amzn-s3-demo-bucket ...
Uploaded image.part.00
Uploaded image.part.01
Uploaded image.part.02
Uploaded image.part.03
Uploaded image.part.04
Uploaded image.part.05
Uploaded image.part.06
Uploaded image.part.07
Uploaded image.part.08
Uploaded image.part.09
Uploaded image.part.10
Uploaded image.part.11
Uploaded image.part.12
Uploaded image.part.13
Uploaded image.part.14
Uploading manifest ...
Uploaded manifest.
Bundle upload completed.
```

Allgemeine Optionen für AMI-Tools

Die meisten AMI-Tools akzeptieren die folgenden optionalen Parameter.

`--help, -h`

Zeigt die Hilfenachricht an.

`--version`

Zeigt die Version und das Copyright an.

`--manual`

Zeigt die manuelle Eingabe an.

`--batch`

Wird im Stapelmodus ausgeführt und unterdrückt interaktive Eingabeaufforderungen.

`--debug`

Zeigt Informationen an, die bei der Problembehebung hilfreich sind.

Konvertieren Sie Ihre Amazon-S3-gestütztes AMI in ein Amazon EBS-gestütztes AMI

Sie können ein Amazon-S3-gestütztes Linux-AMI, dessen Eigentümer Sie sind, in ein Amazon-EBS-gestütztes Linux-AMI konvertieren.

> **Important**
>
> Sie können kein AMI konvertieren, das Ihnen nicht gehört.

So konvertieren Sie ein Amazon-S3-gestütztes AMI in ein Amazon-EBS-gestütztes AMI

1. Starten Sie eine Amazon Linux-Instance über ein Amazon EBS-gestütztes AMI. Weitere Informationen finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten. Amazon Linux-Instances haben die AWS CLI- und AMI-Tools vorinstalliert.
2. Laden Sie den privaten X.509-Schlüssel, den Sie zum Bündeln Ihres Amazon-S3-gestützten AMI verwendet haben, auf Ihre Instance hoch. Wir verwenden diesen Schlüssel, um sicherzustellen, dass nur Sie und Amazon EC2 Zugriff auf Ihr AMI haben.

   a. Erstellen Sie auf Ihrer Instance wie folgt ein temporäres Verzeichnis für Ihren privaten X.509-Schlüssel:

   ```
   [ec2-user ~]$ mkdir /tmp/cert
   ```

   b. Kopieren Sie Ihren privaten X.509-Schlüssel von Ihrem Computer in das Verzeichnis `/tmp/cert` auf Ihrer Instance, indem Sie ein Secure Copy-Tool nutzen, z. B. scp. Der Parameter *`my-private-key`* im folgenden Befehl ist der private Schlüssel, den Sie zum Herstellen der Verbindung für Ihre Instance mit SSH verwenden. Zum Beispiel:

   ```
   you@your_computer:~ $ scp -i my-private-key.pem /
   path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
   user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
   pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
   ```

3. Konfigurieren Sie Ihre Umgebungsvariablen für die Verwendung der AWS CLI. Weitere Informationen finden Sie unter Umgebungsvariablen.

   a. (Empfohlen) Legen Sie Umgebungsvariablen für Ihren AWS-Zugriffsschlüssel, Ihren geheimen Schlüssel und Ihr Sitzungstoken fest.

   ```
   [ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
   [ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
   [ec2-user ~]$ export AWS_SESSION_TOKEN=your_session_token
   ```

   b. Legen Sie Umgebungsvariablen für Ihren AWS-Zugriffsschlüssel und geheimen Schlüssel fest.

   ```
   [ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
   [ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
   ```

4. Bereiten Sie ein Volume Amazon Elastic Block Store (Amazon EBS) für Ihr neues AMI vor.

   a. Erstellen Sie ein leeres EBS-Volume in derselben Availability Zone wie für Ihre Instance, indem Sie den Befehl create-volume verwenden. Notieren Sie sich die Volume-ID in der Befehlsausgabe.

   > **Important**
   >
   > Dieses EBS-Volume muss mindestens die gleiche Größe wie das ursprüngliche Stamm-Volume des Instance-Speichers haben.

   ```
   aws ec2 create-volume \
       --size 10 \
       --region us-west-2 \
       --availability-zone us-west-2b
   ```

   b. Fügen Sie das Volume mit dem Befehl attach-volume an Ihre Amazon EBS-gestützte Instance an.

   ```
   aws ec2 attach-volume \
       --volume-id vol-01234567890abcdef \
       --instance-id i-1234567890abcdef0 \
       --region us-west-2
   ```

5. Erstellen Sie einen Ordner für Ihr Paket.

```
[ec2-user ~]$ mkdir /tmp/bundle
```

6. Laden Sie das Paket für Ihr Instance Store-Backed AMI in das Verzeichnis `/tmp/bundle` herunter, indem Sie den Befehl ec2-download-bundle verwenden.

```
[ec2-user ~]$ ec2-download-bundle -b amzn-s3-demo-bucket/bundle_folder/bundle_name
 -m image.manifest.xml -a $AWS_ACCESS_KEY_ID -s $AWS_SECRET_ACCESS_KEY --
privatekey /path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d /tmp/bundle
```

7. Stellen Sie die Image-Datei mit dem Befehl ec2-unbundle aus dem Paket wieder her.

   a. Wechseln Sie in den Paketordner (bundle).

   ```
   [ec2-user ~]$ cd /tmp/bundle/
   ```

   b. Führen Sie den Befehl ec2-unbundle aus.

   ```
   [ec2-user bundle]$ ec2-unbundle -m image.manifest.xml --privatekey /path/to/pk-
   HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem
   ```

8. Kopieren Sie die Dateien aus dem entpackten Image auf das neue EBS-Volume.

```
[ec2-user bundle]$ sudo dd if=/tmp/bundle/image of=/dev/sdb bs=1M
```

9. Überprüfen Sie das Volume auf neue Partitionen, die aus dem Paket entpackt wurden.

```
[ec2-user bundle]$ sudo partprobe /dev/sdb1
```

10. Listen Sie die Blockgeräte auf, um den Gerätenamen für das Mounten ermitteln zu können.

```
[ec2-user bundle]$ lsblk
NAME         MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
/dev/sda    202:0    0   8G  0 disk
##/dev/sda1 202:1    0   8G  0 part /
/dev/sdb    202:80   0  10G  0 disk
##/dev/sdb1 202:81   0  10G  0 part
```

In diesem Beispiel lautet die Partition für das Mounten `/dev/sdb1`, aber Ihr Gerätename lautet wahrscheinlich anders. Falls Ihr Volume nicht partitioniert ist, lautet das Gerät für das Mounten etwa `/dev/sdb` (ohne nachgestellte Ziffer für die Gerätepartition).

11. Erstellen Sie einen Mounting-Punkt für das neue EBS-Volume und mounten Sie das Volume.

```
[ec2-user bundle]$ sudo mkdir /mnt/ebs
[ec2-user bundle]$ sudo mount /dev/sdb1 /mnt/ebs
```

12. Öffnen Sie die Datei `/etc/fstab` auf dem EBS-Volume mit Ihrem bevorzugten Text-Editor (z. B. vim oder nano) und entfernen Sie alle Einträge für Instance-Speicher-Volumes (flüchtiger Speicher). Da das EBS-Volume unter `/mnt/ebs` gemountet wurde, befindet sich die Datei `fstab` unter `/mnt/ebs/etc/fstab`.

```
[ec2-user bundle]$ sudo nano /mnt/ebs/etc/fstab
#
LABEL=/     /           ext4    defaults,noatime  1   1
tmpfs       /dev/shm    tmpfs   defaults        0   0
devpts      /dev/pts    devpts  gid=5,mode=620  0   0
sysfs       /sys        sysfs   defaults        0   0
proc        /proc       proc    defaults        0   0
/dev/sdb        /media/ephemeral0       auto    defaults,comment=cloudconfig    0
     2
```

In diesem Beispiel sollte die letzte Zeile entfernt werden.

13. Heben Sie das Mounting des Volumes auf und trennen Sie es von der Instance.

```
[ec2-user bundle]$ sudo umount /mnt/ebs
[ec2-user bundle]$ aws ec2 detach-volume --volume-id vol-01234567890abcdef --
region us-west-2
```

14. Erstellen Sie aus dem neuen EBS-Volume wie folgt ein AMI.

    a. Erstellen Sie einen Snapshot des neuen EBS-Volumes.

```
[ec2-user bundle]$ aws ec2 create-snapshot --region us-west-2 --description
 "your_snapshot_description" --volume-id vol-01234567890abcdef
```

    b. Überprüfen Sie, ob Ihr Snapshot vollständig ist.

```
[ec2-user bundle]$ aws ec2 describe-snapshots --region us-west-2 --snapshot-
id snap-0abcdef1234567890
```

c. Ermitteln Sie die auf dem ursprünglichen AMI verwendete Prozessorarchitektur, den Virtualisierungstyp und das Kernel-Image (`aki`) mit dem Befehl describe-images. Für diesen Schritt benötigen Sie die AMI-ID des ursprünglichen Amazon-S3-gestützten AMI.

```
[ec2-user bundle]$ aws ec2 describe-images --region us-west-2 --image-
id ami-0abcdef1234567890 --output text
IMAGES x86_64 amazon/amzn-ami-pv-2013.09.2.x86_64-s3 ami-8ef297be amazon
 available public machine aki-fc8f11cc instance-store paravirtual xen
```

In diesem Beispiel werden als Architektur `x86_64` und als Kernel-Image-ID `aki-fc8f11cc` verwendet. Nutzen Sie diese Werte im folgenden Schritt. Falls in der Ausgabe des obigen Befehls auch eine `ari`-ID aufgeführt ist, sollten Sie sich diese ebenfalls notieren.

d. Registrieren Sie Ihr neues AMI mit der Snapshot-ID Ihres neuen EBS-Volumes und den Werten aus dem vorherigen Schritt. Wenn in der Ausgabe des vorherigen Befehls eine `ari`-ID aufgeführt ist, sollten Sie diese im folgenden Befehl als `--ramdisk-id` *`ari_id`* einfügen.

```
[ec2-user bundle]$ aws ec2 register-image --region us-west-2 --
name your_new_ami_name --block-device-mappings DeviceName=device-
name,Ebs={SnapshotId=snap-0abcdef1234567890} --virtualization-type paravirtual
 --architecture x86_64 --kernel-id aki-fc8f11cc --root-device-name device-name
```

15. (Optional) Nachdem Sie per Test sichergestellt haben, dass Sie über Ihr neues AMI eine Instance starten können, können Sie das für dieses Verfahren erstellte EBS-Volume löschen.

```
aws ec2 delete-volume --volume-id vol-01234567890abcdef
```

Ein Amazon-EC2-AMI mit Windows Sysprep erstellen

Das Microsoft System Preparation Tool (Windows Sysprep) erstellt eine generalisierte Version des Betriebssystems, wobei die instance-spezifische Systemkonfiguration entfernt wird, bevor ein neues Image erfasst wird.

Es wird empfohlen, EC2 Image Builder zu verwenden, um die Erstellung, Verwaltung und Bereitstellung benutzerdefinierter, sicherer und aktueller „goldener“ Server-Images zu automatisieren, die vorinstalliert und mit Software und Einstellungen vorkonfiguriert sind.

Sie können auch Windows Sysprep verwenden, um ein Standard-AMI mit den folgenden Windows-Start-Agents zu erstellen: EC2Launch v2, EC2Launch und EC2Config.

> **Important**
>
> Verwenden Sie Windows Sysprep nicht zum Erstellen eines Instance-Backups. Windows Sysprep entfernt systemspezifische Informationen. Das Entfernen dieser Informationen kann unbeabsichtigte Folgen für ein Instance-Backup haben.

Informationen zur Fehlerbehebung bei Windows Sysprep finden Sie unter Behebung von Sysprep-Problemen mit Amazon Windows-Instances EC2 .

Inhalt

- Sysprep-Phasen von Windows
- Bevor Sie beginnen
- Ein AMI mithilfe von Windows Sysprep mit EC2Launch v2 erstellen
- Ein AMI mithilfe von Windows Sysprep mit EC2Launch erstellen
- Ein AMI mithilfe von Windows Sysprep mit EC2Config erstellen

Sysprep-Phasen von Windows

Folgende Phasen werden beim Ausführen von Windows Sysprep durchlaufen:

- Generalisieren: Das Sysprep-Tool entfernt Image-spezifische Informationen und Konfigurationen. Zum Beispiel entfernt Windows Sysprep u. a. die Sicherheits-ID (SID), den Computer-Namen, die Ereignisprotokolle und bestimmte Treiber, um nur einige zu nennen. Anschließend kann vom Betriebssystem (OS) ein AMI erstellt werden.

> **Note**
>
> Wenn Sie Windows Sysprep mit den Windows-Start-Agenten ausführen, verhindert das System, dass Treiber entfernt werden, da `PersistAllDeviceInstalls` standardmäßig auf „wahr“ gesetzt ist.

- Spezialisieren: Plug & Play durchsucht den Computer und installiert Treiber für alle erkannten Geräte. Das Sysprep-Tool erstellt Betriebssystemanforderungen, z. B. Computer-Name und SID. Optional können Sie Befehle in dieser Phase ausführen.
- Out-of-Box Experience (OOBE): Das System führt ein verkürztes Windows Setup aus und fordert Sie zur Eingabe von Informationen wie Systemsprache, Zeitzone und einer registrierten Organisation auf. Wenn Sie Windows Sysprep mit Windows-Start-Agenten ausführen, automatisiert die Antwortdatei diese Phase.

Bevor Sie beginnen

- Sie sollten vor Ausführung von Windows Sysprep alle lokalen Benutzerkonten und alle Kontoprofile entfernen, abgesehen von einem einzigen Administratorkonto, mit dem Windows Sysprep ausgeführt wird. Wenn Sie Windows Sysprep mit zusätzlichen Konten und Profilen ausführen, könnte dies zu unerwarteten Verhalten führen, einschließlich des Verlusts von Profildaten oder des nicht erfolgreichen Abschlusses von Windows Sysprep.
- Erfahren Sie mehr unter Sysprep-Übersicht.
- Erfahren Sie, welche Serverrollen von Sysprep unterstützt werden.

Ein AMI mithilfe von Windows Sysprep mit EC2Launch v2 erstellen

Wenn Sie ein Image aus einer Instance erstellen, auf der der Agent EC2Launch v2 installiert ist, führt EC2Launch v2 während der Vorbereitung des Images bestimmte Aufgaben aus. Dies beinhaltet die Arbeit mit Windows Sysprep. Weitere Informationen finden Sie unter the section called “Sysprep-Phasen von Windows”.

Inhalt

- Windows-Sysprep-Aktionen
- Nach Sysprep
- Windows Sysprep mit EC2Launch v2 ausführen

Windows-Sysprep-Aktionen

Windows Sysprep und EC2Launch v2 führen beim Vorbereiten eines Image die folgenden Aktionen aus.

1. Wenn Sie im Dialogfeld EC2Launch-Einstellungen die Option Shutdown with Sysprep wählen, führt das System den Befehl `ec2launch sysprep` aus.
2. EC2Launch v2 bearbeitet den Inhalt der `unattend.xml`-Datei, indem der Registrierungswert unter `HKEY_USERS\.DEFAULT\Control Panel\International\LocaleName` gelesen wird. Die Datei befindet sich im folgenden Verzeichnis: `C:\ProgramData\Amazon\EC2Launch\sysprep`.
3. Das System führt das au `BeforeSysprep.cmd`. Dieser Befehl erstellt den folgenden Registrierungsschlüssel:

   reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 1 /f

   Der Registrierungsschlüssel deaktiviert RDP-Verbindungen bis sie erneut aktiviert werden. Die Deaktivierung von RDP-Verbindungen ist eine notwendige Sicherheitsmaßnahme, da während der ersten Boot-Session nach der Ausführung von Windows Sysprep kurzzeitig Verbindungen von RDP zugelassen werden und noch kein Administratorkennwort vergeben ist.
4. Der EC2Launch-v2-Service ruft Windows Sysprep mit dem folgenden Befehl auf:

   sysprep.exe /oobe /generalize /shutdown /unattend: "C:\ProgramData\Amazon\EC2Launch\sysprep\unattend.xml"

Generalisierungsphase

- EC2Launch v2 entfernt Image-spezifische Informationen und Konfigurationen, z. B. Computer-Name und SID. Wenn die Instance Mitglied einer Domain ist, wird sie von der Domain entfernt. Die `unattend.xml`-Antwortdatei enthält folgende Einstellungen, die sich auf diese Phase auswirken:
  - PersistAllDeviceInstalls: Die Einstellung verhindert, dass Windows Setup Geräte entfernt und neu konfiguriert. Dies beschleunigt die Image-Vorbereitung, da Amazon-AMIs bestimmte Treiber für die Ausführung erfordern und die erneute Erkennung der Treiber Zeit erfordern würde.
  - DoNotCleanUpNonPresentDevices: Die Einstellung hält Plug & Play-Informationen für Geräte zurück, die derzeit nicht vorhanden sind.

- Windows Sysprep beendet das Betriebssystem bei der Vorbereitung der Erstellung des AMI. Das System startet entweder eine neue Instance oder die ursprüngliche Instance.

Spezialisierungsphase

Das System erstellt OS-spezifische Anforderungen, z. B. Computer-Name und eine SID. Das System führt zudem die folgenden Aktionen basierend auf Konfigurationen durch, die Sie in der `unattend.xml`-Antwortdatei angeben.

- CopyProfile: Windows Sysprep kann zur Löschung aller Benutzerprofile konfiguriert werden, einschließlich des integrierten Administratorprofils. Die Einstellung behält das integrierte Administratorkonto bei, sodass alle an diesem Konto vorgenommenen Anpassungen auf das neue Image übertragen werden. Der Standardwert ist `True`.

  CopyProfile ersetzt das Standardprofil durch das vorhandene Profil des lokalen Administrators. Alle Konten, mit denen Sie sich nach der Ausführung von Windows Sysprep anmelden, erhalten bei der ersten Anmeldung eine Kopie dieses Profils und seiner Inhalte.

  Wenn es keine spezifischen Benutzerprofilanpassungen gibt, die Sie auf das neue Image übertragen möchten, legen Sie diese Einstellung auf fes `False`. Windows Sysprep entfernt alle Benutzerprofile. (Das spart Zeit und Festplattenspeicher).
- TimeZone: Die Zeitzone wird standardmäßig auf koordinierte Weltzeit (UTC) festgelegt.
- Synchronous command with order 1: Das System führt den folgenden Befehl zur Aktivierung des Administratorkontos und Angabe der Passwortanforderungen aus.

  ```
  net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER /
  PASSWORDREQ:YES
  ```
- Synchronous command with order 2: Das System verschlüsselt das Administratorpasswort. Die Sicherheitsmaßnahme dient dazu, den Zugriff auf die Instance nach Abschluss von Windows Sysprep zu verhindern, wenn Sie die `setAdminAccount`-Einstellung nicht aktiviert haben.

  Das System führt den folgenden Befehl von Ihrem lokalen Start-Agent-Verzeichnis aus (`C:\Program Files\Amazon\EC2Launch\`) aus.

  ```
  EC2Launch.exe internal randomize-password --username Administrator
  ```
- Um Remote-Desktop-Verbindungen zu aktivieren, setzt das System den Terminal-Server-Registrierungsschlüssel `fDenyTSConnections` auf „Falsch“.

OOBE-Phase

1. Das System gibt die folgenden Konfigurationen mithilfe der EC2Launch v2-Antwortdatei an:
   - `<InputLocale>en-US</InputLocale>`
   - `<SystemLocale>en-US</SystemLocale>`
   - `<UILanguage>en-US</UILanguage>`
   - `<UserLocale>en-US</UserLocale>`
   - `<HideEULAPage>true</HideEULAPage>`
   - `<HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>`
   - `<ProtectYourPC>3</ProtectYourPC>`
   - `<BluetoothTaskbarIconEnabled>false</BluetoothTaskbarIconEnabled>`
   - `<TimeZone>UTC</TimeZone>`
   - `<RegisteredOrganization>Amazon.com</RegisteredOrganization>`
   - `<RegisteredOwner>EC2</RegisteredOwner>`

   > **Note**
   >
   > Während der Verallgemeinerungs- und Spezialisierungsphasen überwacht EC2Launch v2 den Status des Betriebssystems. Wenn EC2Launch v2 erkennt, dass sich das OS in einer Sysprep-Phase befindet, schreibt es die folgende Mitteilung in das Systemprotokoll: Windows wird konfiguriert. SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. Das System führt EC2Launch v2 aus.

Nach Sysprep

Nach Abschluss von Sysprep sendet EC2Launch v2 die folgende Meldung an die Konsolenausgabe:

```
Windows sysprep configuration complete.
```

EC2Launch v2 führt anschließend die folgenden Aktionen aus:

1. Liest den Inhalt der `agent-config.yml`-Datei und führt konfigurierte Aufgaben aus.
2. Führt alle Aufgaben in der `preReady`-Phase aus.
3. Danach sendet es die Nachricht `Windows is ready` an die Systemprotokolle der Instance.

4. Führt alle Aufgaben in der `PostReady`-Phase aus.

Weitere Informationen zu EC2Launch v2 finden Sie unter Den EC2Launch-v2-Agenten verwenden, um Aufgaben während des Starts einer EC2-Windows-Instance auszuführen.

Windows Sysprep mit EC2Launch v2 ausführen

Gehen Sie wie folgt vor, um ein standardisiertes AMI mit Windows Sysprep mit EC2Launch v2 zu erstellen.

1. Suchen Sie in der Amazon-EC2-Konsole ein AMI, dass Sie kopieren wollen.
2. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
3. Einstellungen anpassen
    a. Suchen Sie im Start-Menü von Windows nach Amazon EC2Launch Settings (Amazon EC2Launch-Einstellungen) und wählen Sie diese aus. Weitere Informationen zu den Optionen und Einstellungen im Dialogfeld Amazon EC2Launch Settings (Amazon EC2Launch-Einstellungen) finden Sie unter EC2Launch-v2-Einstellungen für Windows-Instances konfigurieren.
    b. Wenn Sie Änderungen vorgenommen haben, wählen Sie Speichern vor dem Herunterfahren.
4. Wählen Sie Herunterfahren mit Sysprep oder Herunterfahren ohne Sysprep aus.

Wenn Sie zum Bestätigen der Ausführung von Windows Sysprep und zum Beenden der Instance aufgefordert werden, klicken Sie auf Ja. EC2Launch v2 führt Windows Sysprep aus. Sie werden dann von der Instance abgemeldet und die Instance wird beendet. Auf der Seite Instances in der Amazon EC2-Konsole wechselt der Instance-Status von `Running` zu `Stopping` und zu `Stopped`. Jetzt kann ein AMI aus dieser Instance erstellt werden.

Sie können das Windows-Sysprep-Tool manuell mittels Befehlszeile und dem folgenden Befehl aufrufen:

```
"%programfiles%\amazon\ec2launch\ec2launch.exe" sysprep --shutdown=true
```

Ein AMI mithilfe von Windows Sysprep mit EC2Launch erstellen

Wenn Sie ein Image aus einer Instance erstellen, auf der der Agent EC2Launch installiert ist, führt EC2Launch während der Vorbereitung des Images bestimmte Aufgaben aus. Dies beinhaltet die

Arbeit mit Windows Sysprep. Weitere Informationen finden Sie unter the section called “Sysprep-Phasen von Windows”.

EC2Launch bietet eine standardmäßige Antwortdatei und Batch-Dateien für Windows Sysprep, mit denen die Image-Vorbereitung auf Ihrem AMI automatisiert und gesichert wird. Das Ändern dieser Dateien ist optional. Sie befinden sich standardmäßig in folgendem Verzeichnis: `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.

> **Important**
>
> Verwenden Sie Windows Sysprep nicht zum Erstellen eines Instance-Backups. Windows Sysprep entfernt systemspezifische Informationen. Wenn Sie diese Informationen entfernen, könnte dies bei einer Instance-Sicherung unbeabsichtigte Folgen haben.

Inhalt

- EC2Launch-Antwort- und -Batchdateien für Windows Sysprep
- Windows Sysprep mit EC2Launch ausführen
- Aktualisieren von Metadaten/KMS-Routen für Server 2016 und höher beim Starten eines benutzerdefinierten AMI

EC2Launch-Antwort- und -Batchdateien für Windows Sysprep

Die EC2Launch-Antwortdatei und die Batch-Dateien für Windows Sysprep enthalten Folgendes:

`Unattend.xml`

Dies ist die standardmäßige Antwortdatei. Wenn Sie `SysprepInstance.ps1` ausführen oder auf der Benutzeroberfläche auf ShutdownWithSysprep klicken, liest das System die Einstellung aus dieser Datei.

`BeforeSysprep.cmd`

Passen Sie diese Batch-Datei so an, dass Befehle ausgeführt werden, bevor EC2Launch Windows Sysprep ausführt.

`SysprepSpecialize.cmd`

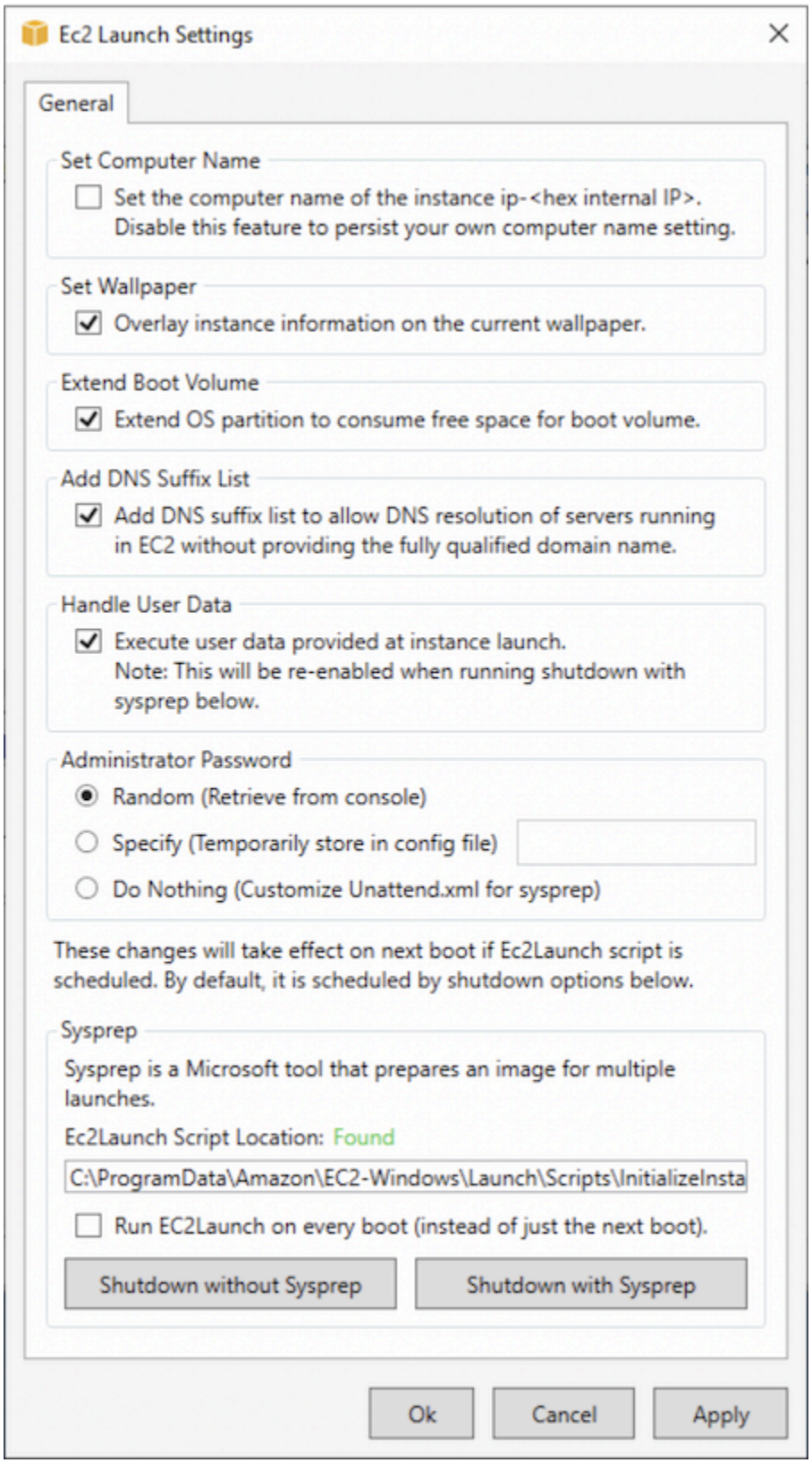
Passen Sie diese Batch-Datei so an, dass Befehle während der Windows-Sysprep-Spezialisierungsphase ausführt werden.

Windows Sysprep mit EC2Launch ausführen

Bei der vollständigen Installation von Windows Server 2016 und höher (mit Desktoperfahrung) können Sie Windows Sysprep manuell mit EC2Launch oder mit der Anwendung der EC2-Starteinstellungen ausführen.

So führen Sie Windows Sysprep mit der Anwendung für EC2Launch-Einstellungen aus

1. Suchen oder erstellen Sie in der Amazon EC2-Konsole ein AMI mit Windows Server 2016 oder höher.
2. Starten Sie über das AMI eine Windows-Instance.
3. Stellen Sie eine Verbindung mit Ihrer Windows-Instance her, und passen Sie sie an.
4. Suchen Sie die Anwendung EC2LaunchSettings, und führen Sie sie aus. Standardmäßig befindet sie sich in folgendem Verzeichnis: `C:\ProgramData\Amazon\EC2-Windows\Launch\Settings`.



5. Wählen oder löschen Sie die Optionen nach Bedarf. Diese Einstellungen werden in der Datei `LaunchConfig.json` gespeichert.

6. Gehen Sie für Administrator Password wie folgt vor:

   - Wählen Sie Random. EC2Launch generiert ein Passwort und verschlüsselt es mit dem Schlüssel des Benutzers: Die Einstellung wird vom System nach dem Start der Instance deaktiviert, so dass das Passwort weiterhin gilt, wenn die Instance neu gestartet bzw. angehalten und gestartet wird.
   - Wählen Sie Specify, und geben Sie ein Passwort ein, das den Systemanforderungen entspricht. Das Passwort wird in `LaunchConfig.json` im Klartext gespeichert und gelöscht, wenn Windows Sysprep das Administratorpasswort einstellt. Wenn Sie den Service gleich beenden, wird das Passwort sofort festgelegt. EC2Launch verschlüsselt das Passwort mit dem Schlüssel des Benutzers.
   - Wählen Sie DoNothing und geben Sie ein Kennwort in der `unattend.xml`-Datei an. Wenn Sie in der Datei `unattend.xml` kein Passwort angeben, ist das Administratorkonto deaktiviert.

7. Wählen Sie Shutdown with Sysprep (Herunterfahren mit Sysprep).

So führen Sie Windows Sysprep manuell mit EC2Launch aus

1. Finden oder erstellen Sie in der Amazon EC2-Konsole ein AMI der Datacenter-Edition von Windows Server 2016 oder höher, das Sie duplizieren wollen.
2. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
3. Passen Sie die Instance an.
4. Geben Sie Einstellungen in der Datei `LaunchConfig.json` an. Diese Datei befindet sich standardmäßig im Verzeichnis `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

   Geben Sie für `adminPasswordType` einen der folgenden Werte an:

   `Random`

   EC2Launch generiert ein Passwort und verschlüsselt es mit dem Schlüssel des Benutzers: Die Einstellung wird vom System nach dem Start der Instance deaktiviert, so dass das Passwort weiterhin gilt, wenn die Instance neu gestartet bzw. angehalten und gestartet wird.

   `Specify`

   EC2Launch verwendet das Passwort, das Sie unter angebe `adminPassword`. Wenn das Passwort nicht den Systemanforderungen entspricht, erstellt EC2Launch stattdessen ein zufälliges Passwort. Das Passwort wird in `LaunchConfig.json` im Klartext gespeichert

und gelöscht, wenn Windows Sysprep das Administratorpasswort einstellt. EC2Launch verschlüsselt das Passwort mit dem Schlüssel des Benutzers.

`DoNothing`

EC2Launch verwendet das Passwort, das Sie in der Datei `unattend.xml`-Datei angeben. Wenn Sie in der Datei `unattend.xml` kein Passwort angeben, ist das Administratorkonto deaktiviert.

5. (Optional) Geben Sie Einstellungen in `unattend.xml` und anderen Konfigurationsdateien an. Wenn Sie eine beaufsichtigte Installation planen, brauchen Sie keine Änderung in diesen Dateien vorzunehmen. Die Dateien befinden sich standardmäßig in folgendem Verzeichnis: `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.
6. Führen Sie in Windows PowerShell au `./InitializeInstance.ps1 -Schedule`. Das Script befindet sich standardmäßig in folgendem Verzeichnis: `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`. Dieses Script plant die Initialisierung der Instance beim nächsten Starten. Sie müssen diese Script ausführen, bevor Sie im nächsten Schritt das Script `SysprepInstance.ps1` ausführen.
7. Führen Sie in Windows PowerShell au `./SysprepInstance.ps1`. Das Script befindet sich standardmäßig in folgendem Verzeichnis: `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`.

Sie werden von der Instance abgemeldet und die Instance wird beendet. Auf der Seite Instances in der Amazon EC2-Konsole wechselt der Instance-Zustand von `Running` zu `Stopping` und zu `Stopped`. Jetzt kann ein AMI aus dieser Instance erstellt werden.

Aktualisieren von Metadaten/KMS-Routen für Server 2016 und höher beim Starten eines benutzerdefinierten AMI

So aktualisieren Sie Metadaten/KMS-Routen für Server 2016 und höher beim Starten eines benutzerdefinierten AMI:

- Führen Sie die GUI EC2LaunchSettings (C:\ProgramData\Amazon\EC2-Windows\Launch\Settings\Ec2LaunchSettings.exe) aus und wählen Sie die Option zum Herunterfahren mit Windows Sysprep aus.
- Führen Sie EC2LaunchSettings aus und fahren Sie ohne Windows Sysprep vor dem Erstellen des AMI herunter. Dadurch wird veranlasst, dass die Initialisierungsaufgaben des EC2-Starts beim nächsten Systemstart ausgeführt werden. Die Routen werden dann basierend auf dem Subnetz für die Instance festgelegt.

- Oder planen Sie die Initialisierungsaufgaben des EC2-Starts manuell neu, bevor Sie ein AMI über PowerShell erstellen.

  > **Important**
  >
  > Beachten Sie das Standardverhalten beim Zurücksetzen des Passworts, bevor Sie Aufgaben neu planen.

- Informationen zum Aktualisieren der Routen auf einer ausgeführten Instance, bei der eine Windows-Aktivierung oder Kommunikation mit Instance-Metadatenfehlern auftritt, finden Sie unter „Windows kann nicht aktiviert werden“.

Ein AMI mithilfe von Windows Sysprep mit EC2Config erstellen

Wenn Sie ein Image aus einer Instance erstellen, auf der der EC2Config-Service installiert ist, führt EC2Config während der Vorbereitung des Images bestimmte Aufgaben aus. Dies beinhaltet die Arbeit mit Windows Sysprep. Weitere Informationen finden Sie unter the section called “Sysprep-Phasen von Windows”.

Inhalt

- Windows-Sysprep-Aktionen
- Nach Sysprep
- Windows Sysprep mit dem EC2Config-Service ausführen

Windows-Sysprep-Aktionen

Windows Sysprep und der EC2Config-Service führen folgende Aktionen beim Vorbereiten eines Images aus.

1. Wenn Sie im Dialogfeld EC2-Serviceeigenschaften die Option Mit Sysprep herunterfahren auswählen, führt das System den Befehl ec2config.exe -sysprep aus.
2. Der EC2Config-Service liest den Inhalt der Datei `BundleConfig.xml` ein. Diese Datei befindet sich standardmäßig im folgenden Verzeichnis: `C:\Program Files\Amazon\Ec2ConfigService\Settings`.

   Die `BundleConfig.xml`-Datei umfasst die folgenden Einstellungen. Sie können diese Einstellungen ändern:

- AutoSysprep: Gibt an, ob Windows Sysprep automatisch verwendet werden soll. Sie brauchen diesen Wert nicht zu ändern, wenn Sie Windows Sysprep vom Dialogfeld „EC2-Service-Eigenschaften“ aus ausführen. Der Standardwert ist `No`.
- SetRDPCertificate: Legt ein selbstsigniertes Zertifikat für den Remote-Desktop-Server fest. Auf diese Weise können Sie das Remote Desktop Protocol (RDP) sicher verwenden, um eine Verbindung zur Instance herzustellen. Ändern Sie den Wert in `Yes`, wenn neue Instances ein Zertifikat verwenden sollen. Diese Einstellung wird für Windows Server 2012 Instances nicht verwendet, da diese Betriebssysteme ihre eigenen Zertifikate generieren können. Der Standardwert ist `No`.
- SetPasswordAfterSysprep: Legt ein zufälliges Passwort für eine neu gestartete Instance fest, verschlüsselt sie mit dem Benutzer-Startschlüssel und gibt das verschlüsselte Passwort an die Konsole aus. Ändern Sie den Wert in `No`, wenn die neuen Instances nicht als zufällig verschlüsseltes Passwort festgelegt werden sollen. Der Standardwert ist `Yes`.
- PreSysprepRunCmd: Der Speicherort des auszuführenden Befehls. Der Befehl befindet sich standardmäßig in folgendem Verzeichnis: `C:\Program Files\Amazon\Ec2ConfigService\Scripts\BeforeSysprep.cmd`

3. Das System führt au `BeforeSysprep.cmd`. Dieser Befehl erstellt den folgenden Registrierungsschlüssel:

   ```
   reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
    fDenyTSConnections /t REG_DWORD /d 1 /f
   ```

   Der Registrierungsschlüssel deaktiviert RDP-Verbindungen bis sie erneut aktiviert werden. Die Deaktivierung von RDP-Verbindungen ist eine notwendige Sicherheitsmaßnahme, da während der ersten Boot-Session nach der Ausführung von Windows Sysprep kurzzeitig Verbindungen von RDP zugelassen werden und noch kein Administratorkennwort vergeben ist.

4. Der EC2Config-Service ruft Windows Sysprep mit dem folgenden Befehl auf:

   ```
   sysprep.exe /unattend: "C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml" /
   oobe /generalize /shutdown
   ```

Generalisierungsphase

- Das Tool entfernt Image-spezifische Informationen und Konfigurationen, z. B. Computer-Name und SID. Wenn die Instance Mitglied einer Domain ist, wird sie von der Domain entfernt. Die

`sysprep2008.xml`-Antwortdatei enthält folgende Einstellungen, die sich auf diese Phase auswirken:

- PersistAllDeviceInstalls: Die Einstellung verhindert, dass Windows Setup Geräte entfernt und neu konfiguriert. Dies beschleunigt die Image-Vorbereitung, da Amazon-AMIs bestimmte Treiber für die Ausführung erfordern und die erneute Erkennung der Treiber Zeit erfordern würde.
- DoNotCleanUpNonPresentDevices: Die Einstellung hält Plug & Play-Informationen für Geräte zurück, die derzeit nicht vorhanden sind.

- Windows Sysprep beendet das Betriebssystem bei der Vorbereitung der Erstellung des AMI. Das System startet entweder eine neue Instance oder die ursprüngliche Instance.

Spezialisierungsphase

Das System erstellt OS-spezifische Anforderungen, z. B. Computer-Name und eine SID. Das System führt zudem die folgenden Aktionen basierend auf Konfigurationen durch, die Sie in der sysprep2008.xml-Antwortdatei angeben.

- CopyProfile: Windows Sysprep kann zur Löschung aller Benutzerprofile konfiguriert werden, einschließlich des integrierten Administratorprofils. Die Einstellung behält das integrierte Administratorkonto bei, sodass alle an diesem Konto vorgenommenen Anpassungen auf das neue Image übertragen werden. Der Standardwert ist „True“.

  CopyProfile ersetzt das Standardprofil durch das vorhandene Profil des lokalen Administrators. Alle Konten, die sich nach der Ausführung von Windows Sysprep anmelden, erhalten bei der ersten Anmeldung eine Kopie dieses Profils und seiner Inhalte.

  Wenn es keine spezifischen Benutzerprofilanpassungen gibt, die Sie auf das neue Image übertragen möchten, legen Sie diese Einstellung auf „False“ fest. Windows Sysprep wird alle Benutzerprofile entfernen. Das spart Zeit und Festplattenspeicher.
- TimeZone: Die Zeitzone wird standardmäßig auf koordinierte Weltzeit (UTC) festgelegt.
- Synchronous command with order 1: Das System führt den folgenden Befehl zur Aktivierung des Administratorkontos und Angabe der Passwortanforderungen aus.

  net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER / PASSWORDREQ:YES
- Synchronous command with order 2: Das System verschlüsselt das Administratorpasswort. Die Sicherheitsmaßnahme dient dazu, den Zugriff auf die Instance nach Abschluss von Windows Sysprep zu verhindern, wenn die ec2setpassword-Einstellung nicht aktiviert wurde.

C:\Programme\Amazon\Ec2ConfigService\ScramblePassword.exe" -u Administrator

- Synchronous command with order 3: Das System führt den folgenden Befehl aus:

  C:\Programme\Amazon\Ec2ConfigService\Scripts\SysprepSpecializePhase.cmd

  Der Befehl fügt den folgenden Registrierungsschlüssel hinzu, der RDP erneut aktiviert:

  reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f

OOBE-Phase

1. Das System gibt mit der EC2Config-Service-Antwortdatei die folgenden Konfigurationen an:
   - <InputLocale>en-US</InputLocale>
   - <SystemLocale>en-US</SystemLocale>
   - <UILanguage>en-US</UILanguage>
   - <UserLocale>en-US</UserLocale>
   - <HideEULAPage>true</HideEULAPage>
   - <HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
   - <NetworkLocation>Other</NetworkLocation>
   - <ProtectYourPC>3</ProtectYourPC>
   - <BluetoothTaskbarIconEnabled>false</BluetoothTaskbarIconEnabled>
   - <TimeZone>UTC</TimeZone>
   - <RegisteredOrganization>Amazon.com</RegisteredOrganization>
   - <RegisteredOwner>Amazon</RegisteredOwner>

   > **Note**
   >
   > Während der Generalisierungs- und Spezialisierungsphasen überwacht der EC2Config-Service den Status des Betriebssystems. Wenn EC2Config erkennt, dass sich das OS in einer Sysprep-Phase befindet, schreibt es die folgende Mitteilung in das Systemprotokoll: EC2ConfigMonitorState: 0 Windows is being configured. SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. Nach Abschluss der OOBE-Phase führt das System `SetupComplete.cmd` von folgendem Standort aus: `C:\Windows\Setup\Scripts\SetupComplete.cmd`. In öffentlichen AMIs von Amazon vor April 2015 war die Datei leer und es wurden keine Befehle für das Image ausgeführt. In öffentlichen AMIs, die nach April 2015 datiert wurden, enthält die Datei den folgenden Wert: call "C:\Program Files\Amazon\Ec2ConfigService\Scripts\PostSysprep.cmd".
3. Das System führt `PostSysprep.cmd` aus, das die folgenden Vorgänge ausführt:
   - Legt das Administratorpasswort so fest, dass es nicht ablaufen kann. Wenn das Passwort abläuft, können sich Administratoren anschließend möglicherweise nicht mehr anmelden.
   - Legt den MSSQLServer-Computer-Namen (sofern installiert) fest, sodass der Name mit dem AMI synchronisiert wird.

Nach Sysprep

Nach dem Abschluss von Windows Sysprep sendet der EC2Config-Service die folgende Mitteilung an die Konsolenausgabe:

```
Windows sysprep configuration complete.
   Message: Sysprep Start
   Message: Sysprep End
```

EC2Config führt anschließend die folgenden Aktionen aus:

1. Liest den Inhalt der config.xml-Datei aus und führt alle aktivierten Plugins aus.
2. Führt alle Plugins vom Typ „Before Windows is ready“ gleichzeitig aus.
   - Ec2SetPassword
   - Ec2SetComputerName
   - Ec2InitializeDrives
   - Ec2EventLog
   - Ec2ConfigureRDP
   - Ec2OutputRDPCert
   - Ec2SetDriveLetter
   - Ec2WindowsActivate
   - Ec2DynamicBootVolumeSize
3. Sendet nach Abschluss die Meldung „Windows is ready“ an die Instance-Systemprotokolle.
4. Führt alle Plugins vom Typ „After Windows is ready“ gleichzeitig aus.

- Amazon CloudWatch Logs
- UserData
- AWS Systems Manager (Systems Manager)

Weitere Informationen über Windows-Plug-ins finden Sie unter Den EC2Config-Service verwenden, um Aufgaben während des Starts der EC2-Legacy-Windows-Betriebssysteminstance auszuführen.

Windows Sysprep mit dem EC2Config-Service ausführen

Verwenden Sie das folgende Verfahren, um ein standardisiertes AMI mit Windows Sysprep und dem EC2Config-Service zu erstellen.

1. Suchen Sie in der Amazon EC2-Konsole das zu duplizierende AMI oder erstellen Sie eines.
2. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
3. Passen Sie sie an.
4. Geben Sie Konfigurationseinstellungen in der EC2Config-Service-Antwortdatei an:

   ```
   C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml
   ```
5. Klicken Sie im Windows-Start-Menü auf Alle Programme und anschließend auf EC2ConfigService Settings (EC2ConfigService-Einstellungen).
6. Wählen Sie die Registerkarte Image (Image) im Dialogfeld Ec2 Service Properties (Ec2-Service-Eigenschaften) aus. Weitere Informationen zu den Optionen und Einstellungen im Ec2 Service Properties-Dialogfeld finden Sie unter Ec2-Service-Eigenschaften.
7. Wählen Sie eine Option für das Administratorpasswort aus und wählen Sie anschließend Shutdown with Sysprep (Herunterfahren mit Sysrep) oder Shutdown without Sysprep (Herunterfahren ohne Sysprep). EC2Config bearbeitet die Einstellungsdateien basierend auf der ausgewählten Passwortoption.
   - Random (Zufällig): EC2Config erstellt ein Passwort, verschlüsselt es mit dem Benutzerschlüssel und gibt das verschlüsselte Passwort an die Konsole aus. Die Einstellung wird nach dem ersten Start deaktiviert, sodass das Passwort weiterhin gilt, wenn die Instance neu gestartet bzw. angehalten und gestartet wird.
   - Spezifizieren: Das Passwort wird unverschlüsselt (Klartext) in der Windows-Sysprep-Antwortdatei gespeichert. Bei der nächsten Ausführung von Windows Sysprep wird das Administratorpasswort festgelegt. Wenn Sie den Service gleich beenden, wird das Passwort sofort festgelegt. Sobald der Service erneut startet, wird das Administratorpasswort entfernt. Bewahren Sie das Passwort unbedingt gut auf, da Sie es später nicht erneut abrufen können.

- Vorhandenes beibehalten: Das bestehende Passwort für das Administratorkonto ändert sich nicht, wenn Windows Sysprep ausgeführt oder EC2Config neu gestartet wird. Bewahren Sie das Passwort unbedingt gut auf, da Sie es später nicht erneut abrufen können.

8. Klicken Sie auf OK.

Wenn Sie zum Bestätigen der Ausführung von Windows Sysprep und zum Beenden der Instance aufgefordert werden, klicken Sie auf Ja. Sie werden feststellen, dass EC2Config Windows Sysprep ausführt. Anschließend werden Sie von der Instance abgemeldet und die Instance wird beendet. Auf der Seite Instances in der Amazon EC2-Konsole wechselt der Instance-Zustand von `Running` zu `Stopping` und abschließend zu `Stopped`. Jetzt kann ein AMI aus dieser Instance erstellt werden.

Sie können das Windows-Sysprep-Tool manuell mittels Befehlszeile und dem folgenden Befehl aufrufen:

```
"%programfiles%\amazon\ec2configservice\"ec2config.exe -sysprep""
```

> **Note**
>
> Die doppelten Anführungszeichen sind nicht erforderlich, wenn sich die CMD-Shell bereits im Verzeichnis C:\Programme\Amazon\EC2ConfigService\ befindet.

Achten Sie aber sorgfältig auf die Angabe der richtigen XML-Dateioptionen im Ordner `Ec2ConfigService\Settings`, andernfalls kann möglicherweise keine Verbindung zur Instance hergestellt werden. Weitere Informationen zu diesen Einstellungsdateien finden Sie unter EC2Config-Einstellungsdateien. Ein Beispiel für die Konfiguration und das anschließende Ausführen von Windows Sysprep über die Befehlszeile finden Sie unter `Ec2ConfigService\Scripts\InstallUpdates.ps1`.

Ein EC2 Amazon-AMI kopieren

Wenn Sie eine konsistente EC2 Amazon-Instance-Konfiguration für mehrere Regionen benötigen, können Sie ein einzelnes Amazon Machine Image (AMI) als Vorlage verwenden, um alle Instances zu starten. Es AMIs handelt sich jedoch um regionsspezifische Ressourcen — um eine Instance in einer bestimmten Region zu starten AWS-Region, muss sich das AMI in dieser Region befinden. Um dasselbe AMI in mehreren Regionen zu verwenden, müssen Sie es daher von der Quellregion in jede Zielregion kopieren.

Die Methode, mit der Sie ein AMI kopieren, hängt davon ab, ob Sie regionsübergreifend innerhalb derselben Partition oder zwischen verschiedenen Partitionen kopieren:

- Regionsübergreifendes Kopieren — AMIs Regionsübergreifendes Kopieren innerhalb derselben Partition, z. B. zwischen den Regionen innerhalb der kommerziellen Partition. Diese Kopiermethode wird im folgenden Abschnitt beschrieben.
- Partitionsübergreifendes Kopieren — Kopieren Sie AMIs von einer Partition auf eine andere Partition, z. B. von der kommerziellen Partition auf die AWS GovCloud (US) Partition. Weitere Informationen zu dieser Kopiermethode finden Sie unter Speichern und Wiederherstellen eines AMI.
- Kontoübergreifendes Kopieren — Erstellen Sie eine Kopie eines AMI, das ein anderer AWS-Konto Benutzer mit Ihrem AWS-Konto geteilt hat. Diese Kopiermethode wird im folgenden Abschnitt beschrieben.

Die Zeit, die benötigt wird, um den Kopiervorgang für regionsübergreifendes und kontenübergreifendes AMI-Kopieren abzuschließen, wird nach bestem Wissen berechnet. Wenn Sie die Fertigstellungszeit kontrollieren möchten, können Sie ein Abschlussfenster zwischen 15 Minuten und 48 Stunden angeben, um sicherzustellen, dass Ihr AMI innerhalb des erforderlichen Zeitraums kopiert wird. Für zeitbasierte AMI-Kopiervorgänge fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter Zeitbasierte Kopien im Amazon-EBS-Benutzerhandbuch.

Inhalt

- Überlegungen
- Kosten
- Erteilen Sie Berechtigungen zum Kopieren von Amazon EC2 AMIs
- Kopieren eines AMI
- Anhalten eines ausstehenden AMI-Kopiervorgangs
- So funktioniert Amazon EC2 AMI Copy

Überlegungen

- Genehmigung zum Kopieren AMIs — Sie können IAM-Richtlinien verwenden, um Benutzern die Erlaubnis zum Kopieren zu erteilen oder zu verweigern. AMIs Ab dem 28. Oktober 2024 können Sie Berechtigungen auf Ressourcenebene für die `CopyImage`-Aktion im Quell-AMI angeben. Berechtigungen auf Ressourcenebene für das neue AMI sind wie bisher verfügbar.

- Startberechtigungen und Amazon S3 S3-Bucket-Berechtigungen — kopiert AWS keine Startberechtigungen oder Amazon S3 S3-Bucket-Berechtigungen vom Quell-AMI in das neue AMI. Nachdem der Kopiervorgang abgeschlossen ist, können Sie Startberechtigungen und Amazon-S3-Bucketberechtigungen auf das neue AMI anwenden.
- Tags – Sie können nur benutzerdefinierte AMI-Tags kopieren, die Sie an das Quell-AMI angefügt haben. System-Tags (Präfix mit `aws:`) und benutzerdefinierte Tags, die von anderen AWS-Konten angehängt wurden, werden nicht kopiert. Wenn Sie ein AMI kopieren, können Sie dem neuen AMI und seinen Backup-Snapshots neue Tags hinzufügen.
- Kontingente für zeitbasierte AMI-Kopien – Nachdem Sie Ihr kumulatives Durchsatzkontingent für Snapshot-Kopien erreicht haben, schlagen nachfolgende zeitbasierte AMI-Kopieranforderungen fehl. Weitere Informationen finden Sie unter Kontingente für zeitbasierte Kopien im Amazon-EBS-Benutzerhandbuch.
- Unterstützte Quell-Ziel-Kopien – Der Speicherort des Quell-AMI bestimmt, ob Sie es kopieren können und welche Ziele für das neue AMI zulässig sind:
  - Wenn sich das Quell-AMI in einer Region befindet, können Sie es innerhalb dieser Region, in eine andere Region, in einen mit dieser Region verknüpften Außenposten oder in eine Local Zone in dieser Region kopieren.
  - Wenn sich das Quell-AMI in einer Local Zone befindet, können Sie es innerhalb dieser Local Zone, in die übergeordnete Region dieser Local Zone oder in bestimmte andere Local Zonen mit derselben übergeordneten Region kopieren.
  - Wenn sich das Quell-AMI auf einem Outpost befindet, können Sie es nicht kopieren.
- CLI-Parameter für Quelle und Ziel – Bei Verwendung der CLI werden die folgenden Parameter unterstützt, um den Quellspeicherort des zu kopierenden AMI und das Ziel des neuen AMI anzugeben. Beachten Sie, dass der Kopiervorgang in der Zielregion initiiert werden muss. Wenn Sie den `--region` Parameter weglassen, nimmt das Ziel die in Ihren AWS CLI Einstellungen konfigurierte Standardregion an.

Von der Quelle zum Ziel	Quellparameter	Zielparameter
Von Region zu Region	`--source-region`	`--region`
Von Region zu Outpost	`--source-region`	`--destination-outpost-arn` (der ARN des Outpost)

Von der Quelle zum Ziel	Quellparameter	Zielparameter
Von einer Region zu einer Local Zone	`--source-region` Muss die übergeordnete Region der Local Zone sein.	`--destination-availability-zone` (der Name der Local Zone) oder `--destination-availability-zone-id` (die ID der Local Zone)
Von einer Local Zone zu einer Region	`--source-region` Muss die übergeordnete Region der Local Zone sein. Die Quell-Local-Zone wird vom Standort der angegebenen Quell-AMI-ID abgeleitet.	`--region` Muss die übergeordnete Region der Local Zone sein.
Von einer Local Zone in eine andere Local Zone	`--source-region` Muss die übergeordnete Region der Local Zone sein. Die Quell-Local-Zone wird vom Standort der angegebenen Quell-AMI-ID abgeleitet.	`--destination-availability-zone` (der Name der Local Zone) oder `--destination-availability-zone-id` (die ID der Local Zone)

Kosten

Für das Kopieren eines AMI, wenn keine Abschlusszeit angegeben ist, fallen keine Gebühren an. Für zeitbasierte AMI-Kopiervorgänge fallen jedoch zusätzliche Gebühren an. Weitere Informationen finden Sie unter Zeitbasierte Kopien im Amazon-EBS-Benutzerhandbuch.

Es fallen die Standardgebühren für Datenspeicherung und -übertragung an. Wenn Sie ein EBS-gestütztes AMI kopieren, fallen Gebühren für die Speicherung zusätzlicher EBS-Snapshots an.

Erteilen Sie Berechtigungen zum Kopieren von Amazon EC2 AMIs

Um ein EBS- oder Amazon-S3-gestütztes AMI zu kopieren, benötigen Sie die folgenden IAM-Berechtigungen:

- `ec2:CopyImage` – Um das AMI zu kopieren. Für EBS-gestützte Geräte wird auch die Erlaubnis erteilt AMIs, die Backing-Snapshots des AMI zu kopieren.
- `ec2:CreateTags` – So versehen Sie das Ziel-AMI mit Tags. Für EBS-gestützte Geräte wird außerdem die Erlaubnis erteiltAMIs, die Backing-Snapshots des Ziel-AMIs mit Tags zu versehen.

Wenn Sie ein auf einer Instance-Speicher-gestütztes AMI kopieren, benötigen Sie die folgenden zusätzlichen IAM-Berechtigungen:

- `s3:CreateBucket` – Um das S3-Bucket in der Zielregion für das neue AMI zu erstellen
- `s3:GetBucketAcl` – Um die ACL-Berechtigungen für den Quell-Bucket zu lesen
- `s3:ListAllMyBuckets`— Um einen vorhandenen S3-Bucket für AMIs in der Zielregion zu finden
- `s3:GetObject` – Um die Objekte im Quell-Bucket zu lesen
- `s3:PutObject` – Um die Objekte in den Ziel-Bucket zu schreiben
- `s3:PutObjectAcl` – Um die Berechtigungen für die neuen Objekte in den Ziel-Bucket zu schreiben

> **Note**
>
> Ab dem 28. Oktober 2024 können Sie Berechtigungen auf Ressourcenebene für die `CopyImage`-Aktion im Quell-AMI angeben. Berechtigungen auf Ressourcenebene für das Ziel-AMI sind wie bisher verfügbar. Weitere Informationen finden Sie CopyImagein der Tabelle unter Von Amazon definierte Aktionen EC2 in der Service Authorization Reference.

Beispiel für eine IAM-Richtlinie zum Kopieren eines EBS-gestützten AMI und zum Markieren des Ziel-AMI und der Snapshots

Die folgende Beispielrichtlinie gewährt Ihnen die Berechtigung, jedes EBS-gestützte AMI zu kopieren und das Ziel-AMI und seine Backup-Snapshots mit Tags zu versehen.

> **Note**
>
> Ab dem 28. Oktober 2024 können Sie Snapshots im Element `Resource` angeben. Weitere Informationen finden Sie CopyImagein der Tabelle unter Von Amazon definierte Aktionen EC2 in der Service Authorization Reference.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Sid": "PermissionToCopyAllImages",
        "Effect": "Allow",
        "Action": [
            "ec2:CopyImage",
            "ec2:CreateTags"
        ],
        "Resource": [
            "arn:aws:ec2:*::image/*",
            "arn:aws:ec2:*::snapshot/*"
        ]
    }]
}
```

Beispiel für eine IAM-Richtlinie zum Kopieren eines EBS-gestützten AMI, aber Verweigerung des Tagging der neuen Snapshots

Die `ec2:CopySnapshot`-Berechtigung wird automatisch gewährt, wenn Sie die `ec2:CopyImage`-Berechtigung erhalten. Die Berechtigung, die neuen Backup-Snapshots mit Tags zu versehen, kann explizit verweigert werden, wodurch der `Allow`-Effekt der `ec2:CreateTags`-Aktion außer Kraft gesetzt wird.

Die folgende Beispielrichtlinie gewährt Ihnen die Berechtigung, jedes EBS-gestützte AMI zu kopieren, aber verweigert Ihnen, das Ziel-AMI und seine Backup-Snapshots mit Tags zu versehen.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*::image/*",
                "arn:aws:ec2:*::snapshot/*"
            ]
        },
        {
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:::snapshot/*"
        }
    ]
}
```

Beispiel für eine IAM-Richtlinie zum Kopieren eines Amazon-S3-gestützten AMI und zum Markieren des Ziel-AMI

Die folgende Beispielrichtlinie gewährt Ihnen die Berechtigung, jedes Amazon-S3-gestützte AMI im angegebenen Quell-Bucket in die angegebene Region zu kopieren und das Ziel-AMI zu markieren.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "PermissionToCopyAllImages",
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": "s3:ListAllMyBuckets",
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:PutObjectAcl",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amis-for-111122223333-in-us-east-2-hash"
            ]
        }
    ]
}
```

Um den Amazon-Ressourcennamen (ARN) des AMI-Quell-Buckets zu finden, öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/AMIs, wählen Sie im Navigationsbereich und suchen Sie den Bucket-Namen in der Spalte Quelle.

> **Note**
>
> Die `s3:CreateBucket`-Berechtigung ist nur erforderlich, wenn Sie das erste Mal ein Amazon-S3-gestütztes AMI in eine individuelle Region kopieren. Danach wird der Amazon S3 S3-Bucket, der bereits in der Region erstellt wurde, verwendet, um alle future Daten zu speichern AMIs , die Sie in diese Region kopieren.

Kopieren eines AMI

Sie können ein AMI kopieren, das Sie besitzen oder ein AMI, das mit Ihnen von einem anderen Konto geteilt wurde. Informationen zu den unterstützten Quell- und Zielkombinationen finden Sie unter Überlegungen.

Console

So kopieren Sie ein AMI

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Konsolennavigationsleiste die Region mit dem AMI aus.
3. Wählen Sie im Navigationsbereich aus, ob AMIsdie Liste der AMIs verfügbaren Optionen in der Region angezeigt werden soll.
4. Wenn Sie das AMI, das Sie kopieren möchten, nicht sehen, wählen Sie einen anderen Filter. Sie können nach „Mein AMIs Eigentum“, „Private Bilder“, „Öffentliche Bilder“ und „Deaktivierte Bilder“ filtern.
5. Wählen Sie das zu kopierende AMI und anschließend Aktionen, AMI kopieren aus.
6. Geben Sie auf der Seite Amazon Machine Image (AMI) kopieren die folgenden Informationen an:

   a. Name der AMI-Kopie: Der Name für das neue AMI. Sie können die Betriebssysteminformationen in den Namen aufnehmen, da Amazon diese Informationen bei der Anzeige von Details zum AMI EC2 nicht bereitstellt.

   b. Beschreibung der AMI-Kopie: Standardmäßig enthält die Beschreibung Informationen zum Quell-AMI zur Unterscheidung der Kopie vom Original. Sie können die Beschreibung bei Bedarf ändern.

   c. Zielregion: Die Region, in die das AMI kopiert werden soll. Weitere Informationen erhalten Sie unter Regionsübergreifendes Kopieren und Kontoübergreifendes Kopieren.

   d. Tags kopieren: Aktivieren Sie dieses Kontrollkästchen, um Ihre benutzerdefinierten AMI-Tags beim Kopieren des AMI einzubeziehen. System-Tags (Präfix mit `aws:`) und benutzerdefinierte Tags, die von anderen AWS-Konten angehängt wurden, werden nicht kopiert.

   e. Zeitbasiertes Kopieren: Sie können wie folgt angeben, ob der Kopiervorgang innerhalb eines bestimmten Zeitrahmens oder nach bestem Wissen abgeschlossen werden soll:

      - Um den Kopiervorgang innerhalb eines bestimmten Zeitrahmens abzuschließen:

- Wählen Sie Zeitbasiertes Kopieren aktivieren aus.
- Geben Sie unter Dauer der Fertigstellung die Anzahl der Minuten (in Schritten von 15 Minuten) ein, die für den Kopiervorgang zulässig sind. Die Abschlussdauer gilt für alle Snapshots, die dem AMI zugeordnet sind.

  Weitere Informationen finden Sie unter Zeitbasierte Kopien im Amazon-EBS-Benutzerhandbuch.

- So können Sie nach bestem Wissen kopieren lassen:
  - Lassen Sie die Option Zeitbasiertes Kopieren aktivieren nicht ausgewählt.

f. (AMIs Nur EBS-gestützt) EBS-Snapshots der AMI-Kopie verschlüsseln: Wählen Sie dieses Kontrollkästchen, um die Ziel-Snapshots zu verschlüsseln oder um sie mit einem anderen Schlüssel erneut zu verschlüsseln. Wenn Sie die standardmäßige Verschlüsselung aktiviert haben, ist das Kontrollkästchen EBS-Snapshots der AMI-Kopie verschlüsseln aktiviert und kann nicht deaktiviert werden. Weitere Informationen finden Sie unter Verschlüsselung und Kopieren.

g. (AMIs Nur EBS-gestützt) KMS-Schlüssel: Der KMS-Schlüssel, der zum Verschlüsseln der Ziel-Snapshots verwendet wird.

h. Tags: Sie können das neue AMI und die neuen Snapshots mit denselben Tags kennzeichnen oder sie mit verschiedenen Tags kennzeichnen.

   - Um das AMI und die Snapshots mit den gleichen Tags zu markieren, wählen Sie Image und Snapshots zusammen markieren. Die gleichen Tags werden auf das neue AMI und jeden erstellten Snapshot angewendet.
   - Um das AMI und die Snapshots mit verschiedenen Tags zu markieren, wählen Sie Image und Snapshots separat markieren. Unterschiedliche Tags werden auf das AMI und die erstellten Snapshots angewendet. Beachten Sie jedoch, dass alle neu erstellten Snapshots die gleichen Tags erhalten. Sie können nicht jeden neuen Snapshot mit einem anderen Tag versehen.

   Sie fügen ein Tag (Markierung) hinzu, indem Sie Add Tags (Tag (Markierung) hinzufügen) auswählen und den Schlüssel und den Wert für das Tags (Markierungen) eingeben. Wiederholen Sie diesen Schritt für jeden Tag (Markierung).

i. Wenn Sie bereit sind, das AMI zu kopieren, wählen Sie AMI kopieren.

Der ursprüngliche Status des neuen AMI ist `Pending`. Der AMI-Kopiervorgang ist abgeschlossen, wenn der Status `Available` lautet.

AWS CLI

So kopieren Sie ein AMI von einer Region in eine andere

Verwenden Sie den Befehl copy-image . Geben Sie die Quell- und Zielregionen an. Geben Sie die Quellregion mit dem `--source-region`-Parameter an. Sie können die Zielregion mithilfe des Parameters `--region` angeben (oder diesen Parameter weglassen, um die in Ihren AWS CLI -Einstellungen konfigurierte Standardregion anzunehmen).

```
aws ec2 copy-image \
    --source-image-id ami-0abcdef1234567890 \
    --source-region us-west-2 \
    --name my-ami \
    --region us-east-1
```

Wenn Sie einen Ziel-Snapshot beim Kopieren eines AMI verschlüsseln, müssen Sie diese zusätzlichen Parameter angeben: `--encrypted` und `--kms-key-id`.

So kopieren Sie ein AMI von einer Region in eine Local Zone

Verwenden Sie den Befehl copy-image . Sie müssen die Quell- und Zielregionen angeben. Geben Sie die Quellregion mit dem `--source-region`-Parameter an. Sie geben die Ziel-Local-Zone mithilfe des Parameters `--destination-availability-zone` an (Sie können stattdessen `--destination-availability-zone-id` verwenden). Beachten Sie, dass Sie ein AMI nur von einer Region in eine Local Zone innerhalb derselben Region kopieren können.

```
aws ec2 copy-image \
    --source-image-id ami-0abcdef1234567890 \
    --source-region cn-north-1 \
    --destination-availability-zone cn-north-1-pkx-1a \
    --name my-ami \
    --region cn-north-1
```

So kopieren Sie ein AMI von einer Local Zone in eine Region

Verwenden Sie den Befehl copy-image . Sie müssen die Quell- und Zielregionen angeben. Geben Sie die Quellregion mit dem `--source-region`-Parameter an. Sie geben die Zielregion mithilfe

des Parameters `--region` an (oder lassen Sie diesen Parameter weg, um die in Ihren AWS CLI -Einstellungen konfigurierte Standardregion anzunehmen). Die Quell-Local-Zone wird vom Standort der angegebenen Quell-AMI-ID abgeleitet. Beachten Sie, dass Sie ein AMI nur von einer Local Zone in die übergeordnete Region kopieren können.

```
aws ec2 copy-image \
    --source-image-id ami-0abcdef1234567890 \
    --source-region cn-north-1 \
    --name my-ami \
    --region cn-north-1
```

So kopieren Sie ein AMI von einer Local Zone in eine andere Local Zone

Verwenden Sie den Befehl copy-image . Sie müssen die Quell- und Zielregionen angeben. Sie geben die Quellregion der Local Zone mit dem Parameter `--source-region` an. Sie geben die Ziel-Local-Zone mithilfe des Parameters `--destination-availability-zone` an (Sie können stattdessen `--destination-availability-zone-id` verwenden). Die Quell-Local-Zone wird vom Standort der angegebenen Quell-AMI-ID abgeleitet. Sie geben die übergeordnete Region der lokalen Zielzone mithilfe des `--region` Parameters an (oder lassen Sie diesen Parameter weg, um die in Ihren Einstellungen konfigurierte Standardregion anzunehmen). AWS CLI

```
aws ec2 copy-image \
    --source-image-id ami-0abcdef1234567890 \
    --source-region cn-north-1 \
    --destination-availability-zone cn-north-1-pkx-1a \
    --name my-ami \
    --region cn-north-1
```

PowerShell

So kopieren Sie ein AMI von einer Region in eine andere

Verwenden Sie das cmdlet Copy-EC2Image. Geben Sie die Quell- und Zielregionen an. Geben Sie die Quellregion mit dem `-SourceRegion`-Parameter an. Sie können die Zielregion mithilfe des `-Region` Parameters oder des Cmdlets AWSDefaultSet-Region angeben.

```
Copy-EC2Image `
    -SourceImageId ami-0abcdef1234567890 `
    -SourceRegion us-west-2 `
```

```
    -Name my-ami `
    -Region us-east-1
```

Wenn Sie einen Ziel-Snapshot beim Kopieren eines AMI verschlüsseln, müssen Sie diese zusätzlichen Parameter angeben: `-Encrypted` und `-KmsKeyId`.

So kopieren Sie ein AMI von einer Region in eine Local Zone

Verwenden Sie das cmdlet Copy-EC2Image. Sie müssen die Quell- und Zielregionen angeben. Geben Sie die Quellregion mit dem `-SourceRegion`-Parameter an. Sie geben die Ziel-Local-Zone mithilfe des Parameters `-DestinationAvailabilityZone` an (Sie können stattdessen `-DestinationAvailabilityZoneId` verwenden). Beachten Sie, dass Sie ein AMI nur von einer Region in eine Local Zone innerhalb derselben Region kopieren können.

```
Copy-EC2Image `
    -SourceImageId ami-0abcdef1234567890 `
    -SourceRegion cn-north-1 `
    -DestinationAvailabilityZone cn-north-1-pkx-1a `
    -Name my-ami `
    -Region cn-north-1
```

So kopieren Sie ein AMI von einer Local Zone in eine Region

Verwenden Sie das cmdlet Copy-EC2Image. Sie müssen die Quell- und Zielregionen angeben. Geben Sie die Quellregion mit dem `-SourceRegion`-Parameter an. Sie geben die Zielregion mithilfe des `-Region` Parameters oder des Cmdlets AWSDefaultSet-Region an. Die Quell-Local-Zone wird vom Standort der angegebenen Quell-AMI-ID abgeleitet. Beachten Sie, dass Sie ein AMI nur von einer Local Zone in die übergeordnete Region kopieren können.

```
Copy-EC2Image `
    -SourceImageId ami-0abcdef1234567890 `
    -SourceRegion cn-north-1 `
    -Name my-ami `
    -Region cn-north-1
```

So kopieren Sie ein AMI von einer Local Zone in eine andere Local Zone

Verwenden Sie das cmdlet Copy-EC2Image. Sie müssen die Quell- und Zielregionen angeben. Sie geben die Quellregion der Local Zone mit dem Parameter `-SourceRegion` an. Sie geben die Ziel-Local-Zone mithilfe des Parameters `-DestinationAvailabilityZone` an (Sie können

stattdessen `-DestinationAvailabilityZoneId` verwenden). Die Quell-Local-Zone wird vom Standort der angegebenen Quell-AMI-ID abgeleitet. Sie geben die übergeordnete Region der lokalen Zielzone mithilfe des `-Region` Parameters oder des Cmdlets AWSDefaultSet-Region an.

```
Copy-EC2Image `
    -SourceImageId ami-0abcdef1234567890 `
    -SourceRegion cn-north-1 `
    -DestinationAvailabilityZone cn-north-1-pkx-1a `
    -Name my-ami `
    -Region cn-north-1
```

Anhalten eines ausstehenden AMI-Kopiervorgangs

Sie können eine ausstehende AMI mit den folgenden Verfahren kopieren.

Console

So halten Sie einen AMI-Kopiervorgang an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der oberen Navigationsleiste die Zielregion aus der Regionsauswahl aus.
3. Wählen Sie im Navigationsbereich AMIs aus.
4. Wählen Sie das entsprechende AMI und anschließend Aktionen und AMI-Registrierung abmelden aus.
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie AMI abmelden aus.

AWS CLI

So halten Sie einen AMI-Kopiervorgang an

Verwenden Sie den Befehl deregister-image.

```
aws ec2 deregister-image --image-id ami-0abcdef1234567890
```

PowerShell

So halten Sie einen AMI-Kopiervorgang an mit

Verwenden Sie das cmdlet Unregister-EC2Image.

```
Unregister-EC2Image -ImageId ami-0abcdef1234567890
```

So funktioniert Amazon EC2 AMI Copy

Durch Kopieren eines Quell-AMI wird ein identisches aber eindeutiges neues AMI erstellt, das wir auch als das Ziel-AMI bezeichnen. Das Ziel-AMI hat seine eigene eindeutige AMI-ID. Sie können das Quell-AMI ändern oder die Registrierung aufheben. Dies hat keine Auswirkungen auf das Ziel-AMI. Umgekehrt gilt dies auch.

Mit einem EBS-gestützten AMI wird jeder der Backup-Snapshots zu einem identischen, aber eindeutigen Ziel-Snapshot kopiert. Wenn Sie eine AMI in eine neue Region kopieren, sind die Snapshots vollständige (nicht inkrementelle) Kopien. Wenn Sie unverschlüsselte Backing-Snapshots verschlüsseln oder in einen neuen KMS-Schlüssel verschlüsseln, sind die Snapshots vollständige (nicht inkrementelle) Kopien. Nachfolgende Kopiervorgänge eines AMI-Ergebnisses in inkrementellen Kopien der Backing-Snapshots.

Inhalt

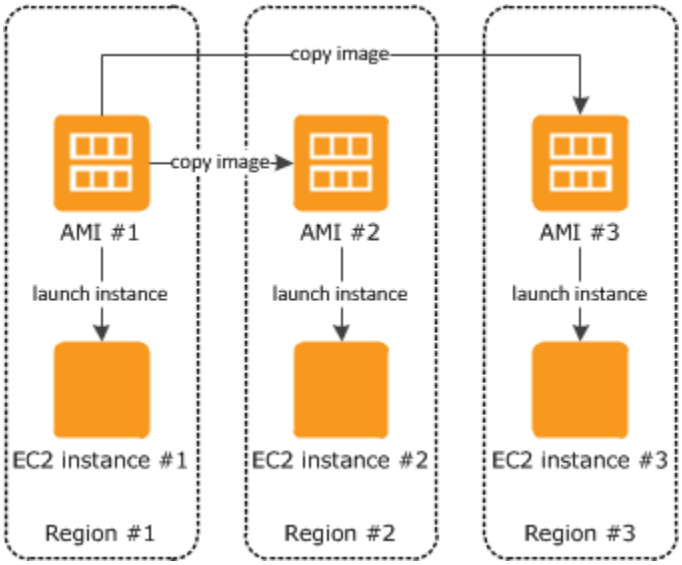
- Regionsübergreifendes Kopieren
- Kontoübergreifendes Kopieren
- Zeitbasierte AMI-Kopiervorgänge
- Verschlüsselung und Kopieren

Regionsübergreifendes Kopieren

Das Kopieren eines AMI zwischen geografisch unterschiedlichen Regionen bietet folgende Vorteile:

- Einheitliche globale Bereitstellung: Kopieren Sie ein AMI aus einer Region in eine andere, um einheitliche, auf dem gleichen AMI basierende Instances in verschiedenen Regionen zu starten.
- Skalierbarkeit: Entwerfen Sie Anwendungen für den globalen Einsatz, die die Anforderungen Ihrer Benutzer erfüllen, unabhängig davon, wo sie sich befinden.
- Performance: Steigern Sie die Leistung von Anwendungen, indem Sie sie verteilen und kritische Komponenten näher an die Benutzer rücken. Zudem können Sie regionsspezifische Features nutzen, z. B. Instance-Typen oder andere AWS -Dienste.
- Hohe Verfügbarkeit: Sie können Anwendungen entwerfen und zwischen AWS -Regionen übergreifend bereitstellen, um die Verfügbarkeit zu erhöhen.

Das folgende Diagramm zeigt die Beziehung zwischen einem Quell-AMI und zwei, die AMIs in verschiedenen Regionen kopiert wurden, sowie die EC2 Instances, die von jeder Region aus gestartet wurden. Beim Starten einer Instance von einem AMI verbleibt sie in derselben Region, in der sich auch das AMI befindet. Wenn Sie Änderungen am Quell-AMI vornehmen und möchten, dass sich diese Änderungen AMIs in den Zielregionen widerspiegeln, müssen Sie das Quell-AMI erneut in die Zielregionen kopieren.



Wenn Sie ein Amazon S3-gestütztes AMI zum ersten Mal in eine Region kopieren, erstellen wir einen Amazon S3 S3-Bucket für das in diese Region AMIs kopierte. Alle Amazon S3-gestützten Dateien AMIs , die Sie in diese Region kopieren, werden in diesem Bucket gespeichert. Die Bucket-Namen haben das folgende Format: amis-for- -in- -*account*. *region hash* Beispiel: `amis-for-123456789012-in-us-east-2-yhjmxvp6`.

Voraussetzung

Aktualisieren Sie vor dem Kopieren eines AMI die Inhalte des Quell-AMI, damit die Ausführung in einer anderen Region unterstützt wird. Aktualisieren Sie z. B. Datenbankverbindungs-Zeichenfolgen oder ähnliche Anwendungskonfigurationsdaten, sodass sie auf die entsprechenden Ressourcen verweisen. Andernfalls verwenden Instances, die vom neuen AMI in der Zielregion gestartet werden, möglicherweise noch die Ressourcen aus der Quellregion, was die Leistung beeinträchtigen und Kosten erhöhen kann.

Einschränkungen

- Die Zielregionen sind auf 300 gleichzeitige AMI-Kopiervorgänge beschränkt. Dies gilt auch für zeitbasierte AMI-Kopiervorgänge.

- Sie können ein paravirtuelles AMI (PV) nicht in eine Region kopieren, die PV nicht unterstützt. AMIs Weitere Informationen finden Sie unter Virtualisierungstypen.

Kontoübergreifendes Kopieren

Wenn ein AMI von einem anderen mit Ihrem geteilt AWS-Konto wird AWS-Konto, können Sie das gemeinsame AMI kopieren. Man spricht auch von einem kontenübergreifenden Zugriff. Das AMI, das für Sie freigegeben wird, ist das Quell-AMI. Wenn Sie das Quell-AMI kopieren, erstellen Sie ein neues AMI. Das neue AMI wird oft als Ziel-AMI bezeichnet.

AMI-Kosten

- Bei einem freigegebenen AMI wird dem Konto des freigegebenen AMI der Speicher in der Region in Rechnung gestellt.
- Wenn Sie ein AMI kopieren, das für Ihr Konto freigegeben wird, sind Sie der Eigentümer des Ziel-AMI in Ihrem Konto.
  - Dem Eigentümer des Quell-AMI werden die standardmäßigen Amazon-EBS- bzw. Amazon-S3-Übertragungsgebühren in Rechnung gestellt.
  - Die Gebühren für den Speicher des Ziel-AMI in der Zielregion werden Ihnen in Rechnung gestellt.

Berechtigungen für Ressourcen

Um ein AMI zu kopieren, das mit Ihnen von einem anderen Konto geteilt wurde, muss Ihnen der Besitzer des Quell-AMI Leseberechtigungen für den Speicher zuweisen, der das AMI sichert, und nicht nur für das AMI selbst. Der Speicher ist entweder der zugehörige EBS-Snapshot (für ein Amazon-EBS-gestütztes AMI) oder ein zugehöriger S3-Bucket (für ein Amazon-S3-gestütztes AMI). Wenn das freigegebene AMI über verschlüsselte Snapshots verfügt, muss der Eigentümer den bzw. die Schlüssel auch für Sie freigeben. Weitere Informationen zur Gewährung von Ressourcenberechtigungen für EBS-Snapshots finden Sie unter Freigabe eines Amazon-EBS-Snapshots für andere AWS-Konten im Benutzerhandbuch für Amazon EBS. Für S3-Buckets siehe Identitäts- und Zugriffsmanagement in Amazon S3 im Benutzerhandbuch für Amazon S3.

> **Note**
>
> Tags, die an das Quell-AMI angefügt sind, werden nicht kontenübergreifend in das Ziel-AMI kopiert.

Zeitbasierte AMI-Kopiervorgänge

Wenn Sie einen zeitbasierten AMI-Kopiervorgang für ein EBS-gestütztes AMI mit einem einzelnen zugehörigen Snapshot initiieren, verhält es sich genauso wie ein einzelner zeitbasierter Snapshot-Kopiervorgang, und es gelten dieselben Durchsatzlimits.

Wenn Sie einen zeitbasierten AMI-Kopiervorgang für ein EBS-gestütztes AMI mit mehreren zugehörigen Snapshots initiieren, verhält es sich genauso wie bei gleichzeitigen zeitbasierten Snapshot-Kopiervorgängen, und es gelten dieselben Durchsatzlimits. Jeder zugehörige Snapshot führt zu einer separaten Snapshot-Kopieranforderung, die jeweils zu Ihrem kumulativen Durchsatzkontingent für Snapshot-Kopien beiträgt. Die von Ihnen angegebene Abschlussdauer gilt für jeden zugehörigen Snapshot.

Weitere Informationen finden Sie unter Zeitbasierte Kopien im Amazon-EBS-Benutzerhandbuch.

Verschlüsselung und Kopieren

In der folgenden Tabelle ist der Verschlüsselungssupport für diverse AMI-Kopierszenarien abgebildet. Sie können zwar einen nicht verschlüsselten Snapshot zur Erstellung eines verschlüsselten Snapshots erstellen, umgekehrt ist dies jedoch nicht möglich.

Szenario	Beschreibung	Unterstützt
1	Nicht verschlüsselt zu nicht verschlüsselt	Ja
2	Verschlüsselt zu verschlüsselt	Ja
3	Nicht verschlüsselt zu verschlüsselt	Ja
4	Verschlüsselt zu nicht verschlüsselt	Nein

> **Note**
>
> Die Verschlüsselung während der `CopyImage` Aktion gilt nur für Amazon AMIs EBS-gestützte Anwendungen. Da ein Amazon-S3-gestütztes AMI keine Snapshots erfordert, können Sie mithilfe des Kopiervorgangs den Verschlüsselungsstatus nicht ändern.

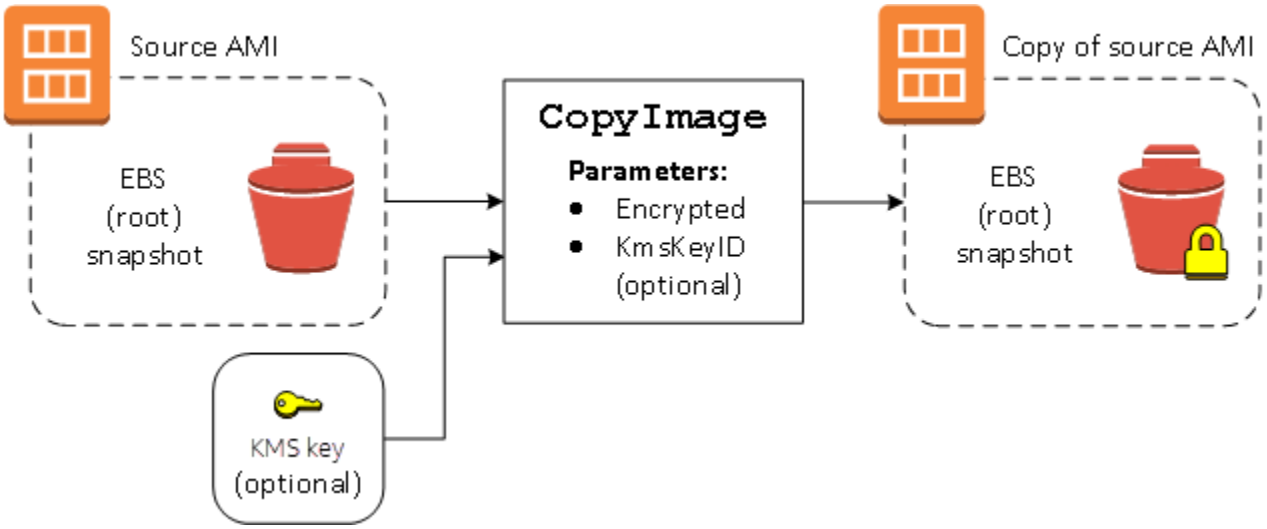
Wenn Sie ein AMI ohne Angabe von Verschlüsselungsparametern kopieren, wird der Backup-Snapshot in der Standardeinstellung mit seinem ursprünglichen Verschlüsselungsstatus kopiert. Wenn das Quell-AMI durch einen unverschlüsselten Snapshot gesichert wird, ist der resultierende Ziel-Snapshot daher auch unverschlüsselt. Wenn der Snapshot des Quell-AMIs verschlüsselt ist, wird auch der resultierende Ziel-Snapshot mit demselben Schlüssel verschlüsselt. AWS KMS Bei einem AMIs Backup durch mehrere Snapshots behält jeder Ziel-Snapshot den Verschlüsselungsstatus des entsprechenden Quell-Snapshots bei.

Um den Verschlüsselungsstatus der Ziel-Backing-Snapshots während einer AMI-Kopie zu ändern, können Sie Verschlüsselungsparameter angeben. Das folgende Beispiel zeigt einen nicht standardmäßigen Fall, in dem mit der `CopyImage`-Aktion Verschlüsselungsparameter bereitgestellt werden, um den Verschlüsselungsstatus des Ziel-AMIs zu ändern.

Kopieren eines nicht verschlüsselten Quell-AMI zu einem verschlüsselten Ziel-AMI

In diesem Szenario wird ein von einem unverschlüsselten Stamm-Snapshot unterstütztes AMI in ein AMI mit einem verschlüsselten Stamm-Snapshot kopiert. Die Aktion `CopyImage` wird mit zwei Verschlüsselungsparametern aufgerufen, einschließlich eines vom Kunden verwalteten Schlüssels. Dadurch ändert sich der Verschlüsselungsstatus des Stamm-Snapshots, sodass das Ziel-AMI durch einen Stamm-Snapshot gestützt wird, der dieselben Daten wie der Quell-Snapshot enthält, aber mit dem angegebenen Schlüssel verschlüsselt wird. In beiden Fällen fallen Speicherkosten für die Snapshots sowie Gebühren für alle Instances anAMIs, die Sie von einem der beiden AMI aus starten.

> **Note**
>
> Das Aktivieren von standardmäßige Verschlüsselung hat die gleiche Wirkung wie das Festlegen des `Encrypted`-Parameters auf `true` für alle Snapshots im AMI.



Wenn der `Encrypted`-Parameter festgelegt wird, wird der einzige Snapshot für diese Instance verschlüsselt. Wenn Sie den `KmsKeyId`-Parameter nicht angeben, wird der standardmäßige vom Kunden verwaltete Schlüssel zum Verschlüsseln der Snapshot-Kopie verwendet.

Weitere Informationen zum Kopieren AMIs mit verschlüsselten Snapshots finden Sie unter. Verwenden der Verschlüsselung mit EBS-gestützten AMIs

Speichern und Wiederherstellen eines AMI mit S3

Sie können ein Amazon Machine Image (AMI) in einem Amazon S3-Bucket speichern, das AMI in einen anderen S3-Bucket kopieren und dann aus dem S3-Bucket wiederherstellen. Durch das Speichern und Wiederherstellen eines AMI mithilfe von S3-Buckets können Sie AMIs von einer AWS Partition auf eine andere kopieren, z. B. von der kommerziellen Hauptpartition auf die AWS GovCloud (US) Partition. Sie können auch Archivkopien von erstellen, AMIs indem Sie sie in einem S3-Bucket speichern.

APIs Für das Speichern und Wiederherstellen eines AMI mit S3 werden `CreateStoreImageTask`, `DescribeStoreImageTasks`, und unterstütztCreateRestoreImageTask.

`CopyImage`ist die empfohlene API für das Kopieren AMIs innerhalb einer AWS Partition. `CopyImage` kann jedoch kein AMI in eine andere Partition kopieren.

Informationen zu den AWS Partitionen finden Sie *`partition`* auf der Seite Amazon Resource Names (ARNs) im IAM-Benutzerhandbuch.

> **Warning**
>
> Stellen Sie sicher, dass Sie beim Verschieben von Daten zwischen AWS Partitionen oder AWS Regionen alle geltenden Gesetze und Geschäftsanforderungen einhalten, einschließlich, aber nicht beschränkt auf, alle geltenden behördlichen Vorschriften und Anforderungen an die Datenresidenz.

Inhalt

- Anwendungsfälle
- Einschränkungen
- Kosten
- Funktionsweise der AMI-Speicherung- und -Wiederherstellung
- Eine Aufgabe zum Speichern eines Images erstellen

Anwendungsfälle

Verwenden Sie Store and Restore APIs , um Folgendes zu tun:

- Kopieren Sie ein AMI zwischen AWS Partitionen
- Erstellen Sie Archivkopien von AMIs

Kopieren Sie ein AMI zwischen AWS Partitionen

Durch Speichern und Wiederherstellen eines AMI mithilfe von S3-Buckets können Sie ein AMI von einer AWS Partition auf eine andere oder von einer AWS Region in eine andere kopieren. Im folgenden Beispiel kopieren Sie ein AMI von der kommerziellen Hauptpartition auf die AWS GovCloud (US) Partition, insbesondere von der `us-east-2` Region in die `us-gov-east-1` Region.

Um ein AMI von einer Partition auf eine andere zu kopieren, führen Sie die folgenden Schritte aus:

- Speichern Sie das AMI in einem S3-Bucket in der aktuellen Region mithilfe von `CreateStoreImageTask`. In diesem Beispiel befindet sich der S3-Bucket in `us-east-2`.
- Überwachen Sie den Fortschritt der Speicheraufgabe mithilfe von `DescribeStoreImageTasks`. Das Objekt wird im S3-Bucket sichtbar, wenn die Aufgabe abgeschlossen ist.
- Kopieren Sie das gespeicherte AMI-Objekt mit einer Prozedur Ihrer Wahl in einen S3-Bucket in der Zielpartition. In diesem Beispiel befindet sich der S3-Bucket in `us-gov-east-1`.

> **Note**
>
> Da Sie für jede Partition unterschiedliche AWS Anmeldeinformationen benötigen, können Sie ein S3-Objekt nicht direkt von einer Partition auf eine andere kopieren. Der Prozess zum Kopieren eines S3-Objekts über Partitionen hinweg liegt außerhalb des Rahmens dieser Dokumentation. Wir stellen die folgenden Kopierprozesse als Beispiele zur Verfügung, aber Sie müssen den Kopierprozess verwenden, der Ihren Sicherheitsanforderungen entspricht.
>
> - Um ein AMI partitionsübergreifend zu kopieren, könnte der Kopiervorgang so einfach sein wie folgt: Laden Sie das Objekt aus dem Quell-Bucket auf einen Zwischenhost (z. B. eine EC2 Instance oder einen Laptop) herunter und laden Sie dann das Objekt vom Zwischenhost in den Ziel-Bucket hoch. Verwenden Sie für jede Phase des Prozesses die AWS Anmeldeinformationen für die Partition.
> - Für eine nachhaltigere Nutzung sollten Sie erwägen, eine Anwendung zu entwickeln, die die Kopien verwaltet, möglicherweise mithilfe von mehrteiligen S3-Downloads und -Uploads.

- Stellen Sie das AMI aus dem S3-Bucket in der Zielpartition mithilfe von `CreateRestoreImageTask` wieder her. In diesem Beispiel befindet sich der S3-Bucket in `us-gov-east-1`.
- Überwachen Sie den Fortschritt der Wiederherstellungsaufgabe, indem Sie das AMI beschreiben, um zu überprüfen, wann sein Status verfügbar wird. Sie können auch die Fortschrittsprozentsätze der Snapshots, aus denen das wiederhergestellte AMI besteht, überwachen, indem Sie die Snapshots beschreiben.

Erstellen Sie Archivkopien von AMIs

Sie können Archivkopien von erstellen, AMIs indem Sie sie in einem S3-Bucket speichern. Das AMI wird in S3 in ein einzelnes Objekt gepackt, und alle AMI-Metadaten (ohne Freigabe-Informationen) bleiben als Teil des gespeicherten AMI erhalten. Die AMI-Daten werden im Rahmen des Speicherprozesses komprimiert. AMIs die Daten enthalten, die leicht komprimiert werden können, führen zu kleineren Objekten in S3. Um die Kosten zu senken, können Sie günstigere S3-Speicherstufen verwenden. Weitere Informationen finden Sie unter Amazon-S3-Speicherklassen und Amazon-S3-Preisen

Einschränkungen

- Um ein AMI zu speichern, AWS-Konto müssen Sie entweder Eigentümer des AMI und seiner Snapshots sein, oder das AMI und seine Snapshots müssen direkt mit Ihrem Konto geteilt werden. Sie können ein AMI nicht speichern, wenn es nur öffentlich freigegeben ist.
- Nur EBS-gestützte Dateien AMIs können mit diesen gespeichert werden. APIs
- Paravirtual (PV) werden nicht unterstützt. AMIs
- Die Größe eines AMI (vor der Komprimierung), das gespeichert werden kann, ist auf 5 000 GB beschränkt.
- Kontingent für Speicher-Image-Anfragen: 1.200 GB an Speicherplatz (Snapshot-Daten) werden ausgeführt.
- Kontingent für Anfragen zur Wiederherstellung von Images: 600 GB an Wiederherstellungsarbeiten (Snapshot-Daten) werden ausgeführt.
- Für die Dauer der Speicheraufgabe dürfen die Snapshots nicht gelöscht werden und der IAM-Prinzipal, der die Speicherung durchführt, muss Zugriff auf die Snapshots haben, andernfalls schlägt der Speicherprozess fehl.
- Sie können nicht mehrere Kopien eines AMI im selben S3-Bucket erstellen.
- Ein AMI, das in einem S3-Bucket gespeichert ist, kann mit seiner ursprünglichen AMI-ID nicht wiederhergestellt werden. Sie können dies abschwächen, indem Sie AMI-Aliasingverwenden.
- Derzeit APIs werden das Speichern und Wiederherstellen nur durch die Verwendung der AWS Command Line Interface, AWS SDKs, und EC2 Amazon-API unterstützt. Sie können ein AMI nicht mit der EC2 Amazon-Konsole speichern und wiederherstellen.

Kosten

Wenn Sie AMIs mit S3 speichern und wiederherstellen, werden Ihnen die Dienste, die vom Speichern und Wiederherstellen in Anspruch genommen werden APIs, sowie die Datenübertragung in Rechnung gestellt. APIs Sie verwenden S3 und die EBS Direct API (von diesen intern für den APIs Zugriff auf die Snapshot-Daten verwendet). Weitere Informationen finden Sie unter Amazon S3 – Preise und Amazon EBS – Preise.

Funktionsweise der AMI-Speicherung- und -Wiederherstellung

Um ein AMI mit S3 zu speichern und wiederherzustellen, verwenden Sie Folgendes APIs:

- `CreateStoreImageTask` – Speichert das AMI in einem S3-Bucket

- `DescribeStoreImageTasks` – Liefert den Fortschritt der AMI-Speicheraufgabe
- `CreateRestoreImageTask` – Stellt das AMI aus einem S3-Bucket wieder her

Wie APIs funktionieren sie

- CreateStoreImageTask
- DescribeStoreImageTasks
- CreateRestoreImageTask
- Dateipfade

CreateStoreImageTask

Die `CreateStoreImageTask`-API speichert ein AMI als einzelnes Objekt in einem S3-Bucket.

Die API erstellt eine Aufgabe, die alle Daten aus dem AMI und seinen Snapshots liest und dann einen mehrteiligen S3-Upload verwendet, um die Daten in einem S3-Objekt zu speichern. Die API nimmt alle Komponenten des AMI, einschließlich der meisten AMI-Metadaten, und aller im non-Region-specific AMI enthaltenen EBS-Snapshots und packt sie in ein einziges Objekt in S3. Die Daten werden im Rahmen des Upload-Prozesses komprimiert, um den in S3 verwendeten Speicherplatz zu reduzieren, sodass das Objekt in S3 möglicherweise kleiner ist als die Summe der Größe der Snapshots im AMI.

Wenn für das Konto, das diese API aufruft, AMI- und Snapshot-Tags (Markierungen) sichtbar sind, bleiben diese erhalten.

Das Objekt in S3 hat die gleiche ID wie das AMI, jedoch mit einer `.bin`-Erweiterung. Die folgenden Daten werden auch als S3-Metadaten-Tags (Markierungen) für das S3-Objekt gespeichert: AMI-Name, AMI-Beschreibung, AMI-Registrierungsdatum, AMI-Besitzerkonto und ein Zeitstempel für den Speichervorgang.

Die Zeit, die benötigt wird, um die Aufgabe abzuschließen, hängt von der Größe des AMI ab. Dies hängt auch davon ab, wie viele andere Aufgaben ausgeführt werden, da Aufgaben in die Warteschlange gestellt werden. Sie können den Fortschritt der Aufgabe verfolgen, indem Sie die `DescribeStoreImageTasks`-API aufrufen.

Die Summe der Größen aller laufenden Dateien ist auf 1.200 GB EBS-Snapshot-Daten pro Konto begrenzt. AMIs Die weitere Aufgabenerstellung wird abgelehnt, bis die laufenden Aufgaben unter dem Grenzwert liegen. Wenn beispielsweise derzeit ein AMI mit 200 GB Snapshot-Daten und

ein anderes AMI mit 400 GB Snapshot-Daten gespeichert wird, wird eine weitere Anforderung akzeptiert, da die laufende Gesamtzahl 600 GB beträgt, was unter dem Limit liegt. Wenn jedoch derzeit ein einzelnes AMI mit 1.200 GB an Snapshot-Daten gespeichert wird, werden weitere Aufgaben zurückgewiesen, bis die Aufgabe abgeschlossen ist.

DescribeStoreImageTasks

Die `DescribeStoreImageTasks`-API beschreibt den Fortschritt der AMI-Speicheraufgaben. Sie können Aufgaben für bestimmte AMIs Aufgaben beschreiben. Wenn Sie nichts angeben AMIs, erhalten Sie eine paginierte Liste aller Store-Image-Aufgaben, die in den letzten 31 Tagen bearbeitet wurden.

Für jede AMI-Aufgabe gibt die Antwort an, ob die Aufgabe `InProgress`, `Completed` oder `Failed` ist. Bei Aufgaben `InProgress` zeigt die Antwort einen geschätzten Fortschritt in Prozent.

Aufgaben werden in umgekehrter chronologischer Reihenfolge aufgeführt.

Derzeit können nur Aufgaben des Vormonats eingesehen werden.

CreateRestoreImageTask

Die `CreateRestoreImageTask`-API startet eine Aufgabe, die ein AMI aus einem S3-Objekt wiederherstellt, das zuvor mithilfe einer `CreateStoreImageTask`-Anforderung erstellt wurde.

Die Wiederherstellungsaufgabe kann in derselben oder einer anderen Region ausgeführt werden, in der die Speicheraufgabe ausgeführt wurde.

Der S3-Bucket, aus dem das AMI-Objekt wiederhergestellt wird, muss sich in derselben Region befinden, in der die Wiederherstellungsaufgabe angefordert wird. Das AMI wird in dieser Region wiederhergestellt.

Das AMI wird mit seinen Metadaten wie dem Namen, der Beschreibung und den Blockgeräte-Zuweisungen wiederhergestellt, die den Werten des gespeicherten AMI entsprechen. Der Name muss AMIs in der Region für dieses Konto eindeutig sein. Wenn Sie keinen Namen angeben, erhält das neue AMI den gleichen Namen wie das ursprüngliche AMI. Das AMI erhält eine neue AMI-ID, die zum Zeitpunkt des Wiederherstellungsprozesses generiert wird.

Die Zeit, die zum Abschließen der AMI-Wiederherstellungsaufgabe benötigt wird, hängt von der Größe des AMI ab. Dies hängt auch davon ab, wie viele andere Aufgaben ausgeführt werden, da Aufgaben in die Warteschlange gestellt werden. Sie können den Fortschritt der Aufgabe anzeigen, indem Sie das AMI (describe-images) oder seine EBS-Snapshots (describe-snapshots) beschreiben.

Wenn die Aufgabe fehlschlägt, werden das AMI und die Snapshots in einen fehlgeschlagenen Zustand verschoben.

Die Summe der Größen aller laufenden Dateien ist auf 600 GB (basierend auf der AMIs Größe nach der Wiederherstellung) an EBS-Snapshot-Daten pro Konto begrenzt. Die weitere Aufgabenerstellung wird abgelehnt, bis die laufenden Aufgaben unter dem Grenzwert liegen.

Dateipfade

Sie können Dateipfade beim Speichern und Wiederherstellen AMIs wie folgt verwenden:

- Beim Speichern eines AMI in S3 kann der Dateipfad zum Bucket-Namen hinzugefügt werden. Intern trennt das System den Pfad vom Bucket-Namen und fügt den Pfad dann dem Objektschlüssel hinzu, der zum Speichern des AMI generiert wird. Der vollständige Objektpfad wird in der Antwort auf den API-Aufruf angezeigt.
- Da bei der Wiederherstellung des AMI ein Objektschlüsselparameter verfügbar ist, kann der Pfad am Anfang des Objektschlüsselwerts hinzugefügt werden.

Beispiel: Bucket-Name mit angehängtem Dateipfad

Wenn Sie das AMI speichern, geben Sie den Dateipfad nach dem Bucket-Namen an.

```
amzn-s3-demo-bucket/path1/path2
```

Der resultierende Objektschlüssel sieht wie folgt aus.

```
path1/path2/ami-0abcdef1234567890.bin
```

Wenn Sie das AMI wiederherstellen, geben Sie den Bucket-Namen und den Objektschlüssel an. Beispiele finden Sie unter the section called “Eine Aufgabe zum Speichern eines Images erstellen”.

Eine Aufgabe zum Speichern eines Images erstellen

Wenn Sie ein AMI in einem S3-Bucket speichern, wird eine Aufgabe zum Speichern von Images erstellt. Sie können die Aufgabe zum Speichern von Images verwenden, um den Fortschritt und das Ergebnis des Prozesses zu überwachen.

Inhalt

- Sicherung Ihrer AMIs

- Berechtigungen für das Speichern und Wiederherstellen mit S3 AMIs
- Eine Aufgabe zum Speichern eines Images erstellen
- Eine Aufgabe zum Wiederherstellen eines Images erstellen

Sicherung Ihrer AMIs

Es ist wichtig sicherzustellen, dass das S3-Bucket mit ausreichender Sicherheit konfiguriert ist, um den Inhalt des AMI zu sichern, und dass die Sicherheit so lange erhalten bleibt, wie die AMI-Objekte im Bucket verbleiben. Wenn dies nicht möglich ist, APIs wird deren Verwendung nicht empfohlen. Stellen Sie sicher, dass der öffentliche Zugriff auf den S3-Bucket nicht erlaubt ist. Wir empfehlen, die serverseitige Verschlüsselung für die S3-Buckets zu aktivieren, in denen Sie die speichern AMIs, obwohl dies nicht erforderlich ist.

Informationen zum Festlegen der geeigneten Sicherheitseinstellungen für Ihre S3-Buckets finden Sie in den folgenden Sicherheitsthemen:

- Blockieren des öffentlichen Zugriffs auf Ihren Amazon S3-Speicher
- Einstellen des Verhaltens der serverseitigen Verschlüsselung für Amazon S3-Buckets
- Welche S3-Bucket-Richtlinie kann ich verwenden, um die AWS Config Regel s3- einzuhalten? bucket-ssl-requests-only
- Aktivieren der Amazon S3-Serverzugriffsprotokollierung

Wenn die AMI-Snapshots in das S3-Objekt kopiert werden, werden die Daten danach über TLS-Verbindungen kopiert. Sie können AMIs mit verschlüsselten Snapshots speichern, aber die Snapshots werden im Rahmen des Speichervorgangs entschlüsselt.

Berechtigungen für das Speichern und Wiederherstellen mit S3 AMIs

Wenn Ihre IAM-Prinzipale AMIs mithilfe von Amazon S3 speichern oder wiederherstellen, müssen Sie ihnen die erforderlichen Berechtigungen erteilen.

Die folgende Beispielrichtlinie enthält alle Aktionen, die erforderlich sind, um einem IAM-Prinzipal die Durchführung der Speicher- und Wiederherstellungsaufgaben zu ermöglichen.

Sie können auch IAM-Richtlinien erstellen, die Prinzipalen nur Zugriff auf bestimmte Ressourcen gewähren. Weitere Beispielrichtlinien finden Sie unter Zugriffsverwaltung für AWS Ressourcen im IAM-Benutzerhandbuch.

> **Note**
>
> Wenn die Snapshots, aus denen das AMI besteht, verschlüsselt sind oder Ihr Konto standardmäßig für Verschlüsselung aktiviert ist, muss Ihr IAM-Prinzipal über die Berechtigung verfügen, den KMS-Schlüssel zu verwenden.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:PutObjectTagging",
                "s3:AbortMultipartUpload",
                "ebs:CompleteSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:ListChangedBlocks",
                "ebs:ListSnapshotBlocks",
                "ebs:PutSnapshotBlock",
                "ebs:StartSnapshot",
                "ec2:CreateStoreImageTask",
                "ec2:DescribeStoreImageTasks",
                "ec2:CreateRestoreImageTask",
                "ec2:GetEbsEncryptionByDefault",
                "ec2:DescribeTags",
                "ec2:CreateTags"
            ],
            "Resource": "*"
        }
    ]
}
```

Eine Aufgabe zum Speichern eines Images erstellen

Um ein AMI in einem S3-Bucket zu speichern, erstellen Sie zunächst eine Aufgabe zum Speichern von Images. Die Zeit, die benötigt wird, um die Aufgabe abzuschließen, hängt von der Größe des AMI ab. Sie können den Fortschritt der Aufgabe verfolgen, bis sie erfolgreich ist oder fehlschlägt.

AWS CLI

So erstellen Sie eine Aufgabe zum Speichern von Images

Verwenden Sie den Befehl create-store-image-task.

```
aws ec2 create-store-image-task \
    --image-id ami-0abcdef1234567890 \
    --bucket amzn-s3-demo-bucket
```

Es folgt eine Beispielausgabe.

```
{
  "ObjectKey": "ami-0abcdef1234567890.bin"
}
```

So beschreiben Sie den Fortschritt der Aufgabe zum Speichern von Images

Verwenden Sie den Befehl describe-store-image-tasks.

```
aws ec2 describe-store-image-tasks \
    --image-ids ami-0abcdef1234567890 \
    --query StoreImageTaskResults[].StoreTaskState \
    --output text
```

Es folgt eine Beispielausgabe.

```
InProgress
```

PowerShell

So erstellen Sie eine Aufgabe zum Speichern von Images

Verwenden Sie das cmdlet New-EC2StoreImageTask.

```
New-EC2StoreImageTask `
    -ImageId ami-0abcdef1234567890 `
    -Bucket amzn-s3-demo-bucket
```

Es folgt eine Beispielausgabe.

```
ObjectKey         : ami-0abcdef1234567890.bin
```

So beschreiben Sie den Fortschritt der Aufgabe zum Speichern von Images

Verwenden Sie das cmdlet Get-EC2StoreImageTask.

```
(Get-EC2StoreImageTask -ImageId ami-0abcdef1234567890).StoreTaskState
```

Es folgt eine Beispielausgabe.

```
InProgress
```

Eine Aufgabe zum Wiederherstellen eines Images erstellen

Sie müssen einen Namen für das wiederhergestellte AMI angeben. Der Name muss AMIs in der Region für dieses Konto eindeutig sein. Das wiederhergestellte AMI erhält eine neue AMI-ID.

AWS CLI

So erstellen Sie eine Aufgabe zum Wiederherstellen eines Images

Verwenden Sie den Befehl create-restore-image-task.

```
aws ec2 create-restore-image-task \
    --object-key ami-0abcdef1234567890.bin \
    --bucket amzn-s3-demo-bucket \
    --name "my-restored-ami"
```

Es folgt eine Beispielausgabe.

```
{
   "ImageId": "ami-1234567890abcdef0"
```

```
}
```

PowerShell

So erstellen Sie eine Aufgabe zum Wiederherstellen eines Images

Verwenden Sie das cmdlet New-EC2RestoreImageTask.

```
New-EC2RestoreImageTask `
    -ObjectKey ami-0abcdef1234567890.bin `
    -Bucket amzn-s3-demo-bucket `
    -Name "my-restored-ami"
```

Es folgt eine Beispielausgabe.

```
ImageId         : ami-1234567890abcdef0
```

Verwenden Sie AMI-Abstammung, um den Ursprung eines AMI nachzuverfolgen

AMI-Abstammung hilft Ihnen dabei, den Ursprung eines AMI nachzuvollziehen, indem es die IDs und Regionen aller seiner Vorfahren AMIs zurückgibt. Wenn Sie ein AMI erstellen oder kopieren, behält das neue AMI die ID und Region seines Quell-AMI (übergeordnetes AMI) bei. Auf diese Weise können Sie die Kette bis AMIs zum Root-AMI verfolgen.

Wichtigste Vorteile

Die Verwendung von AMI ancestry hilft Ihnen:

- Verfolgen Sie AMI-Derivate, um die Einhaltung interner Richtlinien sicherzustellen.
- Identifizieren Sie potenziell anfällig AMIs , wenn ein Sicherheitsproblem in einem Vorgänger-AMI gefunden wird.
- Behalten Sie den Überblick über die AMI-Ursprünge in mehreren Regionen.

Themen

- So funktioniert AMI ancestry

- Überlegungen
- AMI-Abstammung anzeigen
- Das Quell-AMI identifizieren

So funktioniert AMI ancestry

Die AMI-Abstammung identifiziert das übergeordnete AMI, mit dem das angegebene AMI erstellt wurde, das übergeordnete AMI usw., bis hin zum Root-AMI. Funktionsweise:

- Jedes AMI zeigt die ID und Region seines Quell-AMI (übergeordnetes) AMI an.
- Beginnend mit Ihrem ausgewählten AMI werden in der Liste der Abstammungseinträge die einzelnen übergeordneten AMI nacheinander angezeigt.
- Die Liste der Abstammungseinträge reicht zurück, bis sie das Root-AMI erreicht. Das Root-AMI ist eines der folgenden:
  - Ein öffentliches AMI von einem verifizierten Anbieter (identifiziert durch seinen Eigentümeralias, der entweder `amazon` oder lautet`aws-marketplace`).
  - Ein AMI ohne aufgezeichneten Vorfahren. Wenn Sie beispielsweise verwenden, RegisterImageum ein AMI direkt aus einer Reihe von Snapshots zu erstellen, gibt es kein Quell-AMI, das verfolgt werden kann, anders als bei der Erstellung eines AMI aus einer Instance.
  - Ein AMI, dessen Quell-AMI von einer anderen Partition stammt.
  - Das 50. AMI in der Liste. Die maximale Anzahl von AMIs in einer Abstammungsliste ist 50.

Überlegungen

- Die ID und Region des Quell-AMI sind nur für die AMIs Erstellung mit CreateImageCopyImage, oder verfügbar CreateRestoreImageTask.
- Bei AMIs Created using CreateImage(erstellt ein AMI aus einer Instance) ist die Quell-AMI-ID die ID des AMI, das zum Starten der Instance verwendet wurde.
- Die AMI-Quellinformationen sind nicht verfügbar für:
  - AMIs erstellt mit RegisterImage, weil sie aus Snapshots erstellt wurden.
  - Für einige ältere AMIs.
- Die AMI-Quellinformationen bleiben erhalten, wenn:
  - AMIs werden regionsübergreifend kopiert.
  - Quellen AMIs sind deregistriert (gelöscht).

  - Sie haben keinen Zugriff auf die Quelle. AMIs
- Jede Abstammungsliste ist auf 50 AMIs begrenzt.

AMI-Abstammung anzeigen

Sie können die Herkunft eines AMIs mit den folgenden Methoden anzeigen.

Console

So zeigen Sie die Herkunft eines AMI an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich AMIs aus.
3. Wählen Sie ein AMI aus und klicken Sie auf die Registerkarte AMI-Herkunft.
4. In der Tabelle mit den AMI-Abstammungseinträgen sind alle AMIs in der Abstammungsliste enthaltenen Einträge aufgeführt.

   - AMI-ID — Die Kennung jedes AMI in der Abstammungsliste. Der erste Eintrag in der Tabelle ist das ausgewählte AMI, gefolgt von seinen Vorfahren.
   - Quell-AMI-ID — Die ID des AMI, aus dem das AMI in der AMI-ID-Spalte erstellt wurde. Ein Bindestrich (-) zeigt das Ende der AMI-Abstammungsliste an.
   - Quell-AMI-Region — Der AWS-Region Ort, an dem sich das Quell-AMI befindet.
   - Abstammungsebene — Die Position in der Abstammungsliste, wobei:
     - 0 (Eingabe-AMI) gibt das ausgewählte AMI an, dessen Herkunft Sie wissen möchten.
     - Zunehmende Zahlen zeigen ältere Vorfahren.
     - ***n***(originales AMI) gibt das Stamm-AMI an, wobei die Zahl angibt, wie weit die Abstammungsliste zurückreicht.
   - Erstellungsdatum — Datum, an dem das AMI erstellt wurde, im UTC-Format.
   - Eigentümer-Alias — Der Alias des AMI-Besitzers (z. B.`amazon`). Ein Bindestrich (-) gibt an, dass das AMI keinen Besitzer-Alias hat.

AWS CLI

So zeigen Sie die Herkunft eines AMI an

Verwenden Sie den Befehl get-image-ancestry und geben Sie die AMI-ID an.

```
aws ec2 get-image-ancestry \
    --image-id ami-1111111111EXAMPLE \
    --region us-east-1
```

Es folgt eine Beispielausgabe. Die Ausgabe wird AMIs in der Reihenfolge der Herkunft aufgeführt: Der erste Eintrag ist das angegebene (Eingabe-) AMI, gefolgt von seinem übergeordneten AMI, dem übergeordneten und so weiter, und endet mit dem Stamm-AMI.

```
{
    "ImageAncestryEntries": [
        {
            "CreationDate": "2025-01-17T18:37:50.000Z",
            "ImageId": "ami-1111111111EXAMPLE", // Input AMI
            "SourceImageId": "ami-2222222222EXAMPLE",
            "SourceImageRegion": "us-east-1"

        },
        {
            "CreationDate": "2025-01-17T18:37:50.000Z",
            "ImageId": "ami-2222222222EXAMPLE", // Parent AMI
            "SourceImageId": "ami-3333333333EXAMPLE",
            "SourceImageRegion": "us-east-1"
        },
        ...
        {
            "CreationDate": "2025-01-17T18:37:50.000Z",
            "ImageId": "ami-8888888888EXAMPLE", // Root AMI
            "ImageOwnerAlias": "aws-marketplace",
            "SourceImageId": "ami-9999999999EXAMPLE",
            "SourceImageRegion": "us-east-2"
        }
    ]
}
```

PowerShell

So zeigen Sie die Herkunft eines AMI an

Verwenden Sie das cmdlet Get-EC2ImageAncestry.

```
Get-EC2ImageAncestry -ImageId ami-1111111111EXAMPLE
```

Es folgt eine Beispielausgabe. Die Ausgabe wird AMIs in der Reihenfolge der Herkunft aufgeführt: Der erste Eintrag ist das angegebene (Eingabe-) AMI, gefolgt von seinem übergeordneten AMI, dem übergeordneten und so weiter, und endet mit dem Stamm-AMI.

```
ImageAncestryEntries : {
    @{
        CreationDate = "2025-01-17T18:37:50.000Z"
        ImageId = "ami-1111111111EXAMPLE"    # Input AMI
        SourceImageId = "ami-2222222222EXAMPLE"
        SourceImageRegion = "us-east-1"
    },
    @{
        CreationDate = "2025-01-17T18:37:50.000Z"
        ImageId = "ami-2222222222EXAMPLE"    # Parent AMI
        SourceImageId = "ami-3333333333EXAMPLE"
        SourceImageRegion = "us-east-1"
    },
    ...
    @{
        CreationDate = "2025-01-17T18:37:50.000Z"
        ImageId = "ami-8888888888EXAMPLE"    # Root AMI
        ImageOwnerAlias = "aws-marketplace"
        SourceImageId = "ami-9999999999EXAMPLE"
        SourceImageRegion = "us-east-2"
    }
}
```

Das Quell-AMI identifizieren

Wenn Sie nur das unmittelbar übergeordnete (Quell-) AMI identifizieren müssen, das zur Erstellung eines AMI verwendet wurde, können Sie die folgenden Methoden verwenden.

Console

Um das Quell-AMI zu identifizieren, das zur Erstellung des ausgewählten AMI verwendet wurde

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich AMIs aus.
3. Wählen Sie dias AMI aus, um seine Details anzuzeigen.

Die Quell-AMI-Informationen werden in den folgenden Feldern angezeigt: Quell-AMI-ID und Quell-AMI-Region

AWS CLI

Um das Quell-AMI zu identifizieren, das zur Erstellung des angegebenen AMI verwendet wurde

Verwenden Sie den Befehl describe-images.

```
aws ec2 describe-images \
    --region us-east-1 \
    --image-ids ami-0abcdef1234567890 \
    --query "Images[].{ID:SourceImageId,Region:SourceImageRegion}"
```

Es folgt eine Beispielausgabe.

```
[
    {
        "ID": "ami-0abcdef1234567890",
        "Region": "us-west-2"
    }
}
```

PowerShell

Um das Quell-AMI zu identifizieren, das zur Erstellung des angegebenen AMI verwendet wurde

Verwenden Sie das cmdlet Get-EC2Image.

```
Get-EC2Image -ImageId ami-0abcdef1234567890 | Select SourceImageId,
 SourceImageRegion
```

Es folgt eine Beispielausgabe.

```
SourceImageId           SourceImageRegion
-------------           -----------------
ami-0abcdef1234567890 us-west-2
```

Verwaltung und Überwachung der AMI-Nutzung

AWS bietet mehrere Funktionen, mit denen Sie Ihre AMI-Nutzung effektiv verwalten und überwachen können. Sie können nachverfolgen, welche Konten Ihr geteiltes Konto verwenden AMIs, ermitteln, wann Sie zuletzt verwendet AMIs wurden, und herausfinden, auf welche Ressourcen in Ihrem AWS-Konto Konto spezifisch AMIs verwiesen wird.

Die folgende Tabelle bietet einen Überblick über die Features für die Verwaltung und Überwachung der AMI-Nutzung:

Feature	Anwendungsfall	Wichtigste Vorteile
AMI-Nutzungsberichte	Verschaffen Sie AWS-Konten sich einen Überblick darüber, wer Ihr AMI verwendet AMIs und wie häufig jedes AMI verwendet wird.	• Identifizieren Sie die Ressourcentypen AWS-Konten und die Ressource ntypen, auf die Sie verweisen, AMIs damit Sie sich sicher abmelden oder deaktivieren können. AMIs • Identifizieren Sie ungenutzt e Dateien AMIs für die Abmeldung, um die Speicherkosten zu senken. • Identifizieren Sie die am häufigsten verwendeten. AMIs
Nachverfolgung der letzten Verwendung	Überprüfen Sie, wann Ihr AMI zuletzt verwendet wurde.	• Identifizieren Sie ungenutzt e, AMIs damit Sie sich sicher abmelden können AMIs. •

Feature	Anwendungsfall	Wichtigste Vorteile
		Identifizieren Sie ungenutzte Dateien AMIs für die Abmeldung, um die Lagerkosten zu senken.
AMI-Referenzprüfung	Stellen Sie sicher, dass Ihre AWS Ressourcen die neuesten kompatiblen Versionen verwenden. AMIs	• Prüfen Sie die Verwendung von AMIs in Ihrem Konto. • Prüfen Sie, wo AMIs auf bestimmte verwiesen wird. • Sorgen Sie für die Einhaltung der Vorschriften, indem Sie Ihre Ressourcen auf den neuesten Stand bringenAMIs.

Themen

- Ihre AMI-Nutzung anzeigen
- Prüfen Sie, wann ein Amazon EC2 AMI zuletzt verwendet wurde
- Identifizieren Sie den angegebenen Verweis auf Ihre Ressourcen AMIs

Ihre AMI-Nutzung anzeigen

Wenn Sie Ihre Amazon Machine Images (AMIs) für andere AWS-Konten freigeben – sei es für bestimmte AWS-Konten, Organisationen, Organisationseinheiten (OUs) oder öffentlich – können Sie anhand von AMI-Nutzungsberichten sehen, wie diese AMIs verwendet werden. Die Berichte bieten Einblick in:

- Welche AWS-Konten Ihre AMIs in EC2-Instances oder Startvorlagen verwenden
- Wie viele EC2-Instances oder Startvorlagen auf jedes AMI verweisen

AMI-Nutzungsberichte unterstützen Sie dabei, Ihre AMIs effektiver zu verwalten, indem sie Ihnen helfen:

- Die AWS-Konten und Ressourcentypen zu identifizieren, die auf Ihre AMIs verweisen, sodass Sie AMIs sicher abmelden oder deaktivieren können.
- Ungenutzte AMIs für die Abmeldung zu identifizieren, um die Speicherkosten zu senken.
- Ihre am häufigsten verwendeten AMIs zu identifizieren.

Inhalt

- So funktionieren AMI-Nutzungsberichte
- Einen AMI-Nutzungsbericht erstellen
- AMI-Nutzungsberichte anzeigen
- Einen AMI-Nutzungsbericht löschen
- Berichtskontingente

So funktionieren AMI-Nutzungsberichte

Beim Erstellen eines AMI-Nutzungsberichts geben Sie Folgendes an:

- Das AMI, über das berichtet werden soll.
- Das zu überprüfende AWS-Konten (bestimmte Konten oder alle Konten).
- Die zu prüfenden Ressourcentypen (EC2-Instances, Startvorlagen oder beides).
- Bei Startvorlagen die Anzahl der zu überprüfenden Versionen (standardmäßig die 20 neuesten Versionen).

Amazon EC2 erstellt einen separaten Bericht für jedes AMI. Jeder Bericht enthält:

- Eine Liste der AWS-Konten, die das AMI benutzen.
- Eine Anzahl der Ressourcen, die auf das AMI verweisen, nach Ressourcentyp pro Konto. Beachten Sie, dass bei Startvorlagen die Anzahl nur 1 beträgt, wenn in mehreren Versionen einer Startvorlage auf ein AMI verwiesen wird.

> **Important**
>
> Wenn Sie einen AMI-Nutzungsbericht generieren, enthält er möglicherweise nicht die neuesten Aktivitäten. Instance-Aktivitäten der letzten 24 Stunden und Aktivitäten zum Starten von Vorlagen der letzten Tage werden möglicherweise nicht im Bericht angezeigt.

Amazon EC2 löscht einen Bericht 30 Tage nach der Erstellung automatisch. Sie können Berichte über die EC2-Konsole herunterladen, um sie lokal zu speichern.

Einen AMI-Nutzungsbericht erstellen

Um zu sehen, wie Ihr AMI verwendet wird, müssen Sie zunächst einen AMI-Nutzungsbericht erstellen, in dem Sie die Konten und Ressourcentypen angeben, über die berichtet werden soll. Nachdem der Bericht erstellt wurde, können Sie den Inhalt des Berichts anzeigen. Sie können den Bericht auch über die EC2-Konsole herunterladen.

Console

So erstellen Sie einen AMI-Nutzungsbericht

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie ein AMI aus und wählen Sie dann Aktionen, AMI-Nutzung, Meine AMI-Nutzung anzeigen.
4. Führen Sie auf der Seite Meinen AMI-Nutzungsbericht erstellen die folgenden Schritte aus:
   a. Wählen Sie unter Ressourcentypen einen oder mehrere Ressourcentypen aus, über die ein Bericht erstellt werden soll.
   b. Führen Sie unter Konto eine der folgenden Aktionen aus:
      - Wählen Sie Konto-IDs angeben und anschließend für jedes Konto, über das ein Bericht erstellt werden soll, die Option Konto-ID hinzufügen aus.
      - Wählen Sie Alle Konten einbeziehen, um Berichte über alle Konten zu erstellen.
   c. Wählen Sie Meinen AMI-Nutzungsbericht erstellen aus.
5. Wählen Sie auf der AMI-Seite die Registerkarte Meine AMI-Nutzung aus.
6. Wählen Sie eine Bericht-ID aus, um dessen Details anzuzeigen.

AWS CLI

So erstellen Sie einen AMI-Nutzungsbericht für eine Liste von Konten

Verwenden Sie den Befehl create-image-usage-report mit den folgenden erforderlichen Parametern:

- `--image-id` – Die ID des AMI, über das berichtet werden soll.
- `--resource-types` – Die Ressourcentypen, die überprüft werden sollen. Im folgenden Beispiel handelt es sich bei den zu prüfenden Ressourcentypen um EC2-Instances und Startvorlagen. Darüber hinaus wird auch die Anzahl der zu überprüfenden Versionen der Startvorlagen angegeben (`version-depth=100`).

Um Berichte über bestimmte Konten zu erstellen, verwenden Sie den Parameter `--account-ids`, um die ID der einzelnen Konten anzugeben, für die ein Bericht erstellt werden soll.

```
aws ec2 create-image-usage-report \
    --image-id ami-0abcdef1234567890 \
    --account-ids 111122223333 444455556666 123456789012 \
    --resource-types ResourceType=ec2:Instance \
      'ResourceType=ec2:LaunchTemplate,ResourceTypeOptions=[{OptionName=version-
depth,OptionValues=100}]'
```

So erstellen Sie einen AMI-Nutzungsbericht für alle Konten

Um Berichte über alle Konten zu erstellen, die das angegebene AMI verwenden, verwenden Sie denselben Befehl, lassen Sie jedoch den Parameter `--account-ids` weg.

```
aws ec2 create-image-usage-report \
    --image-id ami-0abcdef1234567890 \
    --resource-types ResourceType=ec2:Instance \
      'ResourceType=ec2:LaunchTemplate,ResourceTypeOptions=[{OptionName=version-
depth,OptionValues=100}]'
```

Es folgt eine Beispielausgabe.

```
{
    "ReportId": "amiur-00b877d192f6b02d0"
}
```

So überwachen Sie den Status der Berichterstellung

Verwenden Sie den Befehl describe-image-usage-reports und geben Sie die Berichts-ID an.

```
aws ec2 describe-image-usage-reports --report-ids amiur-00b877d192f6b02d0
```

Es folgt eine Beispielausgabe. Der Anfangswert für das `State`-Feld ist `pending`. Um die Berichtseinträge anzeigen zu können, muss der Status `available` sein.

```
{
    "ImageUsageReports": [
        {
            "ImageId": "ami-0e9ae3dc21c2b3a64",
            "ReportId": "amiur-abcae3dc21c2b3999",
            "ResourceTypes": [
                {"ResourceType": "ec2:Instance"}
            ],
            "State": "pending",
            "CreationTime": "2025-09-29T13:27:12.322000+00:00",
            "ExpirationTime": "2025-10-28T13:27:12.322000+00:00"
        }
    ]
}
```

PowerShell

So erstellen Sie einen AMI-Nutzungsbericht für eine Liste von Konten

Verwenden Sie das cmdlet New-EC2ImageUsageReport mit den folgenden erforderlichen Parametern:

- `-ImageId` – Die ID des AMI, über das berichtet werden soll.
- `-ResourceType` – Die Ressourcentypen, die überprüft werden sollen. Im folgenden Beispiel handelt es sich bei den zu prüfenden Ressourcentypen um EC2-Instances und Startvorlagen. Darüber hinaus wird auch die Anzahl der zu überprüfenden Versionen der Startvorlagen angegeben (`'version-depth' = 100`).

Um Berichte über bestimmte Konten zu erstellen, verwenden Sie den Parameter `-AccountId`, um die ID der einzelnen Konten anzugeben, für die ein Bericht erstellt werden soll.

```
New-EC2ImageUsageReport `
```

```
    -ImageId ami-0abcdef1234567890 `
    -AccountId 111122223333 444455556666 123456789012 `
    -ResourceType @(
        @{ResourceType = 'ec2:Instance'},
        @{ResourceType = 'ec2:LaunchTemplate'ResourceTypeOptions = @{'version-depth'
 = 100}
        })
```

So erstellen Sie einen AMI-Nutzungsbericht für alle Konten

Um Berichte über alle Konten zu erstellen, die das angegebene AMI verwenden, verwenden Sie denselben Befehl, lassen Sie jedoch den Parameter `-AccountId` weg.

```
New-EC2ImageUsageReport `
    -ImageId ami-0abcdef1234567890 `
    -ResourceType @(
        @{ResourceType = 'ec2:Instance'},
        @{ResourceType = 'ec2:LaunchTemplate'ResourceTypeOptions = @{'version-depth'
 = 100}
        })
```

Es folgt eine Beispielausgabe.

```
ReportId
--------
amiur-00b877d192f6b02d0
```

So überwachen Sie den Status der Berichterstellung

Verwenden Sie den Befehl Get-EC2ImageUsageReport und geben Sie die Bericht-ID an.

```
Get-EC2ImageUsageReport -ReportId amiur-00b877d192f6b02d0
```

Es folgt eine Beispielausgabe. Der Anfangswert für das `State`-Feld ist `pending`. Um die Berichtseinträge anzeigen zu können, muss der Status `available` sein.

```
ImageUsageReports
-----------------
{@{ImageId=ami-0e9ae3dc21c2b3a64; ReportId=amiur-abcae3dc21c2b3999;
 ResourceTypes=System.Object[]; State=pending; CreationTime=2025-09-29;
 ExpirationTime=2025-10-28}}
```

AMI-Nutzungsberichte anzeigen

Sie können alle Nutzungsberichte anzeigen, die Sie in den letzten 30 Tagen für ein AMI erstellt haben. Amazon EC2 löscht einen Bericht 30 Tage nach der Erstellung automatisch.

Für jeden Bericht können Sie die AWS-Konten sehen, die das AMI verwenden, und für jedes Konto die Anzahl der Ressourcen, die auf das AMI verweisen, nach Ressourcentyp. Sie können auch sehen, wann die Erstellung des Berichts initiiert wurde. Diese Informationen sind nur verfügbar, wenn sich der Bericht im Status Vollständig (Konsole) oder `available` (AWS CLI) befindet.

> **Important**
>
> Wenn Sie einen AMI-Nutzungsbericht generieren, enthält er möglicherweise nicht die neuesten Aktivitäten. Instance-Aktivitäten der letzten 24 Stunden und Aktivitäten zum Starten von Vorlagen der letzten Tage werden möglicherweise nicht im Bericht angezeigt.

Console

So zeigen Sie einen AMI-Nutzungsbericht an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie ein AMI aus.
4. Wählen Sie die Registerkarte Meine Nutzungsberichte.

   Die Berichtsliste zeigt:

   - Alle Berichte, die in den letzten 30 Tagen für das ausgewählte AMI generiert wurden.
   - Für jeden Bericht wird in der Spalte Zeit der Berichtsinitiierung das Datum angezeigt, an dem der Bericht erstellt wurde.
5. Wählen Sie die ID eines Berichts, um dessen Inhalt anzuzeigen.
6. Um auf der Seite mit den AMI-Details zur Registerkarte Meine Nutzungsberichte zurückzukehren, wählen Sie Alle Berichte für dieses AMI anzeigen aus.

AWS CLI

So listen Sie alle AMI-Nutzungsberichte für das angegebene AMI auf

Verwenden Sie den Befehl describe-image-usage-reports und geben Sie die ID des AMI an, um eine Liste seiner Berichte abzurufen.

```
aws ec2 describe-image-usage-reports --image-ids ami-0abcdef1234567890
```

Es folgt eine Beispielausgabe. Jede Berichts-ID wird zusammen mit den Ressourcentypen, die gescannt wurden, sowie den Erstellungs- und Ablaufdaten des Berichts aufgeführt. Anhand dieser Informationen können Sie die Berichte identifizieren, deren Einträge Sie anzeigen möchten.


```
{
  "ImageUsageReports": [
    {
      "ImageId": "ami-0abcdef1234567890",
      "ReportId": "amiur-1111111111111111",
      "ResourceTypes": [
        {
          "ResourceType": "ec2:Instance"
        }
      ],
      "State": "available",
      "CreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ExpirationTime": "2025-10-28T13:27:12.322000+00:00",
      "Tags": []
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ReportId": "amiur-2222222222222222",
      "ResourceTypes": [
        {
          "ResourceType": "ec2:Instance"
        },
        {
          "ResourceType": "ec2:LaunchTemplate"
        }
      ],
      "State": "available",
      "CreationTime": "2025-10-01T13:27:12.322000+00:00",
      "ExpirationTime": "2025-10-30T13:27:12.322000+00:00",
      "Tags": []
    }
  ],
  "NextToken": "opaque"
```

```
}
```

So zeigen Sie den Inhalt eines AMI-Nutzungsberichts für das angegebene AMI an

Verwenden Sie den Befehl describe-image-usage-report-entries und geben Sie die ID des AMI an. Die Antwort gibt alle Berichte für das angegebene AMI zurück und zeigt die Konten, die das AMI verwendet haben, und deren Ressourcenanzahl.

```
aws ec2 describe-image-usage-report-entries --image-ids ami-0abcdef1234567890
```

Es folgt eine Beispielausgabe.

```
{
  "ImageUsageReportEntries": [
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:Instance",
      "AccountId": "123412341234",
      "UsageCount": 15,
      "ReportCreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ReportId": "amiur-1111111111111111"
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:Instance",
      "AccountId": "123412341234",
      "UsageCount": 2,
      "ReportCreationTime": "2025-10-01T13:27:12.322000+00:00",
      "ReportId": "amiur-2222222222222222"
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:Instance",
      "AccountId": "001100110011",
      "UsageCount": 39,
      "ReportCreationTime": "2025-10-01T13:27:12.322000+00:00",
      "ReportId": "amiur-2222222222222222"
    }
  ],
  "NextToken": "opaque"
}
```

So zeigen Sie den Inhalt eines AMI-Nutzungsberichts für den angegebenen Bericht an

Verwenden Sie den Befehl describe-image-usage-report-entries und geben Sie die ID des Berichts an. Die Antwort gibt alle Einträge für den angegebenen Bericht zurück und zeigt die Konten, die das AMI verwendet haben, und deren Ressourcenanzahl.

```
aws ec2 describe-image-usage-report-entries --report-ids amiur-1111111111111111
```

Es folgt eine Beispielausgabe.

```
{
  "ImageUsageReportEntries": [
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:Instance",
      "AccountId": "123412341234",
      "UsageCount": 15,
      "ReportCreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ReportId": "amiur-1111111111111111"
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:LaunchTemplate",
      "AccountId": "123412341234",
      "UsageCount": 4,
      "ReportCreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ReportId": "amiur-1111111111111111"
    },
    {
      "ImageId": "ami-0abcdef1234567890",
      "ResourceType": "ec2:LaunchTemplate",
      "AccountId": "001100110011",
      "UsageCount": 2,
      "ReportCreationTime": "2025-09-29T13:27:12.322000+00:00",
      "ReportId": "amiur-1111111111111111"
    }
  ],
  "NextToken": "opaque"
}
```

PowerShell

So listen Sie alle AMI-Nutzungsberichte für das angegebene AMI auf

Verwenden Sie das cmdlet Get-EC2ImageUsageReport und geben Sie die ID des AMI an, um eine Liste seiner Berichte abzurufen.

```
Get-EC2ImageUsageReport -ImageId ami-0abcdef1234567890
```

Es folgt eine Beispielausgabe. Jede Berichts-ID wird zusammen mit den Ressourcentypen, die gescannt wurden, sowie den Erstellungs- und Ablaufdaten des Berichts aufgeführt. Anhand dieser Informationen können Sie die Berichte identifizieren, deren Einträge Sie anzeigen möchten.

```
@{
    ImageUsageReports = @(
        @{
            ImageId = "ami-0abcdef1234567890"
            ReportId = "amiur-1111111111111111"
            ResourceTypes = @(
                @{
                    ResourceType = "ec2:Instance"
                }
            )
            State = "available"
            CreationTime = "2025-09-29T13:27:12.322000+00:00"
            ExpirationTime = "2025-10-28T13:27:12.322000+00:00"
        },
        @{
            ImageId = "ami-0abcdef1234567890"
            ReportId = "amiur-2222222222222222"
            ResourceTypes = @(
                @{
                    ResourceType = "ec2:Instance"
                }
            )
            State = "available"
            CreationTime = "2025-09-30T13:27:12.322000+00:00"
            ExpirationTime = "2025-10-29T13:27:12.322000+00:00"
        },
        @{
            ImageId = "ami-0abcdef1234567890"
            ReportId = "amiur-3333333333333333"
            ResourceTypes = @(
                @{
                    ResourceType = "ec2:Instance"
                }
            )
```

```
            State = "available"
            CreationTime = "2025-10-01T13:27:12.322000+00:00"
            ExpirationTime = "2025-10-30T13:27:12.322000+00:00"
        }
    )
    NextToken = "opaque"
}
```

So zeigen Sie den Inhalt eines AMI-Nutzungsberichts für das angegebene AMI an

Verwenden Sie das cmdlet Get-EC2ImageUsageReportEntry und geben Sie die ID des AMI an. Die Antwort gibt alle Berichte für das angegebene AMI zurück und zeigt die Konten, die das AMI verwendet haben, und deren Ressourcenanzahl.

```
Get-EC2ImageUsageReportEntry -ImageId ami-0abcdef1234567890
```

Es folgt eine Beispielausgabe.

```
ImageUsageReportEntries : {@{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:Instance"
    AccountId = "123412341234"
    UsageCount = 15
    ReportCreationTime = "2025-09-29T13:27:12.322000+00:00"
    ReportId = "amiur-1111111111111111"
    }, @{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:Instance"
    AccountId = "123412341234"
    UsageCount = 7
    ReportCreationTime = "2025-09-30T13:27:12.322000+00:00"
    ReportId = "amiur-2222222222222222"
    }...}
NextToken : opaque
```

So zeigen Sie den Inhalt eines AMI-Nutzungsberichts für den angegebenen Bericht an

Verwenden Sie das cmdlet Get-EC2ImageUsageReportEntry und geben Sie die ID des Berichts an. Die Antwort gibt alle Einträge für den angegebenen Bericht zurück und zeigt die Konten, die das AMI verwendet haben, und deren Ressourcenanzahl.

```
Get-EC2ImageUsageReportEntry -ReportId amiur-1111111111111111
```

Es folgt eine Beispielausgabe.

```
ImageUsageReportEntries : {@{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:Instance"
    AccountId = "123412341234"
    UsageCount = 15
    ReportCreationTime = "2025-09-29T13:27:12.322000+00:00"
    ReportId = "amiur-11111111111111111"
    }, @{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:LaunchTemplate"
    AccountId = "123412341234"
    UsageCount = 4
    ReportCreationTime = "2025-09-29T13:27:12.322000+00:00"
    ReportId = "amiur-11111111111111111"
    }, @{
    ImageId = "ami-0abcdef1234567890"
    ResourceType = "ec2:LaunchTemplate"
    AccountId = "************"
    UsageCount = 2
    ReportCreationTime = "2025-09-29T13:27:12.322000+00:00"
    ReportId = "amiur-11111111111111111"
    }}
NextToken : opaque
```

Einen AMI-Nutzungsbericht löschen

Amazon EC2 löscht einen Bericht 30 Tage nach der Erstellung automatisch. Sie können ihn vor diesem Zeitpunkt manuell löschen.

Console

So löschen Sie einen AMI-Nutzungsbericht

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie ein AMI aus.

4. Wählen Sie die Registerkarte Meine AMI-Nutzung.
5. Wählen Sie das Optionsfeld neben dem Bericht aus, den Sie löschen möchten, und wählen Sie dann Löschen.

AWS CLI

So löschen Sie einen AMI-Nutzungsbericht

Verwenden Sie den Befehl delete-image-usage-report und geben Sie die ID des Berichts an.

```
aws ec2 delete-image-usage-report --report-id amiur-0123456789abcdefg
```

PowerShell

So löschen Sie einen AMI-Nutzungsbericht

Verwenden Sie das cmdlet Remove-EC2ImageUsageReport und geben Sie die ID des Berichts an.

```
Remove-EC2ImageUsageReport -ReportId amiur-0123456789abcdefg
```

Berichtskontingente

Die folgenden Kontingente gelten für die Erstellung von AMI-Nutzungsberichten. Die Kontingente gelten pro AWS-Region.

Beschreibung	Kontingent
In Bearbeitung (`pending`) AMI-Nutzungsberichte pro AWS-Konto	100
In Bearbeitung (`pending`) AMI-Nutzungsberichte pro AMI	1

Prüfen Sie, wann ein Amazon EC2 AMI zuletzt verwendet wurde

Amazon verfolgt EC2 automatisch das Datum und die Uhrzeit, an dem ein AMI zuletzt zum Starten einer Instance verwendet wurde. Wenn Sie über ein AMI verfügen, das lange Zeit nicht mehr zum

Starten einer Instance verwendet wurde, sollten Sie überlegen, ob das AMI für eine Abmeldung oder Veraltung geeignet ist.

Überlegungen

- Wenn ein AMI verwendet wird, um eine Instance zu starten, kommt es zu einer Verzögerung von 24 Stunden, bevor diese Nutzung gemeldet wird.
- Sie müssen der Eigentümer der AMI sein, um die letzte Startzeit zu erfahren.
- AMI-Nutzungsdaten sind ab April 2017 verfügbar.

Console

Uhrzeit des letzten Starts eines AMI anzeigen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option AMIs aus.
3. Wählen Sie in der Filterleiste Owned by me (In meinem Besitz) aus.
4. Aktivieren Sie das Kontrollkästchen für das AMI.
5. Suchen Sie auf der Registerkarte Details nach Uhrzeit des letzten Starts.

AWS CLI

So zeigen Sie die letzte Startzeit an, indem Sie das AMI beschreiben

Verwenden Sie den Befehl describe-images. Falls `LastLaunchedTime` nicht in der Ausgabe vorhanden ist, stellen Sie sicher, dass Sie Eigentümer des AMI sind.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query Images[].LastLaunchedTime \
    --output text
```

Es folgt eine Beispielausgabe.

```
2025-02-17T20:22:19Z
```

So zeigen Sie die Uhrzeit des letzten Starts eines AMI an

Verwenden Sie den Befehl describe-image-attribute. Sie müssen Eigentümer des angegebenen AMI sein.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute lastLaunchedTime \
    --query LastLaunchedTime.Value \
    --output text
```

Es folgt eine Beispielausgabe.

```
2025-02-17T20:22:19Z
```

PowerShell

So zeigen Sie die letzte Startzeit an, indem Sie das AMI beschreiben

Verwenden Sie das cmdlet Get-EC2Image. Falls `LastLaunchedTime` nicht in der Ausgabe vorhanden ist, stellen Sie sicher, dass Sie Eigentümer des AMI sind.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).LastLaunchedTime
```

Es folgt eine Beispielausgabe.

```
2025-02-17T20:22:19Z
```

So zeigen Sie die Uhrzeit des letzten Starts eines AMI an

Verwenden Sie das cmdlet Get-EC2ImageAttribute. Sie müssen Eigentümer des angegebenen AMI sein.

```
(Get-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute LastLaunchedTime).LastLaunchedTime
```

Es folgt eine Beispielausgabe.

```
2025-02-17T20:22:19Z
```

Identifizieren Sie den angegebenen Verweis auf Ihre Ressourcen AMIs

Sie können Ihre AWS Ressourcen identifizieren, die auf bestimmte Amazon Machine Images (AMIs) verweisen, unabhängig davon, ob sie öffentlich oder privat AMIs sind oder wem sie gehören. Durch diese Transparenz können Sie sicherstellen, dass Ihre Ressourcen die neuesten konformen Daten verwenden AMIs.

Wichtigste Vorteile

Die Überprüfung der AMI-Referenzen hilft Ihnen:

- Prüfen Sie die Verwendung von AMIs in Ihrem Konto.
- Prüfen Sie, wo AMIs auf bestimmte verwiesen wird.
- Sorgen Sie für die Einhaltung der Vorschriften, indem Sie Ihre Ressourcen auf den neuesten Stand bringenAMIs.

Themen

- Unterstützte Ressourcen
- So funktionieren AMI-Referenzprüfungen
- Erforderliche IAM-Berechtigungen
- Schritte zur Überprüfung von AMI-Referenzen

Unterstützte Ressourcen

AMI-Referenzen können in den Folgenden überprüft werden:

- EC2 Instanzen
- Startvorlagen
- SSM-Parameter
- Image-Rezepte von Image Builder
- Container-Rezepte von Image Builder

So funktionieren AMI-Referenzprüfungen

Grundlegender Vorgang

Wenn Sie eine AMI-Referenzprüfung durchführen, gehen Sie wie folgt vor:

- Geben Sie AMIs an, welche überprüft werden sollen.
- Wählen Sie aus, welche Ressourcentypen gescannt werden sollen.
- Sie erhalten eine Liste Ihrer Ressourcen, die auf die angegebenen Ressourcen verweisen AMIs.

Auswahl des Ressourcentyps

In der Konsole wählen Sie die Ressourcentypen aus, die gescannt werden sollen.

In der CLI geben Sie die zu scannenden Ressourcentypen mit einem oder beiden der folgenden CLI-Parameter an:

- `IncludeAllResourceTypes`: Scannt alle unterstützten Ressourcentypen.
- `ResourceTypes`: Scannt die angegebenen Ressourcentypen.

Umfang der Antworten

Sie können die Antwort auf EC2 Instances und Startvorlagen eingrenzen, indem Sie die `ResourceTypeOptions` Werte mithilfe des `ResourceTypes` Parameters anpassen. Sowohl die Konsole als auch der `IncludeAllResourceTypes`-Parameter verwenden Standardoptionswerte. Wenn `ResourceTypes` und `IncludeAllResourceTypes` zusammen verwendet werden, haben die `ResourceTypes`-Optionswerte Vorrang vor den Standardwerten.

Die Standardwerte lauten wie folgt:

Ressourcentyp	Umfangsoption (**`OptionName`**)	Zweck	Standardwerte für **`OptionValue`** und Konsole
EC2 Instanzen	`state-name`	Nach Instance-Status filtern	`pending`, `running`, `shutting-down` , `terminated` ,

Ressourcentyp	Umfangsoption (**`OptionName`**)	Zweck	Standardwerte für **`OptionValue`** und Konsole
			`stopping`, `stopped` (alle Status)
Startvorlagen	`version-depth`	Geben Sie die Anzahl der Startvorl agenversionen an, die überprüft werden sollen (ausgehend von der neuesten Version)	`10` (neueste Versionen)

Erforderliche IAM-Berechtigungen

Um mithilfe der DescribeImageReferences API Ihre Ressourcen zu identifizieren, die auf die angegebenen Ressourcen verweisen AMIs, benötigen Sie die folgenden IAM-Berechtigungen, um die Ressourcen zu beschreiben:

- `ec2:DescribeInstances`
- `ec2:DescribeLaunchTemplates`
- `ec2:DescribeLaunchTemplateVersions`
- `ssm:DescribeParameters`
- `ssm:GetParameters`
- `imagebuilder:ListImageRecipes`
- `imagebuilder:ListContainerRecipes`
- `imagebuilder:GetContainerRecipe`

Beispiel für eine IAM-Richtlinie für die Verwendung der DescribeImageReferences-API

Die folgende Beispielrichtlinie gewährt Ihnen die Berechtigungen zur Verwendung der DescribeImageReferences API, einschließlich der Berechtigungen zum Beschreiben von EC2 Instanzen, Startvorlagen, Systems Manager Manager-Parametern, Image Builder Builder-Image-Rezepten und Image Builder Builder-Container-Rezepten.

JSON

```
{
 "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"
     ]
    }
   }
  }
 ]
}
```

Important

Wir empfehlen dringend, die AWS verwaltete Richtlinie [AmazonEC2ImageReferencesAccessPolicy]zu verwenden, anstatt die Richtlinie selbst zu erstellen. Das Erstellen einer benutzerdefinierten IAM-Richtlinie, die nur die erforderlichen

Berechtigungen bereitstellt, erfordert Zeit und Fachwissen und erfordert Aktualisierungen, sobald neue Ressourcentypen verfügbar werden.
Die `AmazonEC2ImageReferencesAccessPolicy`-verwaltete Richtlinie:

- Gewährt alle für die Verwendung der DescribeImageReferences API erforderlichen Berechtigungen (dazu gehören die Berechtigungen zum Beschreiben von EC2 Instanzen, Startvorlagen, Systems Manager Manager-Parametern sowie Image Builder Builder-Container- und Image-Rezepten).
- Unterstützt automatisch neue Ressourcentypen, sobald sie verfügbar sind (besonders wichtig, wenn der `IncludeAllResourceTypes`-Parameter verwendet wird).

Sie können die `AmazonEC2ImageReferencesAccessPolicy`-Richtlinie an Ihre IAM-Identitäten (Benutzer, Gruppen und Rollen) anhängen.
Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AmazonEC2ImageReferencesAccessPolicy in der Referenz zu AWS -verwalteten Richtlinien.

Schritte zur Überprüfung von AMI-Referenzen

Verwenden Sie die folgenden Verfahren, um zu ermitteln, auf welche Ihrer AWS Ressourcen die angegebenen AMIs Referenzen verweisen.

Console

Um die angegebenen Ressourcen zu identifizieren AMIs

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich AMIs aus.
3. Wählen Sie eine oder mehrere aus AMIs , um nach Referenzen zu suchen.
4. Wählen Sie Aktionen, AMI-Nutzung, Referenzierte Ressourcen anzeigen.
5. Gehen Sie auf der AMIs Seite Ressourcen anzeigen, die auf die ausgewählten Ressourcen verweisen, wie folgt vor:
   a. Wählen Sie unter Ressourcentypen einen oder mehrere Ressourcentypen aus.
   b. Wählen Sie Ressourcen anzeigen aus.

6. Der AMIs Abschnitt Ressourcen, die auf die Auswahl verweisen, wird angezeigt. In der Liste werden die Ressourcen angezeigt, die auf die angegebenen Ressourcen verweisen. AMIs Jede Reihe stellt die folgenden Informationen bereit:

   - AMI-ID – Die ID des AMIs, auf das verwiesen wird.
   - Ressourcentyp – Der Ressourcentyp der Ressource, die auf das AMI verweist.
   - Ressourcen-ID – Die ID der Ressource, die auf das AMI verweist.

AWS CLI

So überprüfen Sie AMI-Referenzen für bestimmte Ressourcentypen

Verwenden Sie den Befehl describe-image-references mit dem Parameter `--resource-types`. Im folgenden Beispiel werden EC2 Instanzen (nach Instanzstatus geordnet), Startvorlagen (Gültigkeitsbereich für die 20 neuesten Versionen von Startvorlagen) und andere spezifische Ressourcentypen geprüft.

```
aws ec2 describe-image-references \
    --image-ids ami-0abcdef1234567890 ami-1234567890abcdef0 \
    --resource-types \
        'ResourceType=ec2:Instance,ResourceTypeOptions=[{OptionName=state-
name,OptionValues=[running,pending]}]' \
        'ResourceType=ec2:LaunchTemplate,ResourceTypeOptions=[{OptionName=version-
depth,OptionValues=[20]}]' \
        'ResourceType=ssm:Parameter' \
        'ResourceType=imagebuilder:ImageRecipe' \
        'ResourceType=imagebuilder:ContainerRecipe'
```

Es folgt eine Beispielausgabe.

```
{
    "ImageReferences": [
        {
            "ImageId": "ami-0abcdef1234567890",
            "ResourceType": "ec2:Instance",
            "Arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
        },
        {
            "ImageId": "ami-1234567890abcdef0",
            "ResourceType": "ec2:LaunchTemplate",
```

```
            "Arn": "arn:aws:ec2:us-east-1:123456789012:launch-template/
lt-1234567890abcdef0"
        }
    ]
}
```

So überprüfen Sie AMI-Referenzen für alle unterstützten Ressourcentypen

Verwenden Sie den Befehl describe-image-references mit dem Parameter `--include-all-resource-types`.

```
aws ec2 describe-image-references \
    --image-ids ami-0abcdef1234567890 ami-1234567890abcdef0 \
    --include-all-resource-types
```

So überprüfen Sie AMI-Referenzen für alle unterstützten Ressourcentypen und spezifischen Optionen

Verwenden Sie den describe-image-referencesBefehl sowohl mit den Parametern als auch. `--include-all-resource-types` `--resource-types` In diesem Beispiel werden alle Ressourcentypen überprüft und gleichzeitig die Antwort auf EC2 Instances auf laufende oder ausstehende Instances beschränkt.

```
aws ec2 describe-image-references \
    --image-ids ami-0abcdef1234567890 ami-1234567890abcdef0 \
    --include-all-resource-types \
    --resource-types
 'ResourceType=ec2:Instance,ResourceTypeOptions=[{OptionName=state-
name,OptionValues=[running,pending]}]'
```

PowerShell

So überprüfen Sie AMI-Referenzen für bestimmte Ressourcentypen

Verwenden Sie das Get-EC2ImageReferenceCmdlet mit dem Parameter. `-ResourceType` Im folgenden Beispiel werden EC2 Instanzen (Gültigkeitsbereich nach Instanzstatus), Startvorlagen (Gültigkeitsbereich für die 20 neuesten Versionen von Startvorlagen) und andere spezifische Ressourcentypen geprüft.

```
Get-EC2ImageReference `
    -ImageId 'ami-0abcdef1234567890', 'ami-1234567890abcdef0' `
    -ResourceType @(
```

```
        @{
            ResourceType = 'ec2:Instance'
            ResourceTypeOptions = @(
                @{
                    OptionName = 'state-name'
                    OptionValues = @('running', 'pending')
                }
            )
        },
        @{
            ResourceType = 'ec2:LaunchTemplate'
            ResourceTypeOptions = @(
                @{
                    OptionName = 'version-depth'
                    OptionValues = @('20')
                }
            )
        },
        @{
            ResourceType = 'ssm:Parameter'
        },
        @{
            ResourceType = 'imagebuilder:ImageRecipe'
        },
        @{
            ResourceType = 'imagebuilder:ContainerRecipe'
        }
    )
```

So überprüfen Sie AMI-Referenzen für alle unterstützten Ressourcentypen

Verwenden Sie das Get-EC2ImageReferenceCmdlet mit dem Parameter. `-IncludeAllResourceTypes`

```
Get-EC2ImageReference `
    -ImageId 'ami-0abcdef1234567890', 'ami-1234567890abcdef0' `
    -IncludeAllResourceTypes
```

So überprüfen Sie AMI-Referenzen für alle unterstützten Ressourcentypen und spezifischen Optionen

Verwenden Sie das Get-EC2ImageReferenceCmdlet sowohl mit den als auch mit den Parametern. `-IncludeAllResourceTypes` `-ResourceType` In diesem Beispiel werden

alle Ressourcentypen überprüft und gleichzeitig die Antwort auf Instances auf laufende oder ausstehende EC2 Instances beschränkt.

```
Get-EC2ImageReference `
    -ImageId 'ami-0abcdef1234567890', 'ami-1234567890abcdef0' `
    -IncludeAllResourceTypes `
    -ResourceType @(
        @{
            ResourceType = 'ec2:Instance'
            ResourceTypeOptions = @(
                @{
                    OptionName = 'state-name'
                    OptionValues = @('running', 'pending')
                }
            )
        }
    )
```

Ein Amazon-AMI als veraltet kennzeichnen EC2

Sie können ein AMI verwerfen, um anzuzeigen, dass es veraltet ist und nicht verwendet werden sollte. Sie können auch ein zukünftiges Ablaufdatum für ein AMI angeben, das angibt, wann das AMI veraltet ist. Beispielsweise können Sie ein AMI verwerfen, das nicht mehr aktiv verwaltet wird oder Sie können ein AMI verwerfen, das durch eine neuere Version ersetzt wurde. Standardmäßig werden veraltete Versionen AMIs nicht in AMI-Listen angezeigt, sodass neue Benutzer sie nicht verwenden können. out-of-date AMIs Bestehende Benutzer und Startdienste, wie Startvorlagen und Amazon EC2 Auto Scaling Scaling-Gruppen, können jedoch weiterhin ein veraltetes AMI verwenden, indem sie dessen ID angeben. Um das AMI zu löschen, sodass Benutzer und Services es nicht verwenden können, müssen Sie es Abmelden.

Nachdem ein AMI veraltet ist:

- Für AMI-Benutzer erscheint das veraltete AMI nicht in DescribeImagesAPI-Aufrufen, es sei denn, Sie geben seine ID an oder geben an, dass das veraltete AMIs AMI erscheinen muss. AMI-Besitzer werden AMIs in DescribeImagesAPI-Aufrufen weiterhin als veraltet eingestuft.
- Für AMI-Benutzer kann das veraltete AMI nicht über die EC2 Konsole ausgewählt werden. Ein veraltetes AMI wird beispielsweise nicht im AMI-Katalog des Launch Instance Wizard angezeigt. AMI-Besitzern wird AMIs in der Konsole weiterhin „veraltet“ angezeigt. EC2

- Wenn Sie AMI-Benutzer die ID eines veralteten AMI kennen, können Sie weiterhin Instances starten, die das veraltete AMI verwenden, indem Sie die API, CLI oder die verwenden. SDKs
- Startdienste, wie Startvorlagen und Amazon EC2 Auto Scaling Scaling-Gruppen, können weiterhin auf veraltete AMIs Produkte verweisen.
- EC2 Instances, die mit einem AMI gestartet wurden, das später als veraltet gilt, sind nicht betroffen und können gestoppt, gestartet und neu gestartet werden.

Sie können sowohl private als auch öffentliche Daten als veraltet kennzeichnen. AMIs

Inhalt

- Kosten
- Überlegungen
- AMI als veraltet kennzeichnen
- Beschreiben Sie „veraltet“ AMIs
- Aufhebung der AMI-Veraltung

Kosten

Wenn Sie ein AMI veralten lassen, wird das AMI nicht gelöscht. Der AMI-Besitzer zahlt weiterhin für die Snapshots des AMI. Um die Zahlung für die Schnappschüsse einzustellen, muss der AMI-Besitzer das AMI löschen, indem er es abmeldet.

Überlegungen

- Um ein AMI veralten zu lassen, müssen Sie der Besitzer des AMI sein.
- AMIs die in letzter Zeit nicht zum Starten einer Instance verwendet wurden, eignen sich möglicherweise als veraltet oder für die Abmeldung. Weitere Informationen finden Sie unter the section called “Prüfen, wann ein AMI zuletzt verwendet wurde”.
- Sie können EBS-gestützte AMI-Richtlinien für Amazon Data Lifecycle Manager erstellen, um die Abwertung von EBS-gestützten zu automatisieren. AMIs Weitere Informationen finden Sie unter AMI-Lebenszyklusrichtlinien erstellen.
- Standardmäßig AMIs ist das Verfallsdatum aller öffentlichen Dateien auf zwei Jahre ab dem Datum der AMI-Erstellung festgelegt. Sie können das Veralterungsdatum auf weniger als zwei Jahre festlegen. Um das Veralterungsdatum zu stornieren oder weiter in die Zukunft zu verschieben, müssen Sie das AMI privat machen, indem Sie es nur für bestimmte AWS -Konten freigeben.

AMI als veraltet kennzeichnen

Sie können ein AMI an einem bestimmten Datum und einer bestimmten Uhrzeit veralten lassen Sie müssen Eigentümer des AMI sein.

Die Obergrenze für das Verfallsdatum liegt ab sofort bei 10 Jahren, mit Ausnahme von Public AMIs, wo die Obergrenze 2 Jahre ab dem Erstellungsdatum beträgt. Sie können kein Datum angeben, das in der Vergangenheit liegt.

Console

AMI an einem bestimmten Datum als veraltet kennzeichnen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigator AMIs.
3. Wählen Sie in der Filterleiste Owned by me (In meinem Besitz) aus.
4. Wählen Sie das AMI und dann Actions (Aktionen), Manage AMI Deprecation (AMI-Veralterung verwalten) aus. Sie können mehrere auswählen AMIs , um dasselbe Verfallsdatum für mehrere AMIs gleichzeitig festzulegen.
5. Wählen Sie das Kontrollkästchen Aktivieren aus und geben Sie dann das Datum und die Uhrzeit für die Veraltung ein.
6. Wählen Sie Speichern.

AWS CLI

AMI an einem bestimmten Datum als veraltet kennzeichnen

Verwenden Sie den Befehl enable-image-deprecation. Wenn Sie einen Wert für Sekunden angeben, EC2 rundet Amazon die Sekunden auf die nächste Minute ab.

```
aws ec2 enable-image-deprecation \
    --image-id ami-0abcdef1234567890 \
    --deprecate-at "2025-04-15T13:17:12.000Z"
```

PowerShell

AMI an einem bestimmten Datum als veraltet kennzeichnen

Verwenden Sie das cmdlet Enable-EC2ImageDeprecation. Wenn Sie einen Wert für Sekunden angeben, EC2 rundet Amazon die Sekunden auf die nächste Minute ab.

```
Enable-EC2ImageDeprecation `
    -ImageId ami-0abcdef1234567890 `
    -DeprecateAt 2025-04-15T13:17:12.000Z
```

Beschreiben Sie „veraltet“ AMIs

Sie können das Datum und die Uhrzeit der Verfallszeit eines AMI anzeigen und nach dem Verfallsdatum AMIs filtern.

Console

Veralterungsdatum eines AMI anzeigen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigator das AMI aus AMIs, und wählen Sie es anschließend aus.
3. Überprüfen Sie das Feld Uhrzeit der Veraltung. Wenn Sie das Kontrollkästchen neben dem AMI aktiviert haben, befindet es sich auf der Registerkarte Details. Das Feld zeigt das Datum und die Uhrzeit der Veralterung des AMI. Wenn das Feld leer ist, ist das AMI nicht als veraltet gekennzeichnet.

Um nach dem AMIs Verfallsdatum zu filtern

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigator AMIs.
3. Wählen Sie in der Filterleiste „In meinem Besitz“ oder „Private Bilder“ (zu privaten Bildern gehören sowohl Bilder AMIs, die mit Ihnen geteilt wurden, als auch Bilder, die Ihnen gehören).
4. Geben Sie in der Suchleiste **`Deprecation time`** ein (während Sie die Buchstaben eingeben, wird der Filter Deprecation time (Uhrzeit der Veralterung) angezeigt) und wählen Sie dann einen Operator sowie ein Datum und eine Uhrzeit aus.

AWS CLI

Wenn Sie alle beschreiben AMIs, hängen die Ergebnisse davon ab, ob Sie ein AMI-Benutzer oder der AMI-Besitzer sind.

- AMI-Benutzer — Wenn Sie alle beschreiben, werden standardmäßig veraltete Versionen ausgeschlossen AMIs, AMIs die zwar mit Ihnen geteilt werden, Ihnen aber nicht gehören. Um veraltete Versionen AMIs in die Ergebnisse aufzunehmen, geben Sie die Option an. `--include-deprecated`
- AMI-Besitzer — Wenn Sie alles beschreiben AMIs, sind alle AMIs Ihre Besitztümer, auch veraltete AMIs, enthalten. Sie können veraltete Dateien, die Sie besitzen, nicht ausschließen AMIs , indem Sie die Option verwenden. `--no-include-deprecated`

Um bei der Beschreibung von „Alle“ für ein Konto die Option „veraltet AMIs “ einzubeziehen AMIs

Verwenden Sie den Befehl describe-images.

```
aws ec2 describe-images
    --owners 123456789012 \
    --include-deprecated
```

Um das Veraltete AMIs Element für Ihr Konto zu beschreiben

Verwenden Sie den Befehl describe-images.

```
aws ec2 describe-images \
    --owners self \
    --query "Images[?DeprecationTime!=null].ImageId" \
    --output text
```

Es folgt eine Beispielausgabe.

```
ami-0abcdef1234567890
```

Veralterungsdatum eines AMI beschreiben

Verwenden Sie den Befehl describe-images. Wenn `DeprecationTime` es in der Ausgabe nicht vorhanden ist, wird für das AMI keine Außerbetriebnahme durchgeführt oder für einen zukünftigen Zeitpunkt festgelegt.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[].DeprecationTime \
    --output text
```

Es folgt eine Beispielausgabe.

```
2025-05-01T00:00:00.000Z
```

PowerShell

Um die veralteten AMIs Versionen für Ihr Konto aufzulisten

Verwenden Sie das cmdlet Get-EC2Image.

```
(Get-EC2Image -Owner self | Where-Object {$_.DeprecationTime -ne $null}).ImageId
```

Es folgt eine Beispielausgabe.

```
ami-0abcdef1234567890
```

Veralterungsdatum eines AMI beschreiben

Verwenden Sie das cmdlet Get-EC2Image. Wenn `DeprecationTime` es in der Ausgabe nicht vorhanden ist, wird für das AMI keine Außerbetriebnahme durchgeführt oder für einen zukünftigen Zeitpunkt festgelegt.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).DeprecationTime
```

Es folgt eine Beispielausgabe.

```
2025-05-01T00:00:00.000Z
```

Aufhebung der AMI-Veraltung

Sie können die Außerbetriebnahme eines AMI abbrechen, wodurch das Datum und die Uhrzeit der Außerbetriebnahme entfernt werden. Sie müssen der AMI-Besitzer sein, um dieses Verfahren durchführen zu können.

Console

So brechen Sie die Veralterung eines AMI ab

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigator AMIs.
3. Wählen Sie in der Filterleiste Owned by me (In meinem Besitz) aus.
4. Wählen Sie das AMI und dann Actions (Aktionen), Manage AMI Deprecation (AMI-Veralterung verwalten) aus. Sie können mehrere auswählen AMIs , um die Einstellung mehrerer AMIs gleichzeitig aufzuheben.
5. Deaktivieren Sie das Kontrollkästchen Aktivieren und wählen Sie dann Speichern aus.

AWS CLI

So brechen Sie die Veralterung eines AMI ab

Verwenden Sie den folgenden disable-image-deprecation-Befehl.

```
aws ec2 disable-image-deprecation --image-id ami-0abcdef1234567890
```

PowerShell

So brechen Sie die Veralterung eines AMI ab

Verwenden Sie das cmdlet Disable-EC2ImageDeprecation.

```
Disable-EC2ImageDeprecation -ImageId ami-0abcdef1234567890
```

Ein Amazon EC2 AMI deaktivieren

Sie können ein AMI deaktivieren, um zu verhindern, dass es für Instance-Starts verwendet wird. Sie können keine neuen Instances von einem deaktivierten AMI aus starten. Sie können ein deaktiviertes AMI erneut aktivieren, sodass es wieder für Instance-Starts verwendet werden kann.

Sie können sowohl privat als auch öffentlich deaktivieren AMIs.

Um die Speicherkosten für deaktivierte EBS-gestützte AMIs Geräte zu senken, die selten genutzt werden, aber langfristig aufbewahrt werden müssen, können Sie die zugehörigen Snapshots

archivieren. Weitere Informationen finden Sie unter Amazon-EBS-Snapshots archivieren im Amazon-EBS-Benutzerhandbuch.

Inhalt

- So funktioniert die AMI-Deaktivierung
- Kosten
- Voraussetzungen
- Erforderliche IAM-Berechtigungen
- Deaktivieren eines AMIs
- Beschreiben Sie deaktiviert AMIs
- Ein deaktiviertes AMI erneut aktivieren

So funktioniert die AMI-Deaktivierung

> **Warning**
>
> Durch die Deaktivierung eines AMI werden alle Startberechtigungen entfernt.

Wenn ein AMI deaktiviert ist:

- Der Status des AMI ändert sich zu `disabled`.
- Ein deaktiviertes AMI kann nicht freigegeben werden. Wenn ein AMI öffentlich war oder zuvor freigegeben wurde, wird es privat gemacht. Wenn ein AMI mit einer AWS-Konto Organisation oder Organisationseinheit geteilt wurde, verlieren diese den Zugriff auf das deaktivierte AMI.
- Ein deaktiviertes AMI wird standardmäßig nicht in DescribeImages-API-Aufrufen angezeigt.
- Ein deaktiviertes AMI wird nicht unter dem Konsolenfilter Owned by me angezeigt. Verwenden Sie den Konsolenfilter Disabled Images AMIs, um nach deaktivierten Bildern zu suchen.
- Ein deaktiviertes AMI ist nicht verfügbar, um Instance-Starts in der EC2 Konsole auszuwählen. Ein deaktiviertes AMI wird beispielsweise nicht im AMI-Katalog im Launch Instance Wizard oder beim Erstellen einer Startvorlage angezeigt.
- Startdienste, wie Startvorlagen und Amazon EC2 Auto Scaling Scaling-Gruppen, können weiterhin auf deaktiviert verweisen AMIs. Nachfolgende Instance-Starts von einem deaktivierten AMI aus schlagen fehl. Wir empfehlen daher, Startvorlagen und Amazon EC2 Auto Scaling Scaling-Gruppen so zu aktualisieren, dass sie AMIs nur als Referenz verfügbar sind.

- EC2 Instances, die zuvor mit einem AMI gestartet wurden, das anschließend deaktiviert wurde, sind nicht betroffen und können gestoppt, gestartet und neu gestartet werden.
- Sie können keine Snapshots löschen, die mit „Deaktiviert“ verknüpft sind. AMIs Der Versuch, einen zugehörigen Snapshot zu löschen, führt zu dem `snapshot is currently in use`-Fehler.

Wenn ein AMI wieder aktiviert wird:

- Der Status des AMI ändert sich auf `available` und es kann zum Starten von Instances verwendet werden.
- Das AMI kann gemeinsam genutzt werden.
- AWS-Konten, Organisationen und Organisationseinheiten, die den Zugriff auf das AMI verloren haben, als es deaktiviert wurde, erhalten nicht automatisch wieder Zugriff, aber das AMI kann wieder mit ihnen geteilt werden.

Kosten

Wenn Sie ein AMI deaktivieren, wird das AMI nicht gelöscht. Wenn es sich bei dem AMI um ein EBS-gestütztes AMI handelt, zahlen Sie weiterhin für die EBS-Snapshots des AMI. Wenn Sie das AMI behalten möchten, können Sie möglicherweise Ihre Speicherkosten senken, indem Sie die Snapshots archivieren. Weitere Informationen finden Sie unter Amazon-EBS-Snapshots archivieren im Amazon-EBS-Benutzerhandbuch. Wenn Sie das AMI und seine Snapshots nicht behalten möchten, müssen Sie das AMI abmelden und die Snapshots löschen. Weitere Informationen finden Sie unter Aufheben der Registrierung eines AMI.

Voraussetzungen

Um ein AMI zu deaktivieren oder erneut zu aktivieren, müssen Sie das AMI besitzen.

Erforderliche IAM-Berechtigungen

Sie benötigen die folgenden IAM-Berechtigungen, um ein AMI zu deaktivieren und erneut zu aktivieren:

- `ec2:DisableImage`
- `ec2:EnableImage`

Deaktivieren eines AMIs

Sie können ein AMI deaktivieren, indem Sie die EC2 Konsole oder die AWS Command Line Interface (AWS CLI) verwenden. Sie müssen der AMI-Besitzer sein, um dieses Verfahren durchführen zu können.

Console

So deaktivieren Sie ein AMI

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option AMIs aus.
3. Wählen Sie in der Filterleiste Owned by me (In meinem Besitz) aus.
4. Wählen Sie das AMI aus, dann Aktionen und anschließend AMI deaktivieren. Sie können mehrere auswählen AMIs , um sie gleichzeitig zu deaktivieren.
5. Wählen Sie im Fenster AMI deaktivieren die Option AMI deaktivieren aus.

AWS CLI

So deaktivieren Sie ein AMI

Verwenden Sie den folgenden disable-image-Befehl.

```
aws ec2 disable-image --image-id ami-0abcdef1234567890
```

PowerShell

So deaktivieren Sie ein AMI

Verwenden Sie das cmdlet Disable-EC2Image.

```
Disable-EC2Image -ImageId ami-0abcdef1234567890
```

Beschreiben Sie deaktiviert AMIs

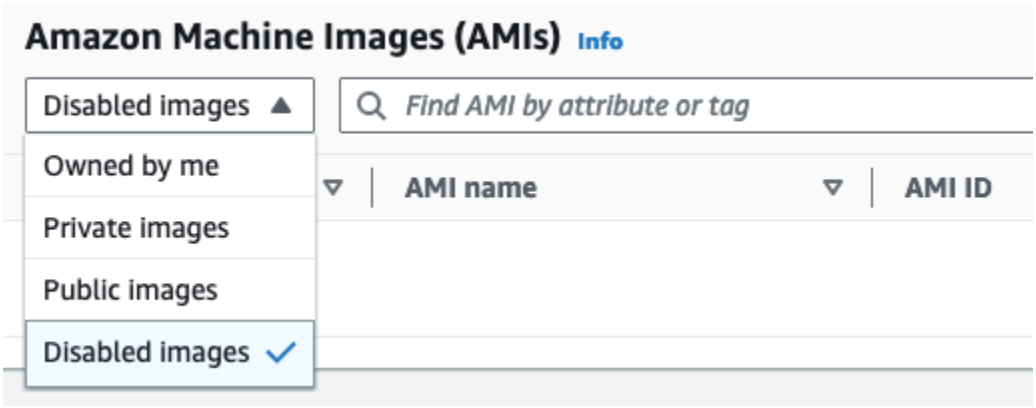
Sie können die Anzeige deaktiviert AMIs in der EC2 Konsole und mithilfe von anzeigen AWS CLI.

Sie müssen der AMI-Besitzer sein, um die Anzeige deaktiviert zu haben AMIs. Deaktivierte AMIs Benutzer werden als privat eingestuft. Sie können deaktivierte Inhalte also nicht aufrufen, AMIs wenn Sie nicht der Besitzer sind.

Console

Zur Ansicht „Deaktiviert“ AMIs

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option AMIs aus.
3. Wählen Sie in der Filterleiste Deaktivierte Images aus.



AWS CLI

Wenn Sie alle AMIs beschreiben, AMIs sind die Deaktivierten standardmäßig nicht in den Ergebnissen enthalten. Um Deaktivierte AMIs in die Ergebnisse aufzunehmen, geben Sie die `--include-disabled` Option an. Das `State`-Feld für ein AMI ist `disabled`, wenn das AMI deaktiviert ist.

Um „ AMIs Deaktiviert“ in die Beschreibung „Alle“ AMIs für ein Konto einzubeziehen

Verwenden Sie den folgenden describe-images-Befehl.

```
aws ec2 describe-images \
    --owners 123456789012 \
    --include-disabled
```

Um die Deaktivierten AMIs für dein Konto aufzulisten

Verwenden Sie den folgenden describe-images-Befehl.

```
aws ec2 describe-images \
    --owners self \
    --include-disabled \
    --filters Name=state,Values=disabled \
    --query Images[].ImageId \
    --output text
```

Es folgt eine Beispielausgabe.

```
ami-0abcdef1234567890
```

So beschreiben Sie den Status eines AMI

Verwenden Sie den folgenden describe-images-Befehl. Wenn `DeprecationTime` es in der Ausgabe nicht vorhanden ist, wird für das AMI keine Außerbetriebnahme durchgeführt oder für einen zukünftigen Zeitpunkt festgelegt.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[].State \
    --output text
```

Es folgt eine Beispielausgabe.

```
disabled
```

PowerShell

Wenn Sie alle AMIs beschreiben, AMIs sind die Deaktivierten standardmäßig nicht in den Ergebnissen enthalten. Um Deaktivierte AMIs in die Ergebnisse aufzunehmen, geben Sie den `-IncludeDisabled` Parameter an. Das `State`-Feld für ein AMI ist `disabled`, wenn das AMI deaktiviert ist.

Um die Deaktivierten AMIs für Ihr Konto aufzulisten

Verwenden Sie das cmdlet Get-EC2Image.

```
(Get-EC2Image `
    -Owner self `
```

```
    -IncludeDisabled $true | Where-Object {$_.State -eq "disabled"}).ImageId
```

Es folgt eine Beispielausgabe.

```
ami-0abcdef1234567890
```

So beschreiben Sie den Status eines AMI

Verwenden Sie das cmdlet Get-EC2Image.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).State.Value
```

Es folgt eine Beispielausgabe.

```
disabled
```

Ein deaktiviertes AMI erneut aktivieren

Sie können ein zuvor deaktiviertes AMI reaktivieren. Sie müssen der AMI-Besitzer sein, um dieses Verfahren durchführen zu können.

Console

So reaktivieren Sie ein zuvor deaktiviertes AMI

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option AMIs aus.
3. Wählen Sie in der Filterleiste Deaktivierte Images aus.
4. Wählen Sie das AMI aus, dann Aktionen und anschließend AMI aktivieren. Sie können mehrere auswählen AMIs , um mehrere gleichzeitig wieder zu aktivieren. AMIs
5. Wählen Sie im Fenster AMI aktivieren die Option Aktivieren aus.

AWS CLI

So reaktivieren Sie ein zuvor deaktiviertes AMI

Verwenden Sie den folgenden enable-image-Befehl.

```
aws ec2 enable-image --image-id ami-0abcdef1234567890
```

PowerShell

So reaktivieren Sie ein zuvor deaktiviertes AMI

Verwenden Sie das cmdlet Enable-EC2Image.

```
Enable-EC2Image -ImageId ami-0abcdef1234567890
```

Aufheben der Registrierung eines Amazon-EC2-AMI

Wenn Sie ein AMI abmelden, löscht Amazon EC2 es dauerhaft. Nachdem Sie ein AMI abgemeldet haben, können Sie es nicht mehr verwenden, um neue Instances zu starten. Sie können die Registrierung eines AMI aufheben, wenn Sie es nicht mehr verwenden.

Zum Schutz vor versehentlicher oder böswilliger Aufhebung der Registrierung eines AMI können Sie den Aufhebungsschutz aktivieren. Wenn Sie die Registrierung eines EBS-gesicherten AMI versehentlich aufheben, können Sie es nur dann über den Papierkorb wiederherstellen, wenn Sie es innerhalb des zulässigen Zeitraums wiederherstellen, bevor es endgültig gelöscht wird.

Wenn Sie ein AMI abmelden, können Sie optional gleichzeitig die zugeordneten Snapshots löschen. Wenn ein Snapshot jedoch mehreren AMIs zugeordnet ist, wird er nicht gelöscht, auch wenn er zum Löschen angegeben wurde, obwohl das AMI trotzdem abgemeldet wird. Für alle Snapshots, die nicht gelöscht werden, werden weiterhin Speichergebühren in Rechnung gestellt.

Die Aufhebung der Registrierung eines AMI hat keine Auswirkungen auf Instances, die über das AMI gestartet wurden. Sie können diese Instances weiter verwenden. Standardmäßig hat die Aufhebung der Registrierung eines AMI auch keine Auswirkungen auf Snapshots, die während des AMI-Erstellungsprozesses erstellt wurden. Für Sie fallen weiterhin Nutzungskosten für diese Instances und Speicherkosten für den Snapshot an. Um unnötige Kosten zu vermeiden, empfehlen wir Ihnen daher, alle Instances zu beenden und Snapshots, die nicht gebraucht werden, zu löschen. Sie können die Snapshots entweder automatisch während der Abmeldung oder manuell nach der Abmeldung löschen. Weitere Informationen finden Sie unter Vermeiden Sie Kosten, die durch ungenutzte Ressourcen entstehen.

Für Instances, die von einem AMI gestartet wurden, dessen Registrierung anschließend aufgehoben wurde, können Sie mit dem Befehl `describe-instance-image-metadata` AWS CLI dennoch

einige allgemeine Informationen über das AMI anzeigen. Weitere Informationen finden Sie unter describe-instance-image-metadata.

Inhalt

- Überlegungen
- Aufheben der Registrierung eines AMI
- Vermeiden Sie Kosten, die durch ungenutzte Ressourcen entstehen
- Schützen Sie ein Amazon-EC2-AMI vor der Aufhebung der Registrierung

Überlegungen

- Sie können ein AMI, das nicht Ihrem Konto gehört, nicht abmelden.
- Sie können Amazon EC2 nicht verwenden, um ein AMI von der Registrierung abzumelden, das vom AWS Backup-Service verwaltet wird. Verwenden Sie stattdessen AWS Backup, um die entsprechenden Wiederherstellungspunkte im Backup-Tresor zu löschen. Weitere Informationen finden Sie unter Löschen von Backups im AWS BackupEntwickler-Leitfaden.

Aufheben der Registrierung eines AMI

Sie können EBS-gestützte AMIs und Amazon-S3-gestützte AMIs abmelden. Bei EBS-gestützten AMIs können Sie optional die zugeordneten Snapshots gleichzeitig löschen. Wenn ein Snapshot jedoch mit anderen AMIs verknüpft ist, wird er nicht gelöscht, auch wenn er zum Löschen angegeben wurde.

Console

So heben Sie die Registrierung eines AMI auf

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie in der Filterleiste In meinem Besitz aus, um Ihre verfügbaren AMIs aufzulisten oder Deaktivierte Images, um Ihre deaktivierten AMIs aufzulisten.
4. Wählen Sie das AMI für die Aufhebung der Registrierung.
5. Wählen Sie Aktionen, AMI abmelden aus.
6. (Optional) Um die zugeordneten Snapshots während der Abmeldung zu löschen, aktivieren Sie das Kontrollkästchen Zugeordnete Snapshots löschen.

> **Note**
>
> Wenn ein Snapshot mit anderen AMIs verknüpft ist, wird er nicht gelöscht, auch wenn das Kontrollkästchen aktiviert ist.

7. Wählen Sie AMI abmelden.

   Es kann einige Minuten dauern, bis die Konsole das AMI aus der Liste entfernt. Wählen Sie Refresh (Aktualisieren) aus, um den Status zu aktualisieren.

AWS CLI

So heben Sie die Registrierung eines AMI auf

Verwenden Sie den folgenden Befehl deregister-image.

```
aws ec2 deregister-image --image-id ami-0abcdef1234567890
```

So melden Sie ein AMI ab und löschen die zugeordneten Snapshots

Verwenden Sie den Befehl deregister-image und geben Sie den Parameter `--delete-associated-snapshots` an. Beachten Sie, dass ein Snapshot, der anderen AMIs zugeordnet ist, nicht gelöscht wird, auch wenn Sie diesen Parameter angeben.

```
aws ec2 deregister-image \
    --image-id ami-0abcdef1234567890 \
    --delete-associated-snapshots
```

PowerShell

So heben Sie die Registrierung eines AMI auf

Verwenden Sie das cmdlet Unregister-EC2Image-

```
Unregister-EC2Image -ImageId ami-0abcdef1234567890
```

So melden Sie ein AMI ab und löschen die zugeordneten Snapshots

Verwenden Sie das cmdlet Unregister-EC2Image und geben Sie den Parameter `-DeleteAssociatedSnapshots` an. Beachten Sie, dass ein Snapshot, der anderen AMIs zugeordnet ist, nicht gelöscht wird, auch wenn Sie diesen Parameter angeben.

```
Unregister-EC2Image `
    -ImageId ami-0abcdef1234567890 `
    -DeleteAssociatedSnapshots
```

Vermeiden Sie Kosten, die durch ungenutzte Ressourcen entstehen

Wenn Sie ein AMI abmelden, werden standardmäßig nicht alle mit dem AMI verknüpften Ressourcen gelöscht. Zu diesen Ressourcen gehören Snapshots für EBS-gestützte AMIs und die Dateien in Amazon S3 für Amazon-S3-gestützte AMIs. Wenn Sie ein AMI abmelden, werden auch keine Instances, die von dem AMI gestartet werden, beendet oder gestoppt.

Es fallen weiterhin Kosten für das Speichern der Snapshots und Dateien an, und es fallen Kosten für alle laufenden Instances an.

Um diese Art von unnötigen Kosten zu vermeiden, empfehlen wir Ihnen, alle nicht benötigten Ressourcen zu löschen.

EBS-gestützte AMIs

- Löschen Sie die zugeordneten Snapshots, während Sie das AMI abmelden. Weitere Informationen finden Sie unter Aufheben der Registrierung eines AMI.
- Wenn Sie ein AMI abmelden, ohne die zugeordneten Snaphots zu löschen, können Sie manuell die Snapshots löschen. Der Snapshot des Instance-Root-Volumes, der während der AMI-Erstellung erstellt wurde, hat das folgende Beschreibungsformat:

  ```
  Created by CreateImage(i-1234567890abcdef0) for ami-0abcdef1234567890
  ```

- Wenn Sie die Instances, die über das AMI gestartet wurden, nicht mehr benötigen, können Sie sie anhalten oder beenden. Um die Instances aufzulisten, filtern Sie nach der ID des AMI.

Amazon-S3-gestützte AMIs

- Löschen Sie das Bundle in Amazon S3 wie folgt mit dem Befehl ec2-delete-bundle (AMI-Tools).

- Wenn der Amazon-S3-Bucket nach dem Löschen des Pakets leer ist und Sie diesen Bucket nicht mehr verwenden möchten, können Sie den Bucket löschen.
- Wenn Sie die Instances, die über das AMI gestartet wurden, nicht mehr benötigen, können Sie sie beenden. Um die Instances aufzulisten, filtern Sie nach der ID des AMI.

Schützen Sie ein Amazon-EC2-AMI vor der Aufhebung der Registrierung

Sie können den Abmeldeschutz für ein AMI aktivieren, um ein versehentliches oder böswilliges Löschen zu verhindern. Wenn Sie den Abmeldeschutz aktivieren, kann das AMI von keinem Benutzer abgemeldet werden, unabhängig von dessen IAM-Berechtigungen. Wenn Sie das AMI abmelden möchten, müssen Sie zuerst den Abmeldeschutz für das AMI deaktivieren.

Wenn Sie den Abmeldeschutz für ein AMI aktivieren, haben Sie die Möglichkeit, eine 24-stündige Ruhephase einzuplanen. Diese Ruhephase ist die Zeit, in der der Abmeldeschutz auch nach dem Ausschalten aktiv bleibt. Während dieser Ruhephase kann das AMI nicht abgemeldet werden. Nach Ablauf der Ruhephase kann die Registrierung des AMI aufgehoben werden.

Standardmäßig ist der Abmeldeschutz für alle vorhandenen und neuen AMIs abgeschaltet.

Abmeldeschutz einschalten

Verwenden Sie die folgenden Verfahren, um den Abmeldeschutz einzuschalten.

Console

So schalten Sie den Abmeldeschutz ein

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie in der Filterleiste In meinem Besitz aus, um Ihre verfügbaren AMIs aufzulisten oder Deaktivierte Images, um Ihre deaktivierten AMIs aufzulisten.
4. Wählen Sie das AMI aus, für das Sie den Abmeldeschutz aktivieren möchten, und klicken Sie dann auf Aktionen, AMI-Abmeldeschutz verwalten.
5. Im Dialogfeld AMI-Abmeldeschutz verwalten können Sie den Abmeldeschutz mit oder ohne Ruhephase aktivieren. Wählen Sie eine der folgenden Optionen:

   - Mit einer Ruhephase von 24 Stunden aktivieren – Bei einer Abklingzeit kann das AMI 24 Stunden lang nicht abgemeldet werden, wenn der Abmeldeschutz ausgeschaltet ist.

- Ohne Ruhephase aktivieren – Ohne Abklingzeit kann das AMI sofort abgemeldet werden, wenn der Abmeldeschutz ausgeschaltet ist.

6. Wählen Sie Speichern.

AWS CLI

So schalten Sie den Abmeldeschutz ein

Verwenden Sie den Befehl enable-image-deregistration-protection. Um die optionale Ruhephase zu aktivieren, fügen Sie die Option `--with-cooldown` hinzu.

```
aws ec2 enable-image-deregistration-protection \
    --image-id ami-0abcdef1234567890 \
    --with-cooldown
```

PowerShell

So schalten Sie den Abmeldeschutz ein

Verwenden Sie das cmdlet Enable-EC2ImageDeregistrationProtection. Um die optionale Ruhephase zu aktivieren, setzen Sie den Parameter `-WithCooldown` auf `true`.

```
Enable-EC2ImageDeregistrationProtection `
    -ImageId ami-0abcdef1234567890 `
    -WithCooldown $true
```

Abmeldeschutz ausschalten

Gehen Sie wie folgt vor, um den Abmeldeschutz zu auszuschalten.

Wenn Sie bei der Aktivierung des Abmeldeschutzes für das AMI eine 24-stündige Ruhephase gewählt haben, können Sie das AMI nicht sofort abmelden, wenn Sie den Abmeldeschutz ausschalten. Diese 24-stündige Ruhephase ist die Zeit, in der der Abmeldeschutz auch nach dem Ausschalten aktiv bleibt. Während dieser Ruhephase kann das AMI nicht abgemeldet werden. Nach Ablauf der Ruhephase kann die Registrierung des AMI aufgehoben werden.

Console

So schalten Sie den Abmeldeschutz aus

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie in der Filterleiste In meinem Besitz aus, um Ihre verfügbaren AMIs aufzulisten oder Deaktivierte Images, um Ihre deaktivierten AMIs aufzulisten.
4. Wählen Sie das AMI aus, für das Sie den Abmeldeschutz zu deaktivieren wollen, und wählen Sie dann Aktionen, AMI-Abmeldeschutz verwalten aus.
5. Wählen Sie im Dialogfeld AMI-Abmeldeschutz verwalten die Option Deaktivieren aus.
6. Wählen Sie Speichern.

AWS CLI

So schalten Sie den Abmeldeschutz aus

Verwenden Sie den Befehl disable-image-deregistration-protection.

```
aws ec2 disable-image-deregistration-protection --image-id ami-0abcdef1234567890
```

PowerShell

So schalten Sie den Abmeldeschutz aus

Verwenden Sie das cmdlet Disable-EC2ImageDeregistrationProtection.

```
Disable-EC2ImageDeregistrationProtection -ImageId ami-0abcdef1234567890
```

Instance-Startverhalten mit Amazon-EC2-Startmodi

Wenn ein Computer hochfährt, ist die erste Software, die er ausführt, für die Initialisierung der Plattform und die Bereitstellung einer Schnittstelle für das Betriebssystem zur Durchführung plattformspezifischer Vorgänge verantwortlich.

In Amazon EC2 werden zwei Varianten der Startmodus-Software unterstützt: Unified Extensible Firmware Interface (UEFI) und Legacy BIOS.

Mögliche Startmodus-Parameter für ein AMI

Ein AMI kann einen der folgenden Werte für den Startmodus-Parameter annehmen: `uefi`, `legacy-bios` oder `uefi-preferred`. Der AMI-Startmodus-Parameter ist optional. Für AMIs ohne Startmodus-Parameter verwenden die Instances, die von diesen AMIs gestartet werden, den Standardstartmodus-Wert des Instance-Typs.

Der Zweck des AMI-Startmodus-Parameters

Der AMI-Startmodus-Parameter signalisiert Amazon EC2, welcher Startmodus beim Starten einer Instance verwendet werden soll. Wenn der Startmodus-Parameter auf `uefi` festgelegt ist, versucht EC2, die Instance mit UEFI zu starten. Wenn das Betriebssystem nicht für die Verwendung von UEFI konfiguriert ist, wird die Instance nicht erfolgreich gestartet.

UEFI-Bevorzugt-Startmodus-Parameter

Sie können AMIs erstellen, die sowohl UEFI als auch Legacy-BIOS unterstützen, indem Sie den `uefi-preferred`-Startmodus-Parameter verwenden. Wenn der Startmodus-Parameter auf `uefi-preferred` festgelegt ist und der Instance-Typ UEFI unterstützt, wird die Instance auf UEFI gestartet. Wenn der Instance-Typ UEFI nicht unterstützt, wird die Instance auf Legacy-BIOS gestartet.

> **Warning**
>
> Einige Features, wie UEFI Secure Boot, sind nur auf Instances verfügbar, die auf UEFI gestartet werden. Wenn Sie den `uefi-preferred`-AMI-Startmodus-Parameter mit einem Instance-Typ verwenden, der UEFI nicht unterstützt, wird die Instance als Legacy-BIOS gestartet und das UEFI-abhängige Feature wird deaktiviert. Wenn Sie auf die Verfügbarkeit eines UEFI-abhängigen Features angewiesen sind, setzen Sie Ihren AMI-Startmodus-Parameter auf `uefi`.

Standard-Startmodi für Instance-Typen

- Instance-Typen für Graviton: UEFI
- Instance-Typen für Intel und AMD: Legacy-System BIOS

Zonenunterstützung

UEFI-Boot wird nicht in Wavelength Zones unterstützt.

Themen zu Startmodus

- Voraussetzungen für den Start einer EC2-Instance im UEFI-Bootmodus
- Den Bootmodus-Parameter für ein Amazon-EC2-AMI bestimmen
- Die unterstützten Bootmodi eines EC2-Instance-Typs bestimmen
- Den Bootmodus einer EC2-Instance bestimmen
- Den Boot-Modus des Betriebssystems für Ihre EC2 Instance bestimmen
- Den Bootmodus eines Amazon-EC2-AMIs festlegen
- UEFI-Variablen für Amazon-EC2-Instances
- UEFI Secure Boot für Amazon-EC2-Instances

Voraussetzungen für den Start einer EC2-Instance im UEFI-Bootmodus

Der Bootmodus der Instance wird durch die Konfiguration des AMI, das darin enthaltene Betriebssystem und den Instance-Typ bestimmt. Um eine Instance im UEFI-Boot-Modus zu starten, müssen Sie die folgenden Anforderungen erfüllen.

AMI

Das AMI muss für UEFI wie folgt konfiguriert sein:

- Betriebssystem – Das im AMI enthaltene Betriebssystem muss für die Verwendung von UEFI konfiguriert sein, andernfalls wird der Start der Instance fehlschlagen. Weitere Informationen finden Sie unter Den Boot-Modus des Betriebssystems für Ihre EC2 Instance bestimmen.
- AMI-Startmodus-Parameter – Der Startmodus-Parameter des AMI muss auf `uefi` oder `uefi-preferred` eingestellt sein. Weitere Informationen finden Sie unter Den Bootmodus-Parameter für ein Amazon-EC2-AMI bestimmen.

Linux – Die folgenden Linux-AMIs unterstützen UEFI:

- Amazon Linux 2023
- Amazon Linux 2 (nur Graviton-Instance-Typen)

Für andere Linux-AMIs müssen Sie das AMI konfigurieren, das AMI über VM Import/Export importieren, oder das AMI über CloudEndure importieren.

Windows – Die folgenden Windows-AMIs unterstützen UEFI:

- Windows_Server-2025-* (außer für AMIs mit dem Namenspräfix `BIOS-`)
- TPM-Windows_Server-2022-English-Full-Base

- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Core-Base
- TPM-Windows_Server-2016-English-Full-Base
- TPM-Windows_Server-2016-English-Core-Base

Instance-Typ

Alle Instances, die auf dem AWS Nitro System aufgebaut sind, unterstützen sowohl UEFI als auch Legacy BIOS, außer: Bare-Metal-Instances, DL1, G4ad, P4, u-3tb1, u-6tb1, u-9tb1, u-12tb1, u-18tb1, u-24tb1, und VT1. Weitere Informationen finden Sie unter the section called “Instance-Typ Startmodus”.

Die folgende Tabelle zeigt, dass der Startmodus einer Instance (angezeigt in der Spalte Resultierender Startmodus der Instance) durch eine Kombination aus dem Startmodus-Parameter des AMI (Spalte 1), der Startmodus-Konfiguration des im AMI enthaltenen Betriebssystems (Spalte 2) und der Startmodus-Unterstützung des Instance-Typs (Spalte 3) bestimmt wird.

AMI-Startmodus-Parameter	Startmodus-Konfiguration des Betriebssystems	Instance-Typ Startmodus-Unterstützung	Resultierender Startmodus der Instance
UEFI	UEFI	UEFI	UEFI
Legacy BIOS	Legacy BIOS	Legacy BIOS	Legacy BIOS
UEFI Preferred	UEFI	UEFI	UEFI
UEFI Preferred	UEFI	UEFI und Legacy BIOS	UEFI
UEFI Preferred	Legacy BIOS	Legacy BIOS	Legacy BIOS
UEFI Preferred	Legacy BIOS	UEFI und Legacy BIOS	Legacy BIOS
Kein Startmodus angegeben – ARM	UEFI	UEFI	UEFI

AMI-Startmodus-Parameter	Startmodus-Konfiguration des Betriebssystems	Instance-Typ Startmodus-Unterstützung	Resultierender Startmodus der Instance
Kein Startmodus angegeben – x86	Legacy BIOS	UEFI und Legacy BIOS	Legacy BIOS

Den Bootmodus-Parameter für ein Amazon-EC2-AMI bestimmen

Der AMI-Startmodus-Parameter ist optional. Ein AMI kann einen der folgenden Werte für den Startmodus-Parameter annehmen: `uefi`, `legacy-bios` oder `uefi-preferred`.

Einige AMIs haben keinen Startmodus-Parameter. Wenn ein AMI keinen Startmodus-Parameter hat, verwenden die Instances, die von diesem AMI gestartet werden, den Standardwert des Instance-Typs, der `uefi` für Graviton und `legacy-bios` für alle Intel- und AMD-Instance-Typen ist.

Console

So ermitteln Sie den Startmodus-Parameter eines AMI

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich AMIs und wählen Sie dann das AMI aus.
3. Überprüfen Sie das Feld Startmodus.
   - Ein Wert von uefi gibt an, dass das AMI UEFI unterstützt.
   - Ein Wert von uefi-preferred gibt an, dass das AMI sowohl UEFI als auch Legacy BIOS unterstützt.
   - Wenn kein Wert vorhanden ist, verwenden die über das AMI gestarteten Instances den Standardwert des Instance-Typs.

So ermitteln Sie den Startmodus-Parameter eines AMI beim Start einer Instance

Wenn Sie eine Instance mit dem Launch Instance Wizard starten, überprüfen Sie bei der Auswahl eines AMI das Feld Startmodus. Weitere Informationen finden Sie unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image).

AWS CLI

So ermitteln Sie den Startmodus-Parameter eines AMI

Verwenden Sie den Befehl describe-images, um den Startmodus eines AMI zu bestimmen.

```
aws ec2 describe-images \
    --region us-east-1 \
    --image-id ami-0abcdef1234567890 \
    --query Images[].BootMode \
    --output text
```

Es folgt eine Beispielausgabe.

```
uefi
```

Ein Wert von `uefi` in der Ausgabe gibt an, dass das AMI UEFI unterstützt. Ein Wert von `uefi-preferred` gibt an, dass das AMI sowohl UEFI als auch Legacy BIOS unterstützt. Wenn kein Wert vorhanden ist, verwenden die über das AMI gestarteten Instances den Standardwert des Instance-Typs.

PowerShell

So ermitteln Sie den Startmodus-Parameter eines AMI

Verwenden Sie das cmdlet Get-EC2Image, um den Startmodus eines AMI zu bestimmen.

```
Get-EC2Image -Region us-east-1 `
    -ImageId ami-0abcdef1234567890 | Format-List Name, BootMode, TpmSupport
```

Es folgt eine Beispielausgabe.

```
Name       : TPM-Windows_Server-2016-English-Full-Base-2023.05.10
BootMode   : uefi
TpmSupport : v2.0
```

In der Ausgabe gibt der Wert von `BootMode` den Startmodus des AMI an. Ein Wert von `uefi` gibt an, dass das AMI UEFI unterstützt. Ein Wert von `uefi-preferred` gibt an, dass das AMI sowohl UEFI als auch Legacy BIOS unterstützt. Wenn kein Wert vorhanden ist, verwenden die über das AMI gestarteten Instances den Standardwert des Instance-Typs.

Die unterstützten Bootmodi eines EC2-Instance-Typs bestimmen

Sie können die unterstützten Startmodi eines Instance-Typs ermitteln.

Die Amazon-EC2-Konsole zeigt die unterstützten Startmodi eines Instance-Typen nicht an.

AWS CLI

Verwenden Sie den Befehl describe-instance-types, um die unterstützten Startmodi eines Instance-Typs zu ermitteln. Der `--query`-Parameter filtert die Ausgabe so, dass nur die unterstützten Bootmodi zurückgegeben werden.

Das folgende Beispiel zeigt, dass der angegebene Instance-Typ sowohl den Startmodus UEFI als auch den Startmodus Legacy BIOS unterstützt.

```
aws ec2 describe-instance-types \
    --instance-types m5.2xlarge \
    --query "InstanceTypes[*].SupportedBootModes"
```

Es folgt eine Beispielausgabe.

```
[
    [
        "legacy-bios",
        "uefi"
    ]
]
```

Das folgende Beispiel zeigt, dass `t2.xlarge` nur Legacy BIOS unterstützt.

```
aws ec2 describe-instance-types \
    --instance-types t2.xlarge \
    --query "InstanceTypes[*].SupportedBootModes"
```

Es folgt eine Beispielausgabe.

```
[
    [
        "legacy-bios"
    ]
```

```
]
```

PowerShell

Verwenden Sie das cmdlet Get-EC2InstanceType, um die unterstützten Startmodi eines Instance-Typs zu ermitteln.

Das folgende Beispiel zeigt, dass `m5.2xlarge` sowohl den Startmodus UEFI als auch den Startmodus Legacy-System BIOS unterstützt.

```
Get-EC2InstanceType -InstanceType m5.2xlarge | Format-List InstanceType,
 SupportedBootModes
```

Es folgt eine Beispielausgabe.

```
InstanceType       : m5.2xlarge
SupportedBootModes : {legacy-bios, uefi}
```

Das folgende Beispiel zeigt, dass `t2.xlarge` nur Legacy BIOS unterstützt.

```
Get-EC2InstanceType -InstanceType t2.xlarge | Format-List InstanceType,
 SupportedBootModes
```

Es folgt eine Beispielausgabe.

```
InstanceType       : t2.xlarge
SupportedBootModes : {legacy-bios}
```

So bestimmen Sie die Instance-Typen, die UEFI unterstützen

Sie können die Instance-Typen bestimmen, die UEFI unterstützen. Die Amazon-EC2-Konsole zeigt die Unterstützung für UEFI eines Instance-Typen nicht an.

AWS CLI

Die verfügbaren Instance-Typen variieren je nach AWS-Region. Um die verfügbaren Instance-Typen anzuzeigen, die UEFI in einer Region unterstützen, verwenden Sie den Befehl describe-instance-types. Schließen Sie den Parameter `--filters` ein, um die Ergebnisse auf die

Instance-Typen zu beschränken, die UEFI unterstützen, und den Parameter `--query`, um die Ausgabe auf den Wert von `InstanceType` zu beschränken.

```
aws ec2 describe-instance-types \
    --filters Name=supported-boot-mode,Values=uefi \
    --query "InstanceTypes[*].[InstanceType]" --output text | sort
```

PowerShell

Die verfügbaren Instance-Typen variieren je nach AWS-Region. Um die verfügbaren Instance-Typen anzuzeigen, die UEFI in einer Region unterstützen, verwenden Sie das cmdlet Get-EC2InstanceType.

```
Get-EC2InstanceType | `
 Where-Object {$_.SupportedBootModes -Contains "uefi"} | `
 Sort-Object InstanceType | `
 Format-Table InstanceType -GroupBy CurrentGeneration
```

So bestimmen Sie die Instance-Typen, die UEFI Secure Boot unterstützen und nichtflüchtige Variablen beibehalten

Bare-Metal-Instances unterstützen kein UEFI Secure Boot und keine nicht-flüchtigen Variablen, daher werden sie in diesen Beispielen nicht mit ausgegeben. Informationen zu UEFI Secure Boot finden Sie unter UEFI Secure Boot für Amazon-EC2-Instances.

AWS CLI

Verwenden Sie den Befehl describe-instance-types und filtern Sie die Bare-Metal-Instances aus der Ausgabe heraus.

```
aws ec2 describe-instance-types \
    --filters Name=supported-boot-mode,Values=uefi Name=bare-metal,Values=false \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

PowerShell

Verwenden Sie das cmdlet Get-EC2InstanceType, und filtern Sie die Bare-Metal-Instances aus der Ausgabe heraus.

```
Get-EC2InstanceType | `
    Where-Object { `
        $_.SupportedBootModes -Contains "uefi" -and `
        $_.BareMetal -eq $False
        } | `
    Sort-Object InstanceType  | `
    Format-Table InstanceType, SupportedBootModes, BareMetal, `
        @{Name="SupportedArchitectures";
 Expression={$_.ProcessorInfo.SupportedArchitectures}}
```

Den Bootmodus einer EC2-Instance bestimmen

Der Startmodus einer Instance wird in der Amazon-EC2-Konsole im Feld Startmodus und durch den `currentInstanceBootMode`-Parameter in der AWS CLI angezeigt.

Wenn eine Instance gestartet wird, wird der Wert für ihren Startmodus-Parameter wie folgt durch den Wert des Startmodus-Parameters des zum Start verwendeten AMI bestimmt:

- Ein AMI mit dem Startmodus-Parameter `uefi` erstellt eine Instance mit dem `currentInstanceBootMode`-Parameter `uefi`.
- Ein AMI mit dem Startmodus-Parameter `legacy-bios` erstellt eine Instance mit dem `currentInstanceBootMode`-Parameter `legacy-bios`.
- Ein AMI mit dem Startmodus-Parameter `uefi-preferred` erstellt eine Instance mit dem `currentInstanceBootMode`-Parameter `uefi`, wenn der Instance-Typ UEFI unterstützt; andernfalls erstellt es eine Instance mit einem `currentInstanceBootMode`-Parameter von `legacy-bios`.
- Ein AMI ohne Startmodus-Parameterwert erstellt eine Instance mit einem `currentInstanceBootMode`-Parameterwert, der davon abhängt, ob es sich bei der AMI-Architektur um ARM oder x86 handelt, und vom unterstützten Startmodus des Instance-Typs. Der Standard-Startmodus ist `uefi` für Graviton-Instance-Typen und `legacy-bios` für Intel- und AMD-Instance-Typen.

Console

So ermitteln Sie den Startmodus einer Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie anschließend Ihre Instance aus.
3. Überprüfen Sie auf der Registerkarte Details das Feld Startmodus.

AWS CLI

So ermitteln Sie den Startmodus einer Instance

Verwenden Sie den Befehl describe-instances, um den Startmodus einer Instance zu bestimmen. Sie können auch den Startmodus des AMI bestimmen, das zum Erstellen der Instance verwendet wurde.

```
aws ec2 describe-instances \
    --region us-east-1 \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].BootMode \
    --output text
```

Es folgt eine Beispielausgabe.

```
uefi
```

PowerShell

So ermitteln Sie den Startmodus einer Instance

Verwenden Sie das cmdlet Get-EC2Image, um den Startmodus einer Instance zu bestimmen. Sie können auch den Startmodus des AMI bestimmen, das zum Erstellen der Instance verwendet wurde.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances | Format-List BootMode,
 CurrentInstanceBootMode, InstanceType, ImageId
```

Es folgt eine Beispielausgabe.

```
BootMode                : uefi
CurrentInstanceBootMode : uefi
```

```
InstanceType            : c5a.large
ImageId                 : ami-0abcdef1234567890
```

Den Boot-Modus des Betriebssystems für Ihre EC2 Instance bestimmen

Der Startmodus des AMI leitet Amazon EC2 an, welcher Startmodus zum Starten einer Instance verwendet werden soll. Um festzustellen, ob das Betriebssystem Ihrer Instance für UEFI konfiguriert ist, müssen Sie mithilfe von SSH (Linux-Instances) oder RDP (Windows-Intances) eine Verbindung mit Ihrer Instance herstellen.

Verwenden Sie die Anleitung für das Betriebssystem Ihrer Instance.

Linux

Ermitteln des Startmodus des Betriebssystems der Instance

1. Stellen Sie eine Verbindung zu Ihrer Linux-Instance mit SSH her.
2. Um den Startmodus des Betriebssystems anzuzeigen, führen Sie einen der folgenden Schritte aus:

   - Führen Sie den folgenden Befehl aus.

     ```
     [ec2-user ~]$ sudo /usr/sbin/efibootmgr
     ```

     Erwartete Ausgabe einer im UEFI-Startmodus gestarteten Instance

     ```
     BootCurrent: 0001
     Timeout: 0 seconds
     BootOrder: 0000,0001
     Boot0000* UiApp
     Boot0001* UEFI Amazon Elastic Block Store vol-xyz
     ```

   - Führen Sie den folgenden Befehl aus, um zu überprüfen, ob das Verzeichnis `/sys/firmware/efi` vorhanden ist. Dieses Verzeichnis ist nur dann vorhanden, wenn die Instance mit UEFI gestartet wird. Wenn das Verzeichnis nicht vorhanden ist, gibt der Befehl zurück `Legacy BIOS Boot Detected`.

     ```
     [ec2-user ~]$ [ -d /sys/firmware/efi ] && echo "UEFI Boot Detected" || echo
      "Legacy BIOS Boot Detected"
     ```

Erwartete Ausgabe einer im UEFI-Startmodus gestarteten Instance

```
UEFI Boot Detected
```

Erwartete Ausgabe einer im Legacy-System BIOS-Startmodus gestarteten Instance

```
Legacy BIOS Boot Detected
```

- Führen Sie den folgenden Befehl aus, um zu überprüfen, ob EFI in der Ausgabe `dmesg` enthalten ist.

```
[ec2-user ~]$ dmesg | grep -i "EFI"
```

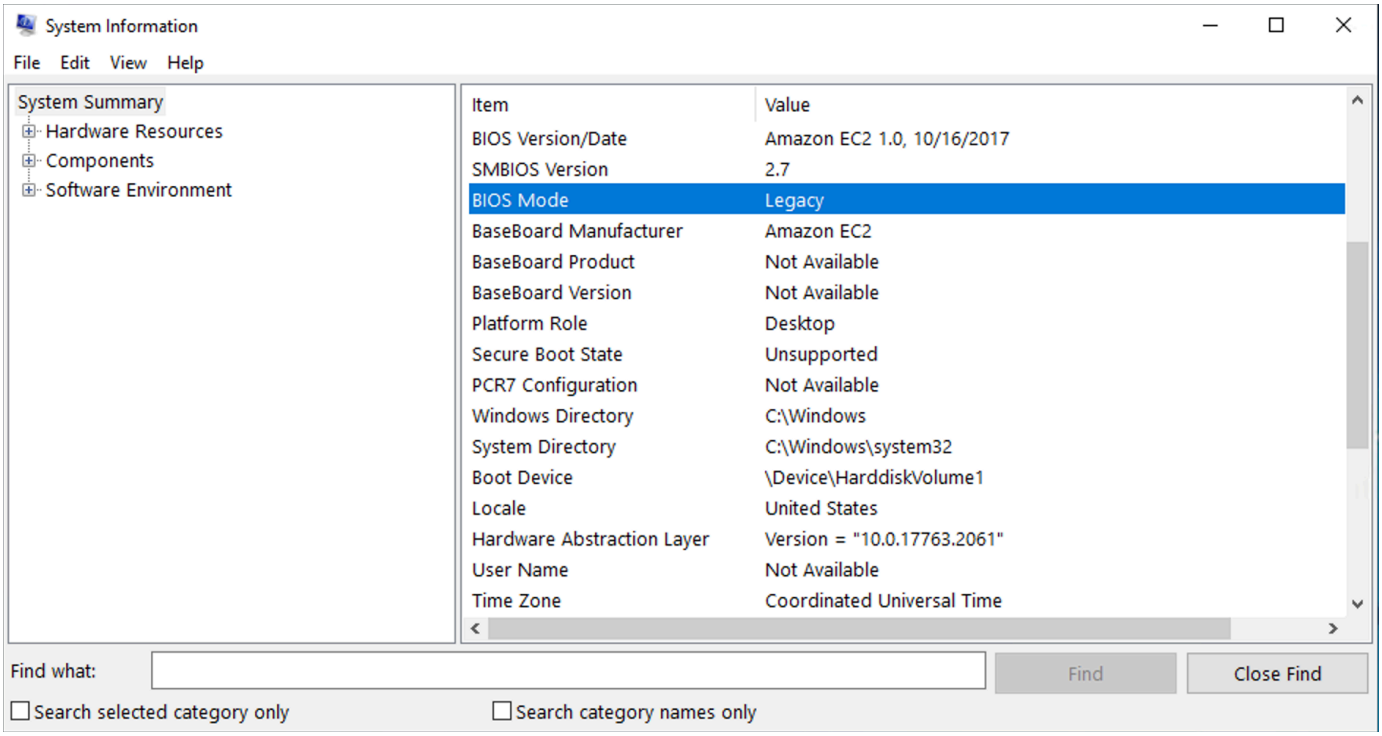
Erwartete Ausgabe einer im UEFI-Startmodus gestarteten Instance

```
[    0.000000] efi: Getting EFI parameters from FDT:
[    0.000000] efi: EFI v2.70 by EDK II
```

Windows

Ermitteln des Startmodus des Betriebssystems der Instance

1. Stellen Sie eine Verbindung mit Ihrer Windows-Instance mithilfe von RDP her.
2. Wechseln Sie zu Systeminformationen und überprüfen Sie die Zeile BIOS-Modus.



Den Bootmodus eines Amazon-EC2-AMIs festlegen

Standardmäßig übernimmt das AMI den Startmodus der EC2-Instance, die zum Erstellen des AMI verwendet wird. Wenn Sie beispielsweise ein AMI aus einer EC2-Instance erstellen, die mit Legacy BIOS ausgeführt wird, ist der Startmodus des neuen AMI `legacy-bios`. Wenn Sie ein AMI aus einer EC2-Instance mit dem Startmodus `uefi-preferred` erstellen, ist der Startmodus des neuen AMI `uefi-preferred`.

Wenn Sie ein AMI registrieren, können Sie den Startmodus des AMI auf `uefi`, `legacy-bios` oder `uefi-preferred` festlegen.

Wenn der AMI-Startmodus auf `uefi-preferred` gesetzt ist, startet die Instance wie folgt:

- Bei Instance-Typen, die sowohl UEFI als auch Legacy BIOS unterstützen (z. B. `m5.large`), startet die Instance mit UEFI.
- Bei Instance-Typen, die nur Legacy BIOS unterstützen (z. B. `m4.large`), startet die Instance mit Legacy BIOS.

Wenn Sie den AMI-Startmodus auf `uefi-preferred` einstellen, muss das Betriebssystem die Fähigkeit unterstützen, sowohl UEFI als auch Legacy BIOS zu starten.

Um eine vorhandene Legacy-BIOS-basierte Instance in UEFI oder eine vorhandene UEFI-basierte Instance in Legacy BIOS zu konvertieren, müssen Sie zunächst das Volume und das Betriebssystem der Instance anpassen, damit der ausgewählte Startmodus unterstützt wird. Erstellen Sie dann einen Snapshot des Volumes. Erstellen Sie zuletzt ein AMI aus dem Snapshot.

Überlegungen

- Durch das Festlegen des AMI-Startmodus-Parameters wird das Betriebssystem nicht automatisch für den angegebenen Startmodus konfiguriert. Sie müssen zuerst entsprechende Änderungen am Volume und am Betriebssystem der Instance vornehmen, um den Start mit dem ausgewählten Startmodus zu unterstützen. Andernfalls kann das resultierende AMI nicht verwendet werden. Wenn Sie beispielsweise eine Legacy-BIOS-basierte Instance zu UEFI umwandeln, können Sie das Tool MBR2GPT von Microsoft verwenden, um die Systemfestplatte von MBR zu GPT zu konvertieren. Die erforderlichen Änderungen sind betriebssystemspezifisch. Weitere Informationen finden Sie im Handbuch zu Ihrem Betriebssystem.
- Sie können nicht den Befehl register-image oder das cmdlet Register-EC2Image verwenden, um ein AMI zu erstellen, das sowohl NitroTPM als auch UEFI Preferred unterstützt.
- Einige Features, wie UEFI Secure Boot, sind nur auf Instances verfügbar, die auf UEFI gestartet werden. Wenn Sie den `uefi-preferred`-AMI-Startmodus-Parameter mit einem Instance-Typ verwenden, der UEFI nicht unterstützt, wird die Instance als Legacy-BIOS gestartet und das UEFI-abhängige Feature wird deaktiviert. Wenn Sie auf die Verfügbarkeit eines UEFI-abhängigen Features angewiesen sind, setzen Sie Ihren AMI-Startmodus-Parameter auf `uefi`.

AWS CLI

So legen Sie den Startmodus für ein AMI fest

1. Nehmen Sie entsprechende Änderungen am Volume und am Betriebssystem der Instance vor, um den Start mit dem ausgewählten Startmodus zu unterstützen. Die erforderlichen Änderungen sind betriebssystemspezifisch. Weitere Informationen finden Sie im Handbuch zu Ihrem Betriebssystem.

   > **Warning**
   >
   > Wenn Sie diesen Schritt nicht ausführen, ist das AMI nicht verwendbar.

2. Um die Volume-ID der Instance zu ermitteln, verwenden Sie den Befehl describe-instances. Im nächsten Schritt erstellen Sie einen Snapshot des Volumes.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].BlockDeviceMappings
```

Es folgt eine Beispielausgabe.

```
[
    [
        {
            "DeviceName": "/dev/xvda",
            "Ebs": {
                "AttachTime": "2024-07-11T01:05:51+00:00",
                "DeleteOnTermination": true,
                "Status": "attached",
                "VolumeId": "vol-1234567890abcdef0"
            }
        }
    ]
]
```

3. Um einen Snapshot des Volumes zu erstellen, verwenden Sie den Befehl create-snapshot. Verwenden Sie die Volume-ID aus dem vorherigen Schritt.

```
aws ec2 create-snapshot \
    --volume-id vol-01234567890abcdef \
    --description "my snapshot"
```

Es folgt eine Beispielausgabe.

```
{
    "Description": "my snapshot",
    "Encrypted": false,
    "OwnerId": "123456789012",
    "Progress": "",
    "SnapshotId": "snap-0abcdef1234567890",
    "StartTime": "",
    "State": "pending",
    "VolumeId": "vol-01234567890abcdef",
    "VolumeSize": 30,
    "Tags": []
```

```
}
```

4. Warten Sie bis der Status des Snapshots `completed` lautet, bevor Sie mit dem nächsten Schritt fortfahren. Um den Status des Snapshots abzufragen, verwenden Sie den describe-snapshots-Befehl mit der Snapshot-ID aus dem vorherigen Schritt.

```
aws ec2 describe-snapshots \
    --snapshot-ids snap-0abcdef1234567890 \
    --query Snapshots[].State \
    --output text
```

Es folgt eine Beispielausgabe.

```
completed
```

5. Verwenden Sie den Befehl register-image, um ein neues AMI zu erstellen. Kopieren Sie den Wert von `SnapshotId` aus der Ausgabe von CreateSnapshot.

- Um den Startmodus auf UEFI festzulegen, fügen Sie den Parameter `--boot-mode` mit einem Wert von `uefi` hinzu.

```
aws ec2 register-image \
   --description "my image" \
   --name "my-image" \
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-0abcdef1234567890,DeleteOnTermination=true}" \
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
   --ena-support \
   --boot-mode uefi
```

- Um den Startmodus auf `uefi-preferred` einzustellen, legen Sie den Wert von `--boot-mode` auf `uefi-preferred` fest.

```
aws ec2 register-image \
   --description "my description" \
   --name "my-image" \
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-0abcdef1234567890,DeleteOnTermination=true}" \
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
```

```
    --ena-support \
    --boot-mode uefi-preferred
```

6. (Optional) Um zu überprüfen, ob das neu erstellte AMI den angegebenen Startmodus aufweist, verwenden Sie den Befehl describe-images.

```
aws ec2 describe-images \
    --image-id ami-1234567890abcdef0 \
    --query Images[].BootMode \
    --output text
```

Es folgt eine Beispielausgabe.

```
uefi
```

PowerShell

So legen Sie den Startmodus für ein AMI fest

1. Nehmen Sie entsprechende Änderungen am Volume und am Betriebssystem der Instance vor, um den Start mit dem ausgewählten Startmodus zu unterstützen. Die erforderlichen Änderungen sind betriebssystemspezifisch. Weitere Informationen finden Sie im Handbuch zu Ihrem Betriebssystem.

> **Warning**
>
> Wenn Sie diesen Schritt nicht ausführen, ist das AMI nicht verwendbar.

2. Um die Volume-ID der Instance zu ermitteln, verwenden Sie das cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.BlockDeviceMappings.Ebs
```

Es folgt eine Beispielausgabe.

```
AssociatedResource  :
AttachTime          : 7/11/2024 1:05:51 AM
DeleteOnTermination : True
Operator            :
```

```
Status              : attached
VolumeId            : vol-01234567890abcdef
```

3. Um einen Snapshot des Volumes zu erstellen, verwenden Sie das cmdlet New-EC2Snapshot. Verwenden Sie die Volume-ID aus dem vorherigen Schritt.

```
New-EC2Snapshot `
    -VolumeId vol-01234567890abcdef `
    -Description "my snapshot"
```

Es folgt eine Beispielausgabe.

```
AvailabilityZone          :
Description               : my snapshot
Encrypted                 : False
FullSnapshotSizeInBytes   : 0
KmsKeyId                  :
OwnerId                   : 123456789012
RestoreExpiryTime         :
SnapshotId                : snap-0abcdef1234567890
SseType                   :
StartTime                 : 4/25/2025 6:08:59 PM
State                     : pending
StateMessage              :
VolumeId                  : vol-01234567890abcdef
VolumeSize                : 30
```

4. Warten Sie bis der Status des Snapshots `completed` lautet, bevor Sie mit dem nächsten Schritt fortfahren. Um den Status des Snapshots abzufragen, verwenden Sie das cmdlet Get-EC2Snapshot mit der Snapshot-ID aus dem vorherigen Schritt.

```
(Get-EC2Snapshot `
    -SnapshotId snap-0abcdef1234567890).State.Value
```

Es folgt eine Beispielausgabe.

```
completed
```

5. Verwenden Sie das cmdlet Register-EC2Image, um ein neues AMI zu erstellen. Kopieren Sie den Wert von `SnapshotId` aus der Ausgabe von New-EC2Snapshot.

- Um den Startmodus auf UEFI festzulegen, fügen Sie den Parameter `-BootMode` mit einem Wert von `uefi` hinzu.

```
$block = @{SnapshotId=snap-0abcdef1234567890}
Register-EC2Image `
   -Description "my image" `
   -Name "my-image" `
   -BlockDeviceMapping @{DeviceName="/dev/xvda";Ebs=$block} `
   -RootDeviceName /dev/xvda `
   -EnaSupport $true `
   -BootMode uefi
```

- Um den Startmodus auf `uefi-preferred` einzustellen, legen Sie den Wert von `-BootMode` auf `uefi-preferred` fest.

```
$block = @{SnapshotId=snap-0abcdef1234567890}
Register-EC2Image `
   -Description "my image" `
   -Name "my-image" `
   -BlockDeviceMapping @{DeviceName="/dev/xvda";Ebs=$block} `
   -RootDeviceName /dev/xvda `
   -EnaSupport $true `
   -BootMode uefi-preferred
```

6. (Optional) Um zu überprüfen, ob das neu erstellte AMI den angegebenen Startmodus aufweist, verwenden Sie das cmdlet Get-EC2Image.

```
(Get-EC2Image `
    -ImageId ami-1234567890abcdef0).BootMode.Value
```

Es folgt eine Beispielausgabe.

```
uefi
```

UEFI-Variablen für Amazon-EC2-Instances

Wenn Sie eine Instance starten, für die der Startmodus auf UEFI eingestellt ist, wird eine Schlüssel-Werte-Datenbank für Variablen erstellt. Der Speicher kann von UEFI und dem Instance-Betriebssystem zum Speichern von UEFI-Variablen verwendet werden.

UEFI-Variablen werden vom Bootloader und dem Betriebssystem verwendet, um den frühen System-Startup zu konfigurieren. Sie ermöglichen es dem Betriebssystem, bestimmte Einstellungen des Startvorgangs zu verwalten, wie die Startreihenfolge oder die Verwaltung der Schlüssel für UEFI Secure Boot.

> **Warning**
>
> Jeder, der eine Verbindung mit der Instance herstellen kann (und potenziell jede Software, die auf der Instance läuft), oder jeder, der die Berechtigung hat, die GetInstanceUefiData-API auf der Instance zu verwenden, kann die Variablen lesen. Speichern Sie sensible Daten wie Passwörter oder personenbezogene Daten niemals im UEFI-Variablenspeicher.

UEFI-Variablen-Persistenz

- Bei Instances, die an oder vor dem 10. Mai 2022 gestartet wurden, werden UEFI-Variablen beim Neustart oder Stopp gelöscht.
- Bei Instances, die am oder nach dem 11. Mai 2022 gestartet werden, werden UEFI-Variablen, die als nicht flüchtig gekennzeichnet sind, beim Neustart und Stopp/Start beibehalten.
- Bare-Metal-Instances behalten nicht flüchtige UEFI-Variablen über Instance-Stopp-/Start-Vorgänge hinweg nicht bei.

UEFI Secure Boot für Amazon-EC2-Instances

UEFI Secure Boot baut auf dem langjährigen sicheren Boot-Prozess von Amazon EC2 auf und bietet zusätzlichen tiefgreifende Verteidigung, die Ihnen dabei hilft, Software vor Bedrohungen zu schützen, die auch Reboots überleben. Es stellt sicher, dass die Instance nur Software startet, die mit kryptografischen Schlüsseln signiert ist. Die Schlüssel werden in der Schlüsseldatenbank des UEFI nicht flüchtige Variablenspeicher gespeichert. UEFI Secure Boot verhindert die unbefugte Änderung des Bootflows der Instance.

Inhalt

- Wie UEFI Secure Boot mit Amazon-EC2-Instances funktioniert
- Anforderungen für UEFI Secure Boot in Amazon EC2
- Überprüfen, ob eine Amazon-EC2-Instance für UEFI Secure Boot aktiviert ist
- Ein Linux-AMI mit benutzerdefinierten UEFI-Secure-Boot-Schlüsseln erstellen

- AWS-Binärblob für UEFI Secure Boot erstellen

Wie UEFI Secure Boot mit Amazon-EC2-Instances funktioniert

UEFI Secure Boot ist ein in UEFI spezifiziertes Feature, das eine Überprüfung des Status der Bootchain ermöglicht. Sie soll sicherstellen, dass nach der Selbstinitialisierung der Firmware nur kryptographisch verifizierte UEFI-Binärdateien ausgeführt werden. Zu diesen Binärdateien gehören UEFI-Treiber und der Haupt-Bootloader sowie kettengeladene Komponenten.

UEFI Secure Boot spezifiziert vier wichtige Datenbanken, die in einer Vertrauenskette verwendet werden. Die Datenbanken werden im UEFI-Variablenspeicher gespeichert.

Die Vertrauenskette lautet wie folgt:

Plattformschlüssel (PK)-Datenbank

Die PK-Datenbank ist der Vertrauensanker. Sie enthält einen einzigen öffentlichen PK-Schlüssel, der in der Vertrauenskette zum Aktualisieren der Schlüsselaustausch-Schlüssel (KEK)-Datenbank verwendet wird.

Um die PK-Datenbank zu ändern, benötigen Sie den privaten PK-Schlüssel, um eine Aktualisierungsanforderung zu signieren. Dies beinhaltet das Löschen der PK-Datenbank durch Schreiben eines leeren PK-Schlüssels.

Schlüsselaustausch-Schlüssel (KEK)-Datenbank

Die KEK-Datenbank ist eine Liste öffentlicher KEK-Schlüssel, die in der Vertrauenskette zum Aktualisieren der Signatur (db)- und Deny-Liste (dbx)-Datenbanken verwendet werden.

Um die um die öffentliche KEK-Datenbank zu ändern, benötigen Sie den privaten PK-Schlüssel, um eine Aktualisierungsanforderung zu signieren.

Signatur (db)-Datenbank

Die db-Datenbank ist eine Liste von öffentlichen Schlüsseln und Hashes, die in der Vertrauenskette verwendet werden, um alle UEFI-Boot-Binärdateien zu validieren.

Um die db-Datenbank zu ändern, benötigen Sie den privaten PK-Schlüssel einen der privaten KEK-Schlüssel, um eine Aktualisierungsanforderung zu signieren.

Signatur-Deny-Liste (dbx)-Datenbank

Die dbx-Datenbank ist eine Liste von öffentlichen Schlüsseln und binären Hashes, die nicht vertrauenswürdig sind und in der Vertrauenskette als Widerrufsdatei verwendet werden.

Die dbx-Datenbank hat immer Vorrang vor allen anderen wichtigen Datenbanken.

Um die dbx-Datenbank zu ändern, benötigen Sie den privaten PK-Schlüssel oder einen der privaten KEK-Schlüssel, um eine Aktualisierungsanforderung zu signieren.

Das UEFI-Forum unterhält eine öffentlich zugängliche dbx für viele bekanntermaßen fehlerhafte Binärdateien und Zertifikate unter https://uefi.org/revocationlistfile.

Important

UEFI Secure Boot erzwingt die Signaturvalidierung für alle UEFI-Binärdateien. Um die Ausführung einer UEFI-Binärdatei in UEFI Secure Boot zu erlauben, signieren Sie sie mit einem der oben beschriebenen privaten db-Schlüssel.

Standardmäßig ist UEFI Secure Boot deaktiviert und das System befindet sich im `SetupMode`. Wenn sich das System im `SetupMode` befindet, können alle Schlüsselvariablen ohne kryptografische Signatur aktualisiert werden. Wenn die PK eingestellt ist, ist UEFI Secure Boot aktiviert und der Setup-Modus wird beendet.

Anforderungen für UEFI Secure Boot in Amazon EC2

Wenn Sie eine Amazon-EC2-Instance mit einem unterstützten AMI und einem unterstützten Instance-Typ starten, validiert diese Instance automatisch UEFI-Boot-Binärdateien anhand ihrer UEFI-Secure-Boot-Datenbank. Es ist keine zusätzliche Konfiguration erforderlich. Sie können UEFI Secure Boot auch nach dem Start für eine Instance konfigurieren.

Note

UEFI Secure Boot schützt Ihre Instance und ihr Betriebssystem vor Änderungen im Bootflow. Wenn Sie ein neues AMI aus einem Quell-AMI erstellen, bei dem UEFI Secure Boot aktiviert ist, und bestimmte Parameter während des Kopiervorgangs ändern, wie beispielsweise die `UefiData` innerhalb des AMI, können Sie UEFI Secure Boot deaktivieren.

Inhalt

- Unterstützte AMIs
- Unterstützte Instance-Typen

Unterstützte AMIs

Linux-AMIs

Um eine Linux-Instance zu starten, muss für das Linux-AMI UEFI Secure Boot aktiviert sein.

Amazon Linux unterstützt UEFI Secure Boot ab AL2023 Release 2023.1. UEFI Secure Boot ist jedoch in den Standard-AMIs nicht aktiviert. Weitere Informationen finden Sie unter UEFI Secure Boot im AL2023 Benutzerhandbuch. Ältere Versionen von Amazon-Linux-AMIs sind für UEFI Secure Boot nicht aktiviert. Um ein unterstütztes AMI zu verwenden, müssen Sie eine Reihe von Konfigurationsschritten für Ihr eigenes Linux-AMI ausführen. Weitere Informationen finden Sie unter Ein Linux-AMI mit benutzerdefinierten UEFI-Secure-Boot-Schlüsseln erstellen.

Windows-AMIs

Um eine Windows-Instance zu starten, muss für das Windows-AMI UEFI Secure Boot aktiviert sein. Informationen zum suchen eines AWS-Windows-AMI, das für UEFI Secure Boot mit Microsoft-Schlüsseln vorkonfiguriert ist, finden Sie unter Suchen von Windows-Server-AMIs, die mit NitroTPM und UEFI Secure Boot konfiguriert sind in der AMI-Referenz für AWS Windows.

Derzeit wird das Importieren von Windows mit UEFI Secure Boot über den Befehl import-image nicht unterstützt.

Unterstützte Instance-Typen

Alle virtualisierten Instance-Typen, die UEFI unterstützen, unterstützen auch UEFI Secure Boot. Informationen zu den Instance-Typen, die UEFI Secure Boot unterstützen, finden Sie unter Anforderungen für den UEFI-Bootmodus.

> **Note**
>
> Bare-Metal-Instance-Typen unterstützen UEFI Secure Boot nicht.

Überprüfen, ob eine Amazon-EC2-Instance für UEFI Secure Boot aktiviert ist

Sie können die folgenden Verfahren verwenden, um festzustellen, ob ein Amazon EC2 für UEFI Secure Boot aktiviert ist.

Linux-Instances

Sie können das `mokutil`-Serviceprogramm verwenden, um zu überprüfen, ob eine Linux Instance für UEFI Secure Boot freigegeben ist. Wenn `mokutil` nicht auf Ihrer Instance installiert ist, müssen Sie es installieren. Die Installationsanweisungen für Amazon Linux 2 finden Sie unter Suchen und Installieren von Softwarepaketen auf einer Amazon-Linux-2-Instance. Für andere Linux-Verteilungen schauen Sie in der spezifischen Dokumentation.

So überprüfen Sie, ob eine Linux-Instance für UEFI Secure Boot aktiviert ist

Verbinden Sie sich mit Ihrer Instance und führen Sie den folgenden Befehl als `root` in einem Terminal-Fenster aus.

```
mokutil --sb-state
```

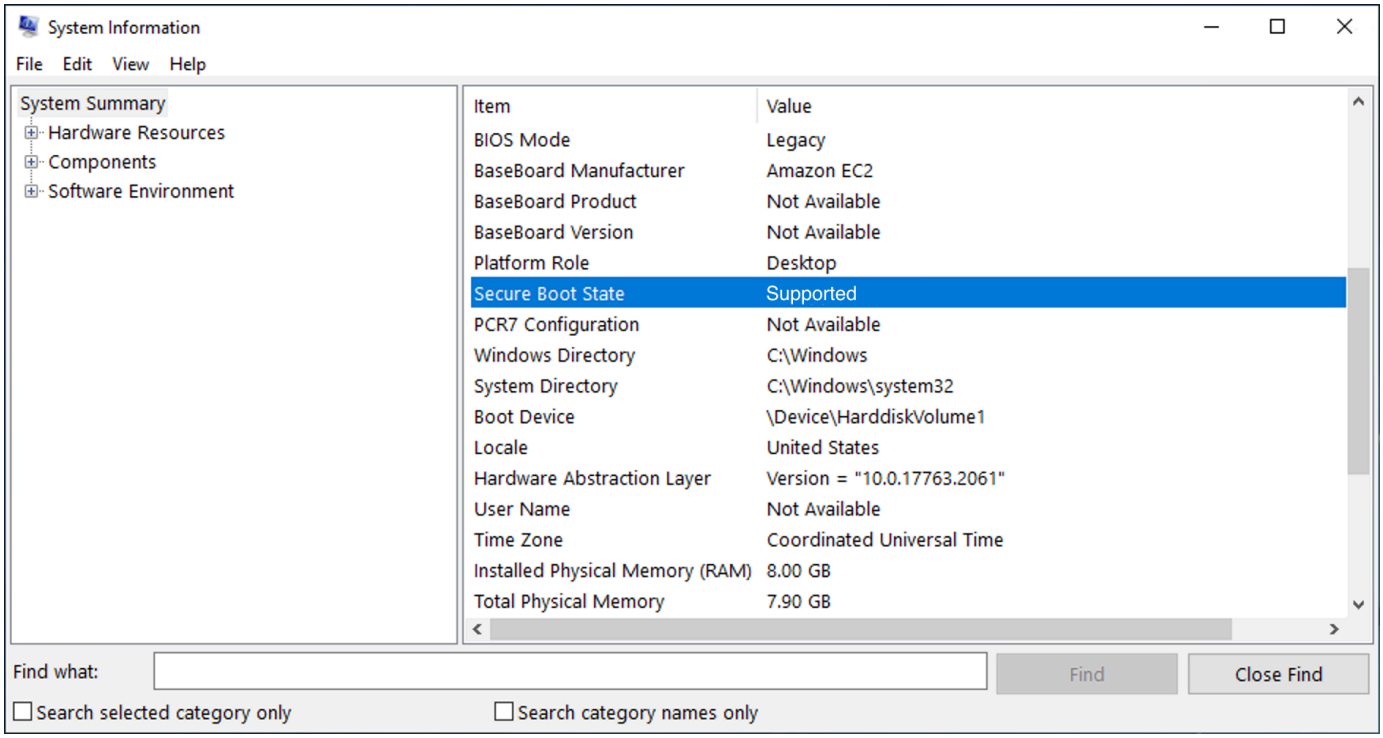
Es folgt eine Beispielausgabe.

- Wenn UEFI Secure Boot aktiviert ist, enthält die Ausgabe `SecureBoot enabled`.
- Wenn UEFI Secure Boot nicht aktiviert ist, enthält die Ausgabe `SecureBoot disabled` oder `Failed to read SecureBoot`.

Windows-Instances

So überprüfen Sie, ob eine Windows-Instance für UEFI Secure Boot aktiviert ist

1. Verbinden Sie sich mit der Instance.
2. Öffnen Sie das msinfo32-Tool.
3. Überprüfen Sie das Feld Secure Boot State (Sicherer Boot-Status). Wenn UEFI Secure Boot aktiviert ist, lautet der Wert Unterstützt, wie in der folgenden Abbildung dargestellt.



Sie können auch das Windows PowerShell Cmdlet `Confirm-SecureBootUEFI` verwenden, um den Secure-Boot-Status zu überprüfen. Weitere Informationen zum Cmdlet finden Sie unter Confirm-SecureBootUEFI in der Microsoft-Dokumentation.

Ein Linux-AMI mit benutzerdefinierten UEFI-Secure-Boot-Schlüsseln erstellen

Diese Anleitung zeigt Ihnen, wie Sie ein Linux-AMI mit UEFI Secure Boot und benutzerdefinierten privaten Schlüsseln erstellen. Amazon Linux unterstützt UEFI Secure Boot ab AL2023 Release 2023.1. Weitere Informationen finden Sie unter UEFI Secure Boot in AL2023 im Benutzerhandbuch für Amazon Linux 2023.

> **Important**
>
> Das folgende Verfahren ist nur für fortgeschrittene Benutzer vorgesehen. Sie müssen über ausreichende Kenntnisse im Bootflow der SSL- und Linux-Distribution verfügen, um diese Verfahren verwenden zu können.

Voraussetzungen

- Die folgenden Tools werden verwendet:

- OpenSSL – https://www.openssl.org/
- efivar – https://github.com/rhboot/efivar
- efitools – https://git.kernel.org/pub/scm/linux/kernel/git/jejb/efitools.git/
- Befehl get-instance-uefi-data

- Ihre Linux-Instance muss mit einem Linux-AMI gestartet worden sein, das den UEFI-Startmodus unterstützt und es müssen nichtflüchtige Daten vorhanden sein.

Neu erstellte Instances ohne UEFI Secure Boot-Schlüssel werden in `SetupMode` erstellt, wodurch Sie Ihre eigenen Schlüssel registrieren können. Einige AMIs sind mit UEFI Secure Boot vorkonfiguriert und Sie können die vorhandenen Schlüssel nicht ändern. Wenn Sie die Schlüssel ändern möchten, müssen Sie ein neues AMI basierend auf dem ursprünglichen AMI erstellen.

Sie haben zwei Möglichkeiten, die Schlüssel im Variablenspeicher zu propagieren, die in den folgenden Optionen A und B beschrieben sind. Option A beschreibt, wie dies innerhalb der Instance geschieht und den Fluss echter Hardware nachahmt. Option B beschreibt, wie ein binäres Blob erstellt wird, das dann als base64-kodierte Datei übergeben wird, wenn Sie das AMI erstellen. Für beide Optionen müssen Sie zuerst die drei Schlüsselpaare erstellen, die für die Vertrauenskette verwendet werden.

Um ein Linux-AMI zur Unterstützung von UEFI Secure Boot zu erstellen, erstellen Sie zuerst die drei Schlüsselpaare und führen Sie dann entweder Option A oder Option B, aber nicht beide aus:

- Aufgabe 1: Schlüsselpaare erstellen
- Aufgabe 2 – Option A: Fügen Sie innerhalb der Instance Schlüssel zum Variablenspeicher hinzu
- Aufgabe 2 – Option B: Erstellen Sie ein binäres Blob mit einem vorgefüllten Variablenspeicher

Aufgabe 1: Schlüsselpaare erstellen

UEFI Secure Boot basiert auf den folgenden drei Schlüsseldatenbanken, die in einer Vertrauenskette verwendet werden: dem Plattformschlüssel (PK), dem Schlüsselaustauschschlüssel (KEK) und der Signaturdatenbank (db).[1]

Sie erstellen jeden Schlüssel auf der Instance. Um die öffentlichen Schlüssel in einem Format vorzubereiten, das für den UEFI Secure Boot-Standard gültig ist, erstellen Sie für jeden Schlüssel ein Zertifikat. `DER` definiert das SSL-Format (Binärkodierung eines Formats). Anschließend konvertieren Sie jedes Zertifikat in eine UEFI-Signaturliste, bei der es sich um das Binärformat handelt, das

von UEFI Secure Boot verstanden wird. Und schließlich signieren Sie jedes Zertifikat mit dem entsprechenden Schlüssel.

Aufgaben

- Bereiten Sie die Erstellung der Schlüsselpaare vor
- Schlüsselpaar 1: Erstellen Sie den Plattformschlüssel (PK)
- Schlüsselpaar 2: Erstellen Sie den Schlüsselaustauschschlüssel (KEK)
- Schlüsselpaar 3: Erstellen Sie die Signaturdatenbank (db)
- Signieren Sie das Boot-Image (Kernel) mit dem privaten Schlüssel.

Bereiten Sie die Erstellung der Schlüsselpaare vor

Erstellen Sie vor dem Erstellen der Schlüsselpaare einen global eindeutigen Bezeichner (GUID), der bei der Schlüsselgenerierung verwendet werden soll.

1. Stellen Sie eine Verbindung zur Instance her.
2. Führen Sie in der Eingabeaufforderung einen Shell-Befehl aus.

```
uuidgen --random > GUID.txt
```

Schlüsselpaar 1: Erstellen Sie den Plattformschlüssel (PK)

Der PK ist der Vertrauensanker für UEFI Secure Boot-Instances. Die private PK wird verwendet, um den KEK zu aktualisieren, der wiederum dazu verwendet werden kann, autorisierte Schlüssel zur Signaturdatenbank (db) hinzuzufügen.

Der X.509-Standard wird zum Erstellen des Schlüsselpaars verwendet. Informationen zum Standard finden Sie unter X.509 auf Wikipedia.

So erstellen Sie den PK

1. Erstellen Sie den Schlüssel. Sie müssen die Variable benennen PK.

```
openssl req -newkey rsa:4096 -nodes -keyout PK.key -new -x509 -sha256 -days 3650 -
subj "/CN=Platform key/" -out PK.crt
```

   Die folgenden Parameter werden angegeben:

- `-keyout PK.key` – Die private Schlüsseldatei.
- `-days 3650` – Die Anzahl der Tage, an denen das Zertifikat gültig ist.
- `-out PK.crt` – Das Zertifikat, das zum Erstellen der UEFI-Variablen verwendet wird.
- `CN=`*`Platform key`* – Der gemeinsame Name (common name, CN) für den Schlüssel. Sie können den Namen Ihrer eigenen Organisation eingeben anstatt des *`Plattformschlüssels`*.

2. Erstellen Sie das Zertifikat.

```
openssl x509 -outform DER -in PK.crt -out PK.cer
```

3. Wandeln Sie das Zertifikat in eine UEFI-Signaturliste um.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" PK.crt PK.esl
```

4. Signieren Sie die UEFI-Signaturliste mit dem privaten PK (selbstsigniert).

```
sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt PK PK.esl PK.auth
```

Schlüsselpaar 2: Erstellen Sie den Schlüsselaustauschschlüssel (KEK)

Der private KEK wird verwendet, um Schlüssel zur Datenbank hinzuzufügen, was die Liste der autorisierten Signaturen darstellt, die im System gestartet werden sollen.

So erstellen Sie den KEK

1. Erstellen Sie den Schlüssel.

```
openssl req -newkey rsa:4096 -nodes -keyout KEK.key -new -x509 -sha256 -days 3650 -
subj "/CN=Key Exchange Key/" -out KEK.crt
```

2. Erstellen Sie das Zertifikat.

```
openssl x509 -outform DER -in KEK.crt -out KEK.cer
```

3. Wandeln Sie das Zertifikat in eine UEFI-Signaturliste um.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" KEK.crt KEK.esl
```

4. Signieren Sie die Signaturliste mit dem privaten PK.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt KEK KEK.esl KEK.auth
```

Schlüsselpaar 3: Erstellen Sie die Signaturdatenbank (db)

Die db-Liste enthält autorisierte Schlüssel, die zum Booten auf dem System autorisiert sind. Um die Liste zu ändern, ist der private KEK erforderlich. Boot-Images werden mit dem privaten Schlüssel signiert, der in diesem Schritt erstellt wird.

So erstellen Sie den db

1. Erstellen Sie den Schlüssel.

```
openssl req -newkey rsa:4096 -nodes -keyout db.key -new -x509 -sha256 -days 3650 -
subj "/CN=Signature Database key/" -out db.crt
```

2. Erstellen Sie das Zertifikat.

```
openssl x509 -outform DER -in db.crt -out db.cer
```

3. Wandeln Sie das Zertifikat in eine UEFI-Signaturliste um.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" db.crt db.esl
```

4. Signieren Sie die Signaturliste mit dem privaten KEK.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k KEK.key -c KEK.crt db db.esl db.auth
```

Signieren Sie das Boot-Image (Kernel) mit dem privaten Schlüssel.

Für Ubuntu 22.04 erfordern die folgenden Images Signaturen.

```
/boot/efi/EFI/ubuntu/shimx64.efi
/boot/efi/EFI/ubuntu/mmx64.efi
/boot/efi/EFI/ubuntu/grubx64.efi
/boot/vmlinuz
```

So signieren Sie ein Image

Verwenden Sie die folgende Syntax, um ein Image zu signieren.

```
sbsign --key db.key --cert db.crt --output /boot/vmlinuz /boot/vmlinuz
```

> **Note**
>
> Sie müssen alle neuen Kernel signieren. */boot/vmlinuz* wird normalerweise einen Link zum zuletzt installierten Kernel führen.

In der Dokumentation Ihrer Distribution erfahren Sie mehr über Ihre Bootchain und die erforderlichen Images.

[1] Danke an die ArchWiki-Community für all die Arbeit, die sie geleistet haben. Die Befehle zum Erstellen des PK, zum Erstellen des KEK, zum Erstellen der DB und zum Signieren des Images stammen aus Erstellen von Schlüsseln, verfasst vom ArchWiki-Wartungsteam und/oder den ArchWiki-Mitwirkenden.

Aufgabe 2 – Option A: Fügen Sie innerhalb der Instance Schlüssel zum Variablenspeicher hinzu

Nachdem Sie die drei Schlüsselpaare erstellt haben, können Sie eine Verbindung zu Ihrer Instance herstellen und die Schlüssel innerhalb der Instance zum Variablenspeicher hinzufügen, indem Sie die folgenden Schritte ausführen. Führen Sie alternativ die Schritte unter the section called “Aufgabe 2 – Option B: Erstellen Sie ein binäres Blob mit einem vorgefüllten Variablenspeicher” aus.

Option A Schritte:

- Schritt 1: Starten Sie eine Instance mit UEFI Secure Boot-Unterstützung
- Schritt 2: Konfigurieren Sie eine Instance zur Unterstützung von UEFI Secure Boot
- Schritt 3: Erstellen eines AMI Ihrer Instance

Schritt 1: Starten Sie eine Instance mit UEFI Secure Boot-Unterstützung

Wenn Sie mit den folgenden Voraussetzungen eine Instance starten, kann die Instance dann für die Unterstützung von UEFI Secure Boot konfiguriert werden. Sie können die Unterstützung für UEFI Secure Boot nur für eine Instance beim Start aktivieren; Sie können sie später nicht aktivieren.

Voraussetzungen

- AMI – Das Linux-AMI muss den UEFI-Startmodus unterstützen. Um zu überprüfen, ob das AMI den UEFI-Startmodus unterstützt, muss der AMI-Startmodus-Parameter uefi sein. Weitere Informationen finden Sie unter Den Bootmodus-Parameter für ein Amazon-EC2-AMI bestimmen.

  Beachten Sie, dass AWS nur Linux-AMIs zur Verfügung stellt, die für die Unterstützung von UEFI für Graviton-basierte Instance-Typen konfiguriert sind. AWS stellt derzeit keine x86_64-Linux-AMIs bereit, die den UEFI-Startmodus unterstützen. Sie können Ihr eigenes AMI so konfigurieren, dass es den UEFI-Boot-Modus für alle Architekturen unterstützt. Um ein Ihren eigenes AMI für die Unterstützung des UEFI-Startmodus zu konfigurieren, müssen Sie eine Reihe von Konfigurationsschritten auf Ihrem eigenen AMI durchführen. Weitere Informationen finden Sie unter Den Bootmodus eines Amazon-EC2-AMIs festlegen.
- Instance-Typ – Alle virtualisierten Instance-Typen, die UEFI unterstützen, unterstützen auch UEFI Secure Boot. Bare-Metal-Instance-Typen unterstützen UEFI Secure Boot nicht. Informationen zu den Instance-Typen, die UEFI Secure Boot unterstützen, finden Sie unter Anforderungen für den UEFI-Bootmodus.
- Starten Sie Ihre Instance nach dem Veröffentlichen von UEFI Secure Boot. Nur Instances, die nach dem 10. Mai 2022 (als UEFI Secure Boot veröffentlicht wurde) gestartet wurden, können UEFI Secure Boot unterstützen.

Nachdem Sie Ihre Instance gestartet haben, können Sie überprüfen, ob sie für die Unterstützung von UEFI Secure Boot konfiguriert werden kann (mit anderen Worten, Sie können mit Schritt 2 fortfahren), indem Sie prüfen, ob UEFI-Daten vorhanden sind. Das Vorhandensein von UEFI-Daten weist darauf hin, dass nichtflüchtige Daten beibehalten werden.

So überprüfen Sie, ob die Instance für Schritt 2 bereit ist

Verwenden Sie den Befehl get-instance-uefi-data und geben Sie die Instance-ID an.

```
aws ec2 get-instance-uefi-data --instance-id i-1234567890abcdef0
```

Die Instance ist bereit für Schritt 2, wenn UEFI-Daten in der Ausgabe vorhanden sind. Wenn die Ausgabe leer ist, kann die Instance nicht für die Unterstützung von UEFI Secure Boot konfiguriert werden. Dies kann passieren, wenn Ihre Instance gestartet wurde, bevor die UEFI Secure Boot-Unterstützung verfügbar wurde. Starten Sie eine neue Instance und versuchen Sie es erneut.

Schritt 2: Konfigurieren Sie eine Instance zur Unterstützung von UEFI Secure Boot

Registrieren Sie die Schlüsselpaare in Ihrem UEFI-Variablenspeicher in der Instance

> **Warning**
>
> Sie müssen Ihre Boot-Images signieren, nachdem Sie die Schlüssel registriert haben, sonst können Sie Ihre Instance nicht starten.

Nachdem Sie die signierten UEFI-Signaturlisten (`PK`, `KEK` und `db`) erstellt haben, müssen sie bei der UEFI-Firmware registriert sein.

Schreiben in der `PK`-Variablen ist nur möglich, wenn:

- Es ist noch keine PK angemeldet, was angegeben wird, wenn die `SetupMode`Variable `1` ist. Prüfen Sie dies mit dem folgenden Befehl: Die Ausgabe ist entweder `1` oder `0`.

  ```
  efivar -d -n 8be4df61-93ca-11d2-aa0d-00e098032b8c-SetupMode
  ```

- Die neue PK ist durch den privaten Schlüssel der bestehenden PK signiert.

So melden Sie die Schlüssel in Ihrem UEFI-Variablenspeicher an

Die folgenden Befehle müssen in der Instance ausgeführt werden.

Wenn der Setup-Modus aktiviert ist (der Wert ist 1) können die Schlüssel registriert werden, indem die folgenden Befehle in der Instance ausgeführt werden:

```
[ec2-user ~]$ efi-updatevar -f db.auth db
```

```
[ec2-user ~]$ efi-updatevar -f KEK.auth KEK
```

```
[ec2-user ~]$ efi-updatevar -f PK.auth PK
```

So überprüfen Sie, ob UEFI Secure Boot aktiviert ist

Führen Sie die Schritte unter aus, um zu überprüfen, ob UEFI Secure Boot aktiviert ist Überprüfen, ob eine Amazon-EC2-Instance für UEFI Secure Boot aktiviert ist.

Sie können Ihren UEFI-Variablenspeicher jetzt mit dem CLI-Befehl get-instance-uefi-data exportieren oder mit dem nächsten Schritt fortfahren und Ihre Boot-Images signieren, um sie in einer UEFI Secure Boot-fähigen Instance neu zu starten.

Schritt 3: Erstellen eines AMI Ihrer Instance

Um ein AMI von der Instance zu erstellen, können Sie die Konsole oder `CreateImage`-API, CLI oder SDKs verwenden. Informationen zur Verwendung der Konsole finden Sie unter Ein Amazon-EBS-gestütztes AMI erstellen. Die API-Anweisungen finden Sie unter CreateImage.

> **Note**
>
> Die `CreateImage`-API kopiert den UEFI-Variablenspeicher der Instance automatisch in das AMI. Die Konsole verwendet die `CreateImage`-API. Nachdem Sie Instances mit diesem AMI gestartet haben, haben die Instances denselben UEFI-Variablenspeicher.

Aufgabe 2 – Option B: Erstellen Sie ein binäres Blob mit einem vorgefüllten Variablenspeicher

Nachdem Sie die drei Schlüsselpaare erstellt haben, können Sie ein binäres Blob erstellen, das einen vorgefüllten Variablenspeicher enthält, der die UEFI Secure Boot-Schlüssel enthält. Führen Sie alternativ die Schritte unter the section called “Aufgabe 2 – Option A: Fügen Sie innerhalb der Instance Schlüssel zum Variablenspeicher hinzu” aus.

> **Warning**
>
> Sie müssen Ihre Boot-Images signieren, bevor Sie die Schlüssel registrieren, sonst können Sie Ihre Instance nicht starten.

Option B Schritte:

- Schritt 1: Erstellen Sie einen neuen Variablenspeicher oder aktualisieren Sie einen vorhandenen
- Schritt 2: Hochladen des binären Blobs bei der AMI-Erstellung

Schritt 1: Erstellen Sie einen neuen Variablenspeicher oder aktualisieren Sie einen vorhandenen

Sie können den Variablenspeicher offline ohne eine laufende Instance erstellen, indem Sie das Python-Uefivars-Tool verwenden. Das Tool kann aus Ihren Schlüsseln einen neuen

Variablenspeicher erstellen. Das Skript unterstützt derzeit das EDK2-Format, das AWS-Format und eine JSON-Darstellung, die mit übergeordneten Tools einfacher zu bearbeiten ist.

So erstellen Sie den Variablenspeicher offline ohne laufende Instance

1. Laden Sie das Tool unter folgendem Link herunter.

   ```
   https://github.com/awslabs/python-uefivars
   ```

2. Erstellen Sie einen neuen Variablenspeicher von Ihren Schlüsseln, indem Sie den folgenden Befehl ausführen. Dies wird ein base64-kodiertes binäres Blob in *ihr_binäres_blob*.bin erstellen. Das Tool unterstützt auch das Aktualisieren eines binären Blobs über die `-I`-Parameter.

   ```
   ./uefivars.py -i none -o aws -O your_binary_blob.bin -P PK.esl -K KEK.esl --db
    db.esl --dbx dbx.esl
   ```

Schritt 2: Hochladen des binären Blobs bei der AMI-Erstellung

Verwenden Sie register-image um Ihre UEFI-Variablenspeicherdaten zu übergeben. Geben Sie für den Parameter `--uefi-data` geben Sie Ihr binäres Blob an, und geben Sie für den Parameter `--boot-mode uefi` an.

```
aws ec2 register-image \
    --name uefi_sb_tpm_register_image_test \
    --uefi-data $(cat your_binary_blob.bin) \
    --block-device-mappings "DeviceName=/dev/sda1,Ebs=
 {SnapshotId=snap-0123456789example,DeleteOnTermination=true}" \
    --architecture x86_64 \
    --root-device-name /dev/sda1 \
    --virtualization-type hvm \
    --ena-support \
    --boot-mode uefi
```

AWS-Binärblob für UEFI Secure Boot erstellen

Sie können die folgenden Schritte ausführen, um die UEFI Secure Boot-Variablen während der AMI-Erstellung anzupassen. Der KEK, der in diesen Schritten verwendet wird, ist auf dem Stand von September 2021. Wenn Microsoft den KEK aktualisiert, müssen Sie den neuesten KEK verwenden.

So erstellen Sie das binäre Blob von AWS

1. Erstellen Sie eine leere PK-Signaturliste.

```
touch empty_key.crt
cert-to-efi-sig-list empty_key.crt PK.esl
```

2. Laden Sie die KEK-Zertifikate herunter.

```
https://go.microsoft.com/fwlink/?LinkId=321185
```

3. Verpacken Sie die KEK-Zertifikate in einer UEFI-Signaturliste (`siglist`).

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_KEK.esl MicCorKEKCA2011_2011-06-24.crt
```

4. Laden Sie Microsofts DB-Zertifikate herunter.

```
https://www.microsoft.com/pkiops/certs/MicWinProPCA2011_2011-10-19.crt
https://www.microsoft.com/pkiops/certs/MicCorUEFCA2011_2011-06-27.crt
```

5. Generieren Sie die DB-Signaturliste.

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_db.esl MicWinProPCA2011_2011-10-19.crt
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_UEFI_db.esl MicCorUEFCA2011_2011-06-27.crt
cat MS_Win_db.esl MS_UEFI_db.esl > MS_db.esl
```

6. Das Unified Extensible Firmware Interface Forum stellt die DBX-Dateien nicht mehr zur Verfügung. Sie werden jetzt von Microsoft auf GitHub bereitgestellt. Laden Sie das neueste DBX-Update aus dem Microsoft Secure Boot Updates Repository unter https://github.com/microsoft/secureboot_objects herunter.
7. Entpacken Sie die signierte Update-Binärdatei.

   Erstellen Sie `SplitDbxContent.ps1` mit dem folgenden Skriptinhalt. Alternativ können Sie das Skript aus der PowerShell Gallery mit `Install-Script -Name SplitDbxContent` installieren.

```
<#PSScriptInfo
```

```
.VERSION 1.0

.GUID ec45a3fc-5e87-4d90-b55e-bdea083f732d

.AUTHOR Microsoft Secure Boot Team

.COMPANYNAME Microsoft

.COPYRIGHT Microsoft

.TAGS Windows Security

.LICENSEURI

.PROJECTURI

.ICONURI

.EXTERNALMODULEDEPENDENCIES

.REQUIREDSCRIPTS

.EXTERNALSCRIPTDEPENDENCIES

.RELEASENOTES
Version 1.0: Original published version.

#>

<#
.DESCRIPTION
 Splits a DBX update package into the new DBX variable contents and the signature
 authorizing the change.
 To apply an update using the output files of this script, try:
 Set-SecureBootUefi -Name dbx -ContentFilePath .\content.bin -SignedFilePath .
\signature.p7 -Time 2010-03-06T19:17:21Z -AppendWrite'
.EXAMPLE
.\SplitDbxAuthInfo.ps1 DbxUpdate_x64.bin
#>


# Get file from script input
$file  = Get-Content -Encoding Byte $args[0]
```

```
# Identify file signature
$chop = $file[40..($file.Length - 1)]
if (($chop[0] -ne 0x30) -or ($chop[1] -ne 0x82 )) {
    Write-Error "Cannot find signature"
    exit 1
}

# Signature is known to be ASN size plus header of 4 bytes
$sig_length = ($chop[2] * 256) + $chop[3] + 4
$sig = $chop[0..($sig_length - 1)]

if ($sig_length -gt ($file.Length + 40)) {
    Write-Error "Signature longer than file size!"
    exit 1
}

# Content is everything else
$content = $file[0..39] + $chop[$sig_length..($chop.Length - 1)]

# Write signature and content to files
Set-Content -Encoding Byte signature.p7 $sig
Set-Content -Encoding Byte content.bin $content
```

Verwenden Sie das Skript, um die signierten DBX-Dateien zu entpacken.

```
PS C:\Windows\system32> SplitDbxContent.ps1 .\dbx.bin
```

Dadurch werden zwei Dateien erzeugt – `signature.p7` und `content.bin`. Verwenden Sie `content.bin` im nächsten Schritt.

8. Erstellen Sie einen UEFI-Variablenspeicher mit dem `uefivars.py`-Skript.

```
./uefivars.py -i none -o aws -O uefiblob-microsoft-keys-empty-pk.bin -P ~/PK.esl -K
 ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx ~/content.bin
```

9. Prüfen Sie das binäre Blob und den UEFI-Variablenspeicher.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o json | less
```

10. Sie können das Blob aktualisieren, indem Sie es erneut an dasselbe Tool übergeben.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o aws -O uefiblob-
microsoft-keys-empty-pk.bin -P ~/PK.esl -K ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx
 ~/content.bin
```

Erwartete Ausgabe

```
Replacing PK
Replacing KEK
Replacing db
Replacing dbx
```

Verwenden der Verschlüsselung mit EBS-gestützten AMIs

AMIs, die durch Amazon EBS-Snapshots gestützt werden, können die Amazon EBS-Verschlüsselung nutzen. Snapshots von Daten- und Stamm-Volumes können verschlüsselt und einem AMI zugeordnet werden. Sie können Instances starten und Images mit vollständiger EBS-Verschlüsselungsunterstützung kopieren. Verschlüsselungsparameter für diese Operationen werden in allen Regionen unterstützt, in denen AWS KMS verfügbar ist.

EC2-Instances mit verschlüsselten EBS-Volumes werden über AMIs genau wie andere Instances gestartet. Zudem können Sie einige oder alle Volumes während des Starts verschlüsseln, wenn Sie eine Instance von einem AMI starten, das von unverschlüsselten EBS-Snapshots unterstützt wird.

Wie bei EBS-Volumes können Snapshots in AMIs entweder durch Ihren Standard-AWS KMS key oder mit einem von Ihnen angegebenen vom Kunden verwalteten Schlüssel verschlüsselt werden. In allen Fällen müssen Sie die Berechtigung haben, den ausgewählten Verschlüsselung zu verwenden.

AMIs mit verschlüsselten Snapshots können für mehrere AWS-Konten gemeinsam genutzt werden. Weitere Informationen finden Sie unter Verstehen Sie die gemeinsame AMI-Nutzung in Amazon EC2.

Themen zur Verschlüsselung mit EBS-gestützten AMIs

- Instance-startende Szenarien
- Image-kopierende Szenarien

Instance-startende Szenarien

Amazon-EC2-Instances werden mithilfe der `RunInstances`-Aktion mit über Blockgerät-Zuweisung bereitgestellten Parametern aus AMIs gestartet, entweder über die AWS-Managementkonsole oder direkt über die Amazon EC2 API oder CLI. Weitere Informationen finden Sie unter Blockgerät-Zuweisungen auf Amazon-EC2-Instances blockieren. Beispiele für die Steuerung der Blockgerät-Zuweisung über die AWS CLI finden Sie unter Launch, List, and Terminate EC2 Instances.

Ohne explizite Verschlüsselungsparameter behält eine `RunInstances`-Aktion standardmäßig den bestehenden Verschlüsselungsstatus der Quell-Snapshots eines AMI bei, während EBS-Volumes von diesen wiederhergestellt werden. Wenn standardmäßige Verschlüsselung aktiviert ist, werden alle Volumes, die aus dem AMI erstellt werden (ob aus verschlüsselten oder unverschlüsselten Snapshots), verschlüsselt. Wenn die Verschlüsselung standardmäßig nicht aktiviert ist, behält die Instance den Verschlüsselungsstatus der AMI bei.

Sie können auch eine Instance starten und gleichzeitig einen neuen Verschlüsselungsstatus auf die sich ergebenden Volumes anwenden, indem Sie Verschlüsselungsparameter angeben. Folglich werden die folgenden Verhaltensweisen beobachtet:

Starten ohne Verschlüsselungsparameter

- Ein unverschlüsselter Snapshot wird in ein unverschlüsseltes Volume wiederhergestellt, es sei denn, die standardmäßige Verschlüsselung ist aktiviert. In diesem Fall werden alle neu erstellten Volumes verschlüsselt.
- Ein verschlüsselter Snapshot, den Sie besitzen, wird in ein Volume wiederhergestellt, das mit demselben Verschlüsselung verschlüsselt wird.
- Ein verschlüsselter Snapshot, den Sie nicht besitzen (z. B., wenn das AMI für Sie freigegeben wurde), wird in einem Volume wiederhergestellt, das mit dem Standard-KMS-Schlüssel Ihres AWS-Kontos verschlüsselt wird.

Durch Angeben von Verschlüsselungsparametern können die Standard-Verhaltensweisen überschrieben werden. Die verfügbaren Parameter sind `Encrypted` und `KmsKeyId`. Werden nur die `Encrypted`-Parameter festgelegt, ergibt sich Folgendes:

Instance-Start-Verhaltensweisen, wenn **`Encrypted`** festgelegt, aber keine **`KmsKeyId`** angegeben ist

- Ein unverschlüsselter Snapshot wird in einem EBS-Volume wiederhergestellt, das mit dem Standard-KMS-Schlüssel Ihres AWS-Kontos verschlüsselt wird.

- Ein verschlüsselter Snapshot, den Sie besitzen, wird in ein EBS-Volume wiederhergestellt, das mit demselben Verschlüsselung verschlüsselt wird. (Mit anderen Worten, der `Encrypted`-Parameter ist wirkungslos.)
- Ein verschlüsselter Snapshot, den Sie nicht besitzen (z. B., wenn das AMI für Sie freigegeben wurde), wird in einem Volume wiederhergestellt, das mit dem Standard-KMS-Schlüssel Ihres AWS-Kontos verschlüsselt wird. (Mit anderen Worten, der `Encrypted`-Parameter ist wirkungslos.)

Durch Festlegen der Parameter `Encrypted` und `KmsKeyId` können Sie einen nicht standardmäßigen Verschlüsselung für eine Verschlüsselungsoperation angeben. Dadurch ergeben sich die folgenden Verhaltensweisen:

Instance, bei der **`Encrypted`** und **`KmsKeyId`** festgelegt sind

- Ein unverschlüsselter Snapshot wird in ein EBS-Volume wiederhergestellt, das mit dem angegebenen Verschlüsselung verschlüsselt wird.
- Ein verschlüsselter Snapshot wird in ein EBS-Volume wiederhergestellt, das nicht mit dem ursprünglichen Verschlüsselung, sondern mit dem angegebenen Verschlüsselung verschlüsselt wird.

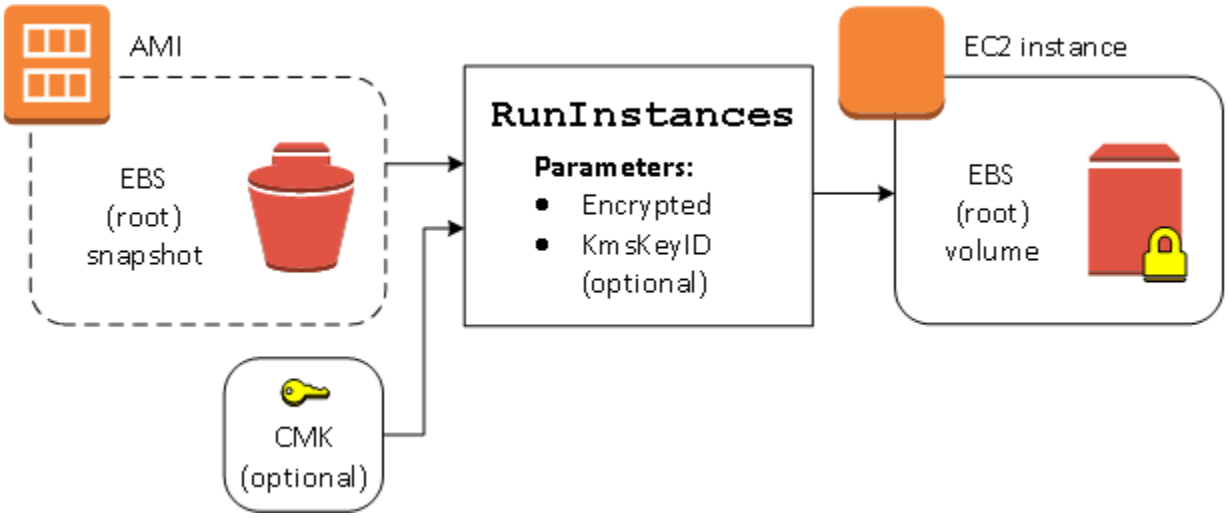
Das Senden einer `KmsKeyId` ohne Festlegen des `Encrypted`-Parameters führt zu einem Fehler.

Die folgenden Abschnitte enthalten Beispiele für das Starten von Instances aus AMIs mithilfe von nicht standardmäßigen Verschlüsselungsparametern. In jedem dieser Szenarien ergibt sich durch die in der `RunInstances`-Aktionen bereitgestellten Parameter eine Änderung des Verschlüsselungsstatus während der Wiederherstellung eines Volumes aus einem Snapshot.

Informationen zur Verwendung der Konsole zum Starten einer Instance von einem AMI aus finden Sie unter Starten Sie eine EC2 Amazon-Instance.

Verschlüsseln eines Volumes während des Startens

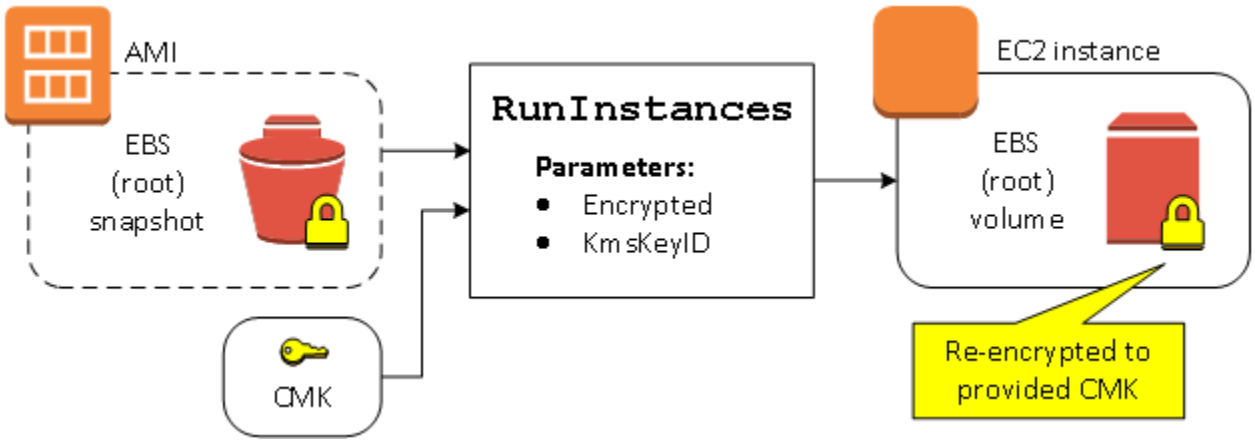
In diesem Beispiel wird ein von einem unverschlüsselten Snapshot unterstütztes AMI verwendet, um eine EC2-Instance mit einem verschlüsselten EBS-Volume zu starten.



Der Parameter `Encrypted` für sich allein bewirkt, dass das Volume für diese Instance verschlüsselt wird. Die Angabe eines Parameters `KmsKeyId` ist optional. Wenn keine KMS-Schlüssel-ID angegeben ist, wird der Standard-KMS-Schlüssel des AWS-Kontos zum Verschlüsseln des Volumes verwendet. Geben Sie den Parameter `KmsKeyId` an, um das Volume mit einem anderen eigenen Verschlüsselung zu verschlüsseln.

Neuverschlüsseln eines Volumes während des Startens

In diesem Beispiel wird ein von einem verschlüsselten Snapshot unterstütztes AMI verwendet, um eine EC2-Instance mit einem EBS-Volume zu starten, das mit einem neuen Verschlüsselung verschlüsselt wird.

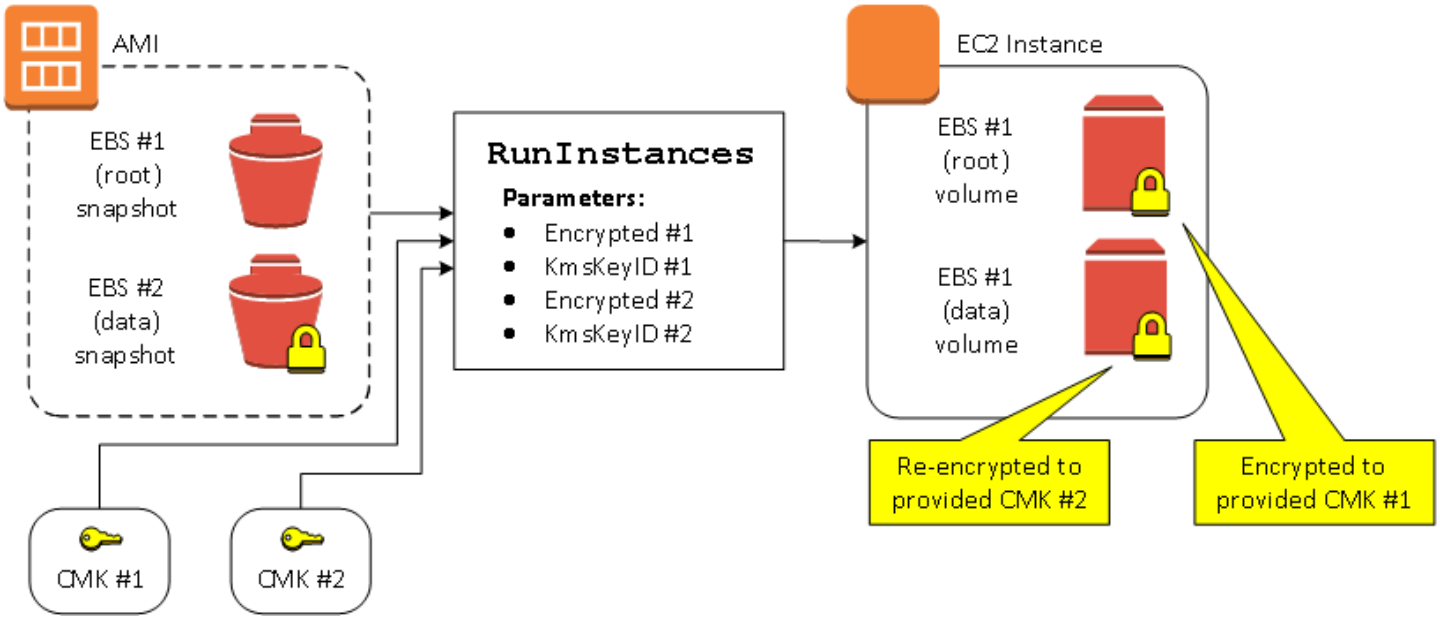


Wenn Sie das AMI besitzen und keine Verschlüsselungsparameter angeben, verfügt die resultierende Instance über ein Volume, das mit demselben KMS-Schlüssel wie der Snapshot verschlüsselt wird. Wenn das AMI gemeinsam genutzt wird und nicht Ihnen gehört – und Sie keine Verschlüsselungsparameter angeben – wird das Volume mit Ihrem Standard-Verschlüsselung

verschlüsselt. Werden die Verschlüsselungsparameter wie gezeigt angegeben, wird das Volume mit dem angegebenen Verschlüsselung verschlüsselt.

Ändern des Verschlüsselungsstatus mehrerer Volumes während des Startens

In diesem komplexeren Beispiel wird ein von mehreren Snapshots unterstütztes AMI (jedes mit einem eigenen Verschlüsselungsstatus) verwendet, um eine EC2-Instance mit einem neu verschlüsselten und einem erneut verschlüsselten Volume zu starten.



In diesem Szenario wird die `RunInstances`-Aktion mit Verschlüsselungsparametern für jeden der Quell-Snapshots bereitgestellt. Wenn alle möglichen Verschlüsselungsparameter angegeben sind, ist die sich ergebende Instance unabhängig davon, ob Sie die AMI besitzen, identisch.

Image-kopierende Szenarien

Amazon-EC2-AMIs werden mit der `CopyImage`-Aktion kopiert, entweder über die AWS-Managementkonsole oder direkt mit der Amazon EC2 API oder CLI.

Ohne explizite Verschlüsselungsparameter behält eine `CopyImage`-Aktion standardmäßig den bestehenden Verschlüsselungsstatus der Quell-Snapshots eines AMI während des Kopierens bei. Sie können auch ein AMI kopieren und gleichzeitig einen neuen Verschlüsselungsstatus auf seine zugeordneten EBS-Snapshots anwenden, indem Sie Verschlüsselungsparameter angeben. Folglich werden die folgenden Verhaltensweisen beobachtet:

Kopieren ohne Verschlüsselungsparameter

- Ein unverschlüsselter Snapshot wird in einen anderen unverschlüsselten Snapshot kopiert, es sei denn, die standardmäßige Verschlüsselung ist aktiviert. In diesem Fall werden alle neu erstellten Snapshots verschlüsselt.
- Ein verschlüsselter Snapshot, den Sie besitzen, wird in einen Snapshot kopiert, der mit demselben Verschlüsselung verschlüsselt wird.
- Ein verschlüsselter Snapshot, den Sie nicht besitzen (d. h., das AMI wurde für Sie freigegeben), wird in einen Snapshot kopiert, der mit dem Standard-KMS-Schlüssel Ihres AWS-Kontos verschlüsselt wird.

All diese Standard-Verhaltensweisen können durch Angeben von Verschlüsselungsparametern überschrieben werden. Die verfügbaren Parameter sind `Encrypted` und `KmsKeyId`. Werden nur die `Encrypted`-Parameter festgelegt, ergibt sich Folgendes:

Copy-image-Verhaltensweisen, wenn **`Encrypted`** festgelegt, aber keine **`KmsKeyId`** angegeben ist

- Ein unverschlüsselter Snapshot wird in einen Snapshot kopiert, der mit dem Standard-KMS-Schlüssel des AWS-Kontos verschlüsselt wird.
- Ein verschlüsselter Snapshot wird in einen Snapshot kopiert, der mit demselben Verschlüsselung verschlüsselt wird. (Mit anderen Worten, der `Encrypted`-Parameter ist wirkungslos.)
- Ein verschlüsselter Snapshot, den Sie nicht besitzen (d. h., das AMI wurde für Sie freigegeben), wird in ein Volume kopiert, das mit dem Standard-KMS-Schlüssel Ihres AWS-Kontos verschlüsselt wird. (Mit anderen Worten, der `Encrypted`-Parameter ist wirkungslos.)

Durch Festlegen der Parameter `Encrypted` und `KmsKeyId` können Sie einen kundenverwalteten Verschlüsselung für eine Verschlüsselungsoperation angeben. Dadurch ergeben sich die folgenden Verhaltensweisen:

Copy-image-Verhaltensweisen, wenn **`Encrypted`** und **`KmsKeyId`** festgelegt sind

- Ein unverschlüsselter Snapshot wird in einen Snapshot kopiert, der mit dem angegebenen Verschlüsselung verschlüsselt wird.
- Ein verschlüsselter Snapshot wird in einen Snapshot kopiert, der nicht mit dem ursprünglichen Verschlüsselung, sondern mit dem angegebenen Verschlüsselung verschlüsselt wird.

Das Senden einer `KmsKeyId` ohne Festlegen des `Encrypted`-Parameters führt zu einem Fehler.

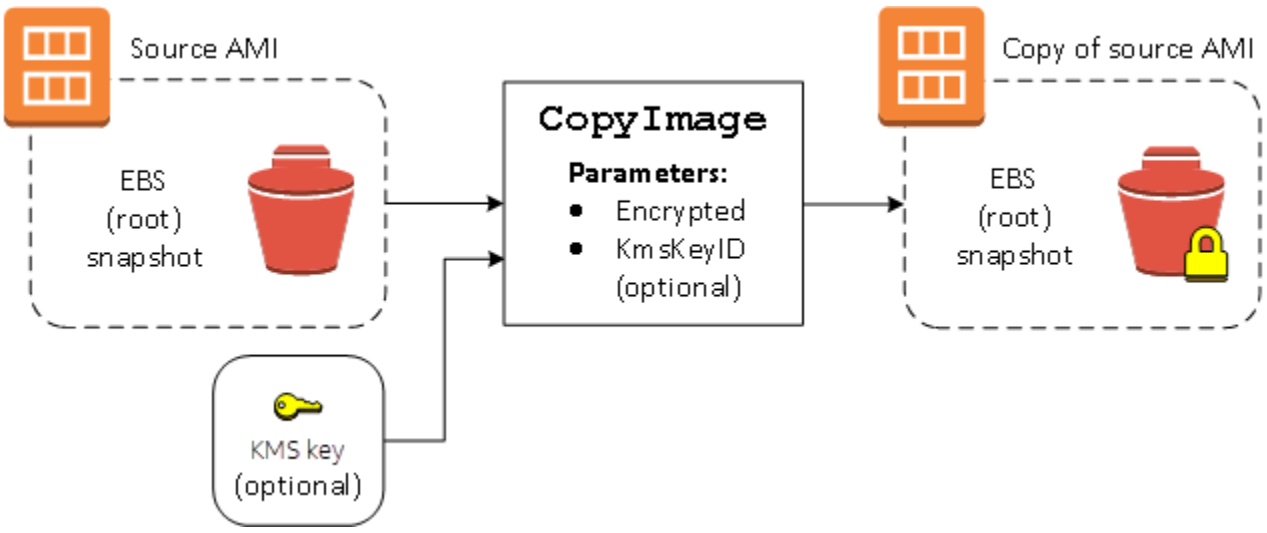
Der folgende Abschnitt enthält ein Beispiel für das Kopieren eines AMI mit nicht standardmäßigen Verschlüsselungsparametern, wodurch sich der Verschlüsselungsstatus ändert.

Detaillierte Anweisungen zur Verwendung der Konsole finden Sie unter Ein EC2 Amazon-AMI kopieren.

Verschlüsseln eines unverschlüsselten Images während des Kopierens

In diesem Szenario wird ein von einem unverschlüsselten Stamm-Snapshot unterstütztes AMI in ein AMI mit einem verschlüsselten Stamm-Snapshot kopiert. Die Aktion `CopyImage` wird mit zwei Verschlüsselungsparametern aufgerufen, einschließlich eines vom Kunden verwalteten Schlüssels. Dadurch ändert sich der Verschlüsselungsstatus des Stamm-Snapshots, sodass das Ziel-AMI durch einen Stamm-Snapshot gestützt wird, der dieselben Daten wie der Quell-Snapshot enthält, aber mit dem angegebenen Schlüssel verschlüsselt wird. Für Sie fallen Speicherkosten für die Snapshots in beiden AMIs sowie Gebühren für Instances an, die Sie von einem der AMIs starten.

> **Note**
>
> Das Aktivieren von standardmäßige Verschlüsselung hat die gleiche Wirkung wie das Festlegen des `Encrypted`-Parameters auf `true` für alle Snapshots im AMI.



Wenn der `Encrypted`-Parameter festgelegt wird, wird der einzige Snapshot für diese Instance verschlüsselt. Wenn Sie den `KmsKeyId`-Parameter nicht angeben, wird der standardmäßige vom Kunden verwaltete Schlüssel zum Verschlüsseln der Snapshot-Kopie verwendet.

> **Note**
>
> Sie können auch ein Image mit mehreren Snapshots kopieren und den Verschlüsselungsstatus individuell konfigurieren.

Verstehen Sie die gemeinsame AMI-Nutzung in Amazon EC2

Ein gemeinsames AMI ist ein AMI, das ein Entwickler nach der Erstellung für Andere verfügbar macht. Eine der einfachsten Möglichkeiten, mit Amazon zu beginnen, EC2 besteht darin, ein gemeinsam genutztes AMI zu verwenden, das die benötigten Komponenten enthält, und dann benutzerdefinierte Inhalte hinzuzufügen. Sie können auch eigene erstellen AMIs und diese mit anderen teilen.

Die Verwendung gemeinsamer AMIs erfolgt auf eigenes Risiko. Amazon kann nicht für die Integrität oder Sicherheit von AMIs geteilten Inhalten durch andere EC2 Amazon-Nutzer bürgen. Daher sollten Sie gemeinsam genutzten Code genauso behandeln AMIs wie jeden fremden Code, den Sie möglicherweise in Ihrem eigenen Rechenzentrum einsetzen möchten, und die entsprechende Sorgfaltspflicht walten lassen. Wir empfehlen Ihnen, eine AMI von einer vertrauenswürdigen Quelle zu beziehen, beispielsweise von einem verifizierten Anbieter.

Verifizierter Anbieter

In der EC2 Amazon-Konsole werden öffentliche AMIs Inhalte, die Amazon oder einem verifizierten Amazon-Partner gehören, als Verifizierter Anbieter gekennzeichnet.

Sie können auch den AWS CLI Befehl describe-images verwenden, um öffentliche Inhalte zu identifizieren AMIs , die von einem verifizierten Anbieter stammen. Öffentliche Images, die im Besitz von Amazon oder einem verifizierten Partner sind, haben einen Aliasbesitzer, der entweder `amazon`, `aws-backup-vault` oder `aws-marketplace` ist. In der CLI-Ausgabe erscheinen diese Werte für `ImageOwnerAlias`. Andere Benutzer können ihre nicht mit einem Alias versehen. AMIs Auf diese Weise können Sie ganz einfach AMIs bei Amazon oder verifizierten Partnern suchen.

Um ein verifizierter Anbieter zu werden, müssen Sie sich als Verkäufer auf der AWS Marketplace registrieren. Nach der Registrierung können Sie Ihr AMI auf der AWS Marketplace auflisten. Weitere Informationen finden Sie unter Erste Schritte als Verkäufer und AMI-basierte Produkte im AWS Marketplace -Verkäuferhandbuch.

Themen über gemeinsame AMIs

- Suchen Sie AMIs nach geteilten Dateien zur Verwendung für EC2 Amazon-Instances
- Bereiten Sie sich auf die Verwendung von Shared für Linux AMIs vor
- Steuern Sie die Entdeckung und Verwendung von AMIs in Amazon EC2 mit Allowed AMIs
- Machen Sie Ihr AMI für die Verwendung in Amazon öffentlich verfügbar EC2
- Verstehen Sie, öffentlichen Zugriff sperren für AMIs
- Ein AMI für bestimmte Organisationen oder Organisationseinheiten freigeben
- Freigeben eines AMI für bestimmte AWS -Konten
- Kündigen Sie die gemeinsame Nutzung eines AMI mit Ihrem AWS-Konto
- Empfehlungen für die Erstellung von gemeinsam genutztem Linux AMIs

Wenn Sie nach Informationen zu anderen Themen suchen

- Weitere Informationen über die Erstellung eines AMI finden Sie unter the section called “Ein Amazon-S3-gestütztes AMI erstellen” oder the section called “Erstellen eines AMI”.
- Informationen zum Erstellen, Bereitstellen und Verwalten Ihrer Anwendungen auf der AWS Marketplace finden Sie in der AWS Marketplace -Dokumentation.

Suchen Sie AMIs nach geteilten Dateien zur Verwendung für EC2 Amazon-Instances

Sie können die EC2 Amazon-Konsole oder die Befehlszeile verwenden, um öffentliche oder private geteilte Dateien zu findenAMIs , die Sie mit Ihren EC2 Amazon-Instances verwenden können.

AMIs sind eine regionale Ressource. Wenn Sie also nach einem gemeinsamen AMI (öffentlich oder privat) suchen, müssen Sie in derselben Region danach suchen, aus der es freigegeben wird. Um ein AMI in einer anderen Region verfügbar zu machen, kopieren Sie das AMI in die Region und geben Sie es dann frei. Weitere Informationen finden Sie unter Ein EC2 Amazon-AMI kopieren.

Console

Die Konsole bietet ein AMI-Filterfeld. Sie können Ihre Suchanfragen auch mithilfe der Filter im Suchfeld eingrenzen.

So suchen Sie ein freigegebenes AMI

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich AMIs aus.
3. Wählen Sie beim ersten Filter eine der folgenden Optionen aus:
   - Private Bilder — Listet alle Bilder auf AMIs , die mit Ihnen geteilt wurden.
   - Öffentliche Bilder — Listet alle öffentlichen Bilder auf AMIs.
4. (Optional) Um nur die öffentlichen Images von Amazon anzuzeigen, wählen Sie das Feld Suche und wählen Sie dann aus den Menüoptionen Besitzer-Alias, dann = und dann amazon.
5. (Optional) Fügen Sie Filter hinzu, um Ihre Suche AMIs so einzugrenzen, dass sie Ihren Anforderungen entsprechen.

So suchen Sie ein gemeinsames öffentliches AMI von einem verifizierten Anbieter

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMI-Katalog aus.
3. Wählen Sie Community AMIs.
4. Wählen Sie im Bereich Ergebnisse verfeinern die Option Verifizierter Anbieter aus. Das Label Verifizierter Anbieter gibt an, dass AMIs sie von Amazon oder einem verifizierten Partner stammen.

AWS CLI

Verwenden Sie zum Auflisten den Befehl describe-images. AMIs Sie können die Liste auf die Typen beschränken AMIs , die Sie interessieren, wie in den folgenden Beispielen gezeigt.

Um alle öffentlichen Inhalte aufzulisten AMIs

Der folgende Befehl listet alle öffentlichen Dateien auf AMIs, einschließlich aller öffentlichen Dateien AMIs , deren Eigentümer Sie sind.

```
aws ec2 describe-images --executable-users all
```

Zur Liste AMIs mit expliziten Startberechtigungen

Der folgende Befehl listet die auf, AMIs für die Sie explizite Startberechtigungen haben. Diese Liste enthält keine AMIs , die Sie besitzen.

```
aws ec2 describe-images --executable-users self
```

Zur Liste, die verifizierten Anbietern AMIs gehört

Der folgende Befehl listet die Anbieter auf, die AMIs sich im Besitz verifizierter Anbieter befinden. Öffentliche AMIs Eigentümer verifizierter Anbieter (entweder Amazon oder verifizierte Partner) haben einen Aliasinhaber, der `aws-marketplace` im Kontofeld als `amazonaws-backup-vault`, oder angezeigt wird. Auf diese Weise können Sie problemlos AMIs verifizierte Anbieter finden. Andere Benutzer können ihre nicht mit einem Alias versehenAMIs.

```
aws ec2 describe-images \
    --owners amazon aws-marketplace \
    --query 'Images[*].[ImageId]' \
    --output text
```

Zur Liste, die einem Konto AMIs gehört

Der folgende Befehl listet die Objekte auf, die dem angegebenen Benutzer AMIs gehören AWS-Konto.

```
aws ec2 describe-images --owners 123456789012
```

Um einen Bereich AMIs mithilfe eines Filters zu verwenden

Um die Anzahl der angezeigten Typen zu reduzieren AMIs, verwenden Sie einen Filter, um nur die Typen aufzulistenAMIs , die Sie interessieren. Verwenden Sie beispielsweise den folgenden Filter, um nur AMIs EBS-gestützte Daten anzuzeigen.

```
--filters "Name=root-device-type,Values=ebs"
```

PowerShell

Verwenden Sie das Get-EC2ImageCmdlet (Tools für Windows PowerShell) zum Auflisten. AMIs Sie können die Liste auf die Typen beschränken AMIs , die Sie interessieren, wie in den folgenden Beispielen gezeigt.

Um alle öffentlichen Inhalte aufzulisten AMIs

Der folgende Befehl listet alle öffentlichen Dateien auf AMIs, einschließlich aller öffentlichen Dateien AMIs , deren Eigentümer Sie sind.

```
Get-EC2Image -ExecutableUser all
```

Zur Liste AMIs mit expliziten Startberechtigungen

Der folgende Befehl listet die auf, AMIs für die Sie explizite Startberechtigungen haben. Diese Liste enthält keine AMIs , die Sie besitzen.

```
Get-EC2Image -ExecutableUser self
```

Zur Liste, die verifizierten Anbietern AMIs gehört

Der folgende Befehl listet die Anbieter auf, die AMIs sich im Besitz verifizierter Anbieter befinden. Öffentliche AMIs Eigentümer verifizierter Anbieter (entweder Amazon oder verifizierte Partner) haben einen Aliasinhaber, der `aws-marketplace` im Kontofeld als `amazonaws-backup-vault`, oder angezeigt wird. Auf diese Weise können Sie problemlos AMIs verifizierte Anbieter finden. Andere Benutzer können ihre nicht mit einem Alias versehenAMIs.

```
Get-EC2Image -Owner amazon aws-marketplace
```

Zur Liste, die einem Konto AMIs gehört

Der folgende Befehl listet die Objekte auf, die dem angegebenen Benutzer AMIs gehören AWS-Konto.

```
Get-EC2Image -Owner 123456789012
```

Um einen Bereich AMIs mithilfe eines Filters zu verwenden

Um die Anzahl der angezeigten Typen zu reduzieren AMIs, verwenden Sie einen Filter, um nur die Typen aufzulistenAMIs , die Sie interessieren. Verwenden Sie beispielsweise den folgenden Filter, um nur AMIs EBS-gestützte Daten anzuzeigen.

```
-Filter @{Name="root-device-type"; Values="ebs"}
```

Bereiten Sie sich auf die Verwendung von Shared für Linux AMIs vor

Bevor Sie ein freigegebenes AMI für Linux verwenden, führen Sie die folgenden Schritte durch, um sicherzustellen, dass keine vorinstallierten Anmeldeinformationen vorhanden sind, die einem Dritten unerwünschten Zugriff auf Ihre Instance ermöglichen würden, und dass keine vorkonfigurierte

Fernprotokollierung vorhanden ist, die sensible Daten an Dritte übertragen könnte. Informationen zur Erhöhung der Systemsicherheit finden Sie in der Dokumentation für die von der AMI verwendete Linux-Distribution.

Damit Sie den Zugriff auf die Instance nicht unabsichtlich verlieren, empfehlen wir das Initiieren von zwei SSH-Sitzungen, wobei eine Sitzung offen bleibt, bis Sie alle unbekannten Anmeldeinformationen entfernt und bestätigt haben, dass Sie sich noch immer mit SSH in Ihrer Instance anmelden können.

1. Ermitteln Sie nicht autorisierte öffentliche SSH-Schlüssel und deaktivieren Sie sie. Der einzige Schlüssel in der Datei sollte der zum Starten des AMI verwendete sein. Mit dem folgenden Befehl suchen Sie `authorized_keys`-Dateien:

   ```
   [ec2-user ~]$ sudo find / -name "authorized_keys" -print -exec cat {} \;
   ```

2. Deaktivieren Sie Passwort-basierte Authentifizierung für den Root-Benutzer. Öffnen Sie die Datei `sshd_config` und bearbeiten Sie die `PermitRootLogin`-Zeile wie folgt:

   ```
   PermitRootLogin without-password
   ```

   Alternativ können Sie die Funktion zum Anmelden in der Instance als Root-Benutzer deaktivieren:

   ```
   PermitRootLogin No
   ```

   Starten Sie den sshd-Service neu.

3. Überprüfen Sie, ob es andere Benutzer gibt, die sich bei Ihrer Instance anmelden können. Benutzer mit Super-User-Privilegien sind besonders gefährlich. Entfernen oder sperren Sie die Passwörter unbekannter Konten.
4. Prüfen Sie, ob nicht verwendete offene Ports bestehen, die Netzwerkdienste ausführen und auf eingehende Verbindungen warten.
5. Um die vorkonfigurierte Fernprotokollierung zu verhindern, sollten Sie die vorhandene Konfigurationsdatei löschen und den `rsyslog`-Service neu starten. Zum Beispiel:

   ```
   [ec2-user ~]$ sudo rm /etc/rsyslog.conf
   [ec2-user ~]$ sudo service rsyslog restart
   ```

6. Überprüfen Sie, ob alle cron-Aufträge rechtmäßig sind.

Wenn Sie ein öffentliches AMI entdecken, das ein Sicherheitsrisiko darstellt, wenden Sie sich an das AWS -Sicherheitsteam. Weitere Informationen erhalten Sie im AWS -Sicherheitszentrum.

Steuern Sie die Entdeckung und Verwendung von AMIs in Amazon EC2 mit Allowed AMIs

Um die Erkennung und Verwendung von Amazon Machine Images (AMIs) durch Benutzer in Ihrem zu kontrollieren AWS-Konto, können Sie die AMIs Funktion Zugelassen verwenden. Sie geben Kriterien an, die erfüllt sein AMIs müssen, damit sie in Ihrem Konto sichtbar und verfügbar sind. Wenn die Kriterien aktiviert sind, können Benutzer, die Instances starten, nur Instances sehen und AMIs darauf zugreifen, die den angegebenen Kriterien entsprechen. Sie können beispielsweise eine Liste vertrauenswürdiger AMI-Anbieter als Kriterien angeben, und nur AMIs von diesen Anbietern ist diese Liste sichtbar und kann verwendet werden.

Bevor Sie die AMIs Einstellungen für Zulässig aktivieren, können Sie den Überwachungsmodus aktivieren, um eine Vorschau anzuzeigen, welche angezeigt AMIs werden oder nicht. Auf diese Weise können Sie die Kriterien nach Bedarf verfeinern, um sicherzustellen, dass nur die beabsichtigten Kriterien sichtbar und für Benutzer in Ihrem Konto verfügbar AMIs sind. Verwenden Sie den describe-instance-image-metadataBefehl außerdem, um Instances zu finden, die mit AMIs denen gestartet wurden und die die angegebenen Kriterien nicht erfüllen. Diese Informationen können Ihnen bei der Entscheidung helfen, entweder Ihre Startkonfigurationen so zu aktualisieren, dass sie konform sind AMIs (z. B. indem Sie ein anderes AMI in einer Startvorlage angeben) oder Ihre Kriterien so anzupassen, dass sie dies zulassen AMIs.

Sie geben die AMIs Einstellungen „Zulässig“ auf Kontoebene an, entweder direkt im Konto oder mithilfe einer deklarativen Richtlinie. Diese Einstellungen müssen in jeder AWS-Region konfiguriert werden, in denen Sie die Verwendung von AMIs steuern möchten. Mithilfe einer deklarativen Richtlinie können Sie die Einstellung auf mehrere Regionen gleichzeitig sowie auf mehrere Konten gleichzeitig anwenden. Wenn eine deklarative Richtlinie verwendet wird, können Sie die Einstellung nicht direkt in einem Konto ändern. In diesem Thema wird beschrieben, wie Sie die Einstellung direkt in einem Konto konfigurieren. Informationen zur Verwendung deklarativer Richtlinien finden Sie unter Deklarative Richtlinien im AWS Organizations -Benutzerhandbuch.

> **Note**
>
> Die AMIs Funktion „Zulässig“ steuert nur die Erkennung und Nutzung von öffentlichen AMIs oder mit Ihrem Konto AMIs geteilten Dateien. Sie schränkt nicht die Inhalte ein, die Ihrem

Konto AMIs gehören. Unabhängig von den von Ihnen festgelegten Kriterien sind die von Ihrem Konto AMIs erstellten Daten immer für Benutzer in Ihrem Konto auffindbar und nutzbar.

Die wichtigsten Vorteile von Allowed AMIs

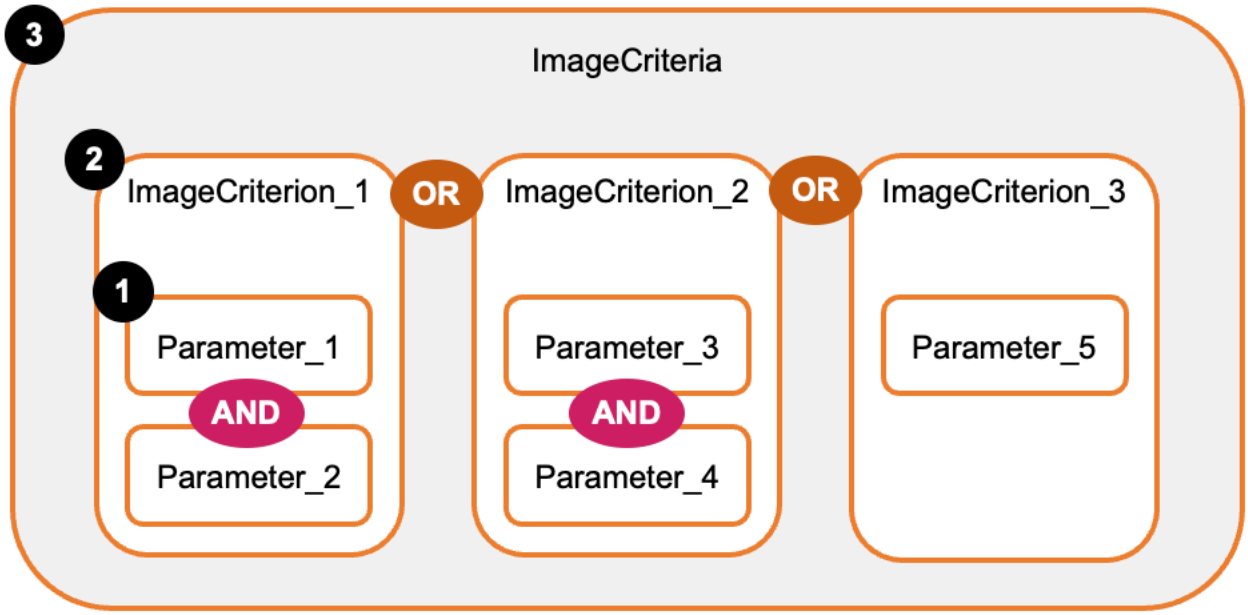
- Compliance und Sicherheit: Benutzer können nur diejenigen entdecken und verwenden AMIs , die die angegebenen Kriterien erfüllen, wodurch das Risiko einer nicht konformen AMI-Nutzung reduziert wird.
- Effizientes Management: Durch die Reduzierung der zulässigen AMIs Anzahl wird die Verwaltung der verbleibenden Dateien einfacher und effizienter.
- Zentralisierte Implementierung auf Kontoebene: Konfigurieren Sie die AMIs Einstellungen „Zulässig“ auf Kontoebene, entweder direkt im Konto oder über eine deklarative Richtlinie. Dies bietet eine zentrale und effiziente Möglichkeit, die AMI-Nutzung für das gesamte Konto zu kontrollieren.

Inhalt

- So funktioniert „Zulässig“ AMIs
- Bewährte Methoden für die Implementierung von Allowed AMIs
- Erforderliche IAM-Berechtigungen
- Verwalten Sie die Einstellungen für „Zugelassen“ AMIs

So funktioniert „Zulässig“ AMIs

Um zu kontrollieren, welche Daten in Ihrem Konto entdeckt und verwendet werden AMIs können, definieren Sie eine Reihe von Kriterien, anhand derer die Daten bewertet werden sollen AMIs. Die Kriterien bestehen aus einem oder mehreren `ImageCriterion`, wie im folgenden Diagramm dargestellt. Eine Erklärung folgt dem Diagramm.



Die Konfiguration besteht aus drei Ebenen:

- 1 – Parameterwerte
  - Parameter mit mehreren Werten
    - `ImageProviders`
    - `ImageNames`
    - `MarketplaceProductCodes`

      Ein AMI kann mit beliebigen Werten innerhalb eines Parameters übereinstimmen, um zulässig zu sein.

      Beispiel: `ImageProviders` = `amazon` ODER Konto `111122223333` ODER Konto `444455556666` (Die Bewertungslogik für Parameterwerte ist im Diagramm nicht dargestellt.)
  - Parameter mit einem Wert:
    - `CreationDateCondition`
    - `DeprecationTimeCondition`
- 2 – `ImageCriterion`
  - Gruppiert mehrere Parameter mit UND-Logik.
  - Ein AMI muss allen Parametern innerhalb eines `ImageCriterion` entsprechen, um zulässig zu sein.

  - Beispiel: `ImageProviders` = `amazon` UND `CreationDateCondition` = 300 Tage oder weniger
- 3 – `ImageCriteria`
  - Gruppiert mehrere `ImageCriterion` mit ODER-Logik.
  - Ein AMI kann einem beliebigen `ImageCriterion` entsprechen, um zulässig zu sein.
  - Bildet die vollständige Konfiguration, anhand derer AMIs bewertet wird.

Themen

- Zulässige AMIs Parameter
- Zulässige AMIs Konfiguration
- So werden Kriterien bewertet
- Einschränkungen
- Zulässige AMIs Operationen

Zulässige AMIs Parameter

Sie können die folgenden Parameter konfigurieren, um `ImageCriterion` zu erstellen:

`ImageProviders`

Die AMI-Anbieter, deren erlaubt AMIs sind.

Gültige Werte sind Aliase, die durch AWS und AWS-Konto IDs wie folgt definiert sind:

- `amazon`— Ein Alias zur Identifizierung, das von Amazon oder verifizierten Anbietern AMIs erstellt wurde
- `aws-marketplace`— Ein Alias, das sich identifiziert, AMIs erstellt von verifizierten Anbietern in AWS Marketplace
- `aws-backup-vault`— Ein Alias, das Backup identifiziert, AMIs die sich in Backup-Tresor-Konten mit logischem Air-Gap befinden. AWS Wenn Sie die AWS Backup-Funktion Logically Air-Gapped Vault verwenden, stellen Sie sicher, dass dieser Alias als AMI-Anbieter enthalten ist.
- AWS-Konto IDs — Eine oder mehrere 12-stellige Ziffern AWS-Konto IDs

- none— Weist darauf hin, dass nur von Ihrem Konto AMIs erstellte Daten entdeckt und verwendet werden können. Öffentlich oder geteilt AMIs können nicht entdeckt und genutzt werden. Wenn angegeben, können keine anderen Kriterien angegeben werden.

`ImageNames`

Die Namen sind zulässig AMIs, wobei exakte Übereinstimmungen oder Platzhalter (`?`oder`*`) verwendet werden.

`MarketplaceProductCodes`

Die AWS Marketplace Produktcodes für erlaubt AMIs.

`CreationDateCondition`

Das Höchstalter für erlaubt AMIs.

`DeprecationTimeCondition`

Der maximale Zeitraum seit dem Verfallsdatum für zulässig. AMIs

Die gültigen Werte und Einschränkungen für jedes Kriterium finden Sie ImageCriterionRequestin der Amazon EC2 API-Referenz.

Zulässige AMIs Konfiguration

Die Kernkonfiguration für „Zulässig“ AMIs ist die `ImageCriteria` Konfiguration, die die Kriterien für „Zulässig“ definiert AMIs. Die folgende JSON-Struktur zeigt die Parameter, die angegeben werden können:

```
{
    "State": "enabled" | "disabled" | "audit-mode",
    "ImageCriteria" : [
        {
            "ImageProviders": ["string",...],
            "MarketplaceProductCodes": ["string",...],
            "ImageNames":["string",...],
            "CreationDateCondition" : {
                "MaximumDaysSinceCreated": integer
            },
            "DeprecationTimeCondition" : {
                "MaximumDaysSinceDeprecated": integer
            }
         },
```

```
        ...
}
```

ImageCriteria Beispiel

Im folgenden `ImageCriteria`-Beispiel werden vier `ImageCriterion` konfiguriert. Ein AMI ist zulässig, wenn es mit einem dieser `ImageCriterion` übereinstimmt. Weitere Informationen über das Auswerten der Kriterien finden Sie unter So werden Kriterien bewertet.

```
{
    "ImageCriteria": [
        // ImageCriterion 1: Allow AWS Marketplace AMIs with product code
 "abcdefg1234567890"
        {
            "MarketplaceProductCodes": [
                "abcdefg1234567890"
            ]
        },
        // ImageCriterion 2: Allow AMIs from providers whose accounts are
        // "123456789012" OR "123456789013" AND AMI age is less than 300 days
        {
            "ImageProviders": [
                "123456789012",
                "123456789013"
            ],
            "CreationDateCondition": {
                "MaximumDaysSinceCreated": 300
            }
        },
        // ImageCriterion 3: Allow AMIs from provider whose account is "123456789014"
        // AND with names following the pattern "golden-ami-*"
        {
            "ImageProviders": [
                "123456789014"
            ],
            "ImageNames": [
                "golden-ami-*"
            ]
        },
        // ImageCriterion 4: Allow AMIs from Amazon or verified providers
        // AND which aren't deprecated
        {
            "ImageProviders": [
```

```
                "amazon"
            ],
            "DeprecationTimeCondition": {
                "MaximumDaysSinceDeprecated": 0
            }
        }
    ]
}
```

So werden Kriterien bewertet

In der folgenden Tabelle werden die Bewertungsregeln erläutert, mit denen festgelegt wird, ob ein AMI zulässig ist, und es wird gezeigt, wie der Operator AND bzw. OR auf jeder Ebene angewendet wird:

Auswertungsdaten	Operator	Anforderung für ein zulässiges AMI
Parameterwerte für ImageProviders , ImageNames und MarketplaceProductCodes	OR	AMI muss mit mindestens einem Wert in jeder Parameterliste übereinstimmen
ImageCriterion	AND	AMI muss allen Parametern in jedem ImageCriterion entsprechen
ImageCriteria	OR	AMI muss mit einem der ImageCriterion übereinstimmen

Sehen wir uns anhand der obigen Bewertungsregeln an, wie diese auf ImageCriteria Beispiel angewendet werden können:

- ImageCriterion1: Erlaubt AMIs , die den AWS Marketplace Produktcode haben abcdefg1234567890

  OR

- `ImageCriterion2`: AMIs Genehmigungen, die diese beiden Kriterien erfüllen:
  - Gehört einem der Konten `123456789012` `OR` `123456789013`
    - `AND`
  - In den letzten 300 Tagen erstellt

  `OR`
- `ImageCriterion3`: AMIs Genehmigungen, die diese beiden Kriterien erfüllen:
  - Gehört dem Konto `123456789014`
    - `AND`
  - Benannt nach dem Muster `golden-ami-*`

  `OR`
- `ImageCriterion4`: Ermöglicht AMIs , die diese beiden Kriterien erfüllen:
  - Von Amazon oder verifizierten Anbietern veröffentlicht (durch den `amazon`-Alias angegeben)
    - `AND`
  - Nicht veraltet (die maximale Anzahl von Tagen seit der Außerbetriebnahme beträgt `0`)

Einschränkungen

Das `ImageCriteria` enthält bis zu:

- 10 `ImageCriterion`

Jedes `ImageCriterion` enthält bis zu:

- 200 Werte für `ImageProviders`
- 50 Werte für `ImageNames`
- 50 Werte für `MarketplaceProductCodes`

Beispiel für Grenzwerte

Unter Verwendung des Vorhergehenden ImageCriteria Beispiel:

- Es gibt 4 `ImageCriterion`. Bis zu 6 weitere können der Anforderung hinzugefügt werden, um das Limit von 10 zu erreichen.

- Im ersten `ImageCriterion` gibt es 1 Wert für `MarketplaceProductCodes`. Bis zu 49 weitere können diesem `ImageCriterion` hinzugefügt werden, um das Limit von 50 zu erreichen.
- Im zweiten `ImageCriterion` gibt es 2 Werte für `ImageProviders`. Bis zu 198 weitere können diesem `ImageCriterion` hinzugefügt werden, um das Limit von 200 zu erreichen.
- Im dritten `ImageCriterion` gibt es 1 Wert für `ImageNames`. Bis zu 49 weitere können diesem `ImageCriterion` hinzugefügt werden, um das Limit von 50 zu erreichen.

Zulässige AMIs Operationen

Die AMIs Funktion „Zugelassen“ hat drei Betriebszustände für die Verwaltung der Bildkriterien: aktiviert, deaktiviert und Überwachungsmodus. Diese ermöglichen es Ihnen, die Image-Kriterien zu aktivieren oder zu deaktivieren oder sie nach Bedarf zu überprüfen.

Aktiviert

Wenn „ AMIs Zulässig“ aktiviert ist:

- Die `ImageCriteria` werden angewendet.
- Nur zulässige Bilder AMIs sind in der EC2 Konsole auffindbar und verwenden APIs dabei Bilder (zum Beispiel Bilder, die Bilder beschreiben, kopieren, speichern oder andere Aktionen ausführen).
- Instanzen können nur mit der Option „Zugelassen“ gestartet werden. AMIs

Disabled

Wenn Allowed deaktiviert AMIs ist:

- Die `ImageCriteria` werden nicht angewendet.
- Es gibt keine Einschränkungen für die Auffindbarkeit oder Nutzung von AMIs.

Prüfmodus

Im Prüfmodus:

- Die `ImageCriteria` sind aktiviert, aber es gibt keine Einschränkungen für die Auffindbarkeit oder Nutzung von AMIs.
- In der EC2 Konsole wird im Feld Zulässiges Bild für jedes AMI entweder Ja oder Nein angezeigt, um anzugeben, ob das AMI für Benutzer im Konto auffindbar und verfügbar sein wird, wenn Allowed aktiviert AMIs ist.

- In der Befehlszeile enthält die Antwort für den `describe-image` Vorgang `"ImageAllowed": true` oder gibt `"ImageAllowed": false` an, ob das AMI auffindbar und für Benutzer im Konto verfügbar sein wird, wenn Allowed aktiviert AMIs ist.
- In der EC2 Konsole wird im AMI-Katalog neben der Option Nicht erlaubt angezeigt AMIs , wenn die Option Zulässig für Benutzer im Konto nicht auffindbar oder verfügbar AMIs ist.

Bewährte Methoden für die Implementierung von Allowed AMIs

Beachten Sie bei der Implementierung von Allowed diese bewährten Methoden AMIs, um einen reibungslosen Übergang zu gewährleisten und potenzielle Störungen in Ihrer AWS Umgebung zu minimieren.

1. Prüfmodus aktivieren

   Aktivieren Sie zunächst die Option AMIs Zulässig im Überwachungsmodus. In diesem Status können Sie sehen, welche Kriterien von Ihren Kriterien betroffen AMIs wären, ohne den Zugriff tatsächlich einzuschränken, was einen risikofreien Testzeitraum ermöglicht.

2. Legen Sie die zulässigen Kriterien fest AMIs

   Stellen Sie sorgfältig fest, welche AMI-Anbieter den Sicherheitsrichtlinien, Compliance-Anforderungen und betrieblichen Anforderungen Ihres Unternehmens entsprechen.

   > **Note**
   >
   > Wenn Sie AWS verwaltete Services wie Amazon ECS oder Amazon EKS verwenden, empfehlen wir, den `amazon` Alias anzugeben, der AMIs erstellt von zugelassen werden soll AWS. Diese Dienste hängen davon ab, ob Amazon Instances veröffentlicht hat AMIs , um sie zu starten.
   > Seien Sie vorsichtig, wenn Sie `CreationDateCondition` Einschränkungen für irgendwelche festlegen. AMIs Wenn Sie zu restriktive Datumsbedingungen festlegen (z. B. AMIs dürfen sie weniger als 5 Tage alt sein), kann dies zu Fehlern beim Starten von Instances führen, wenn die Daten AMIs, unabhängig davon, ob sie von AWS oder anderen Anbietern stammen, nicht innerhalb des angegebenen Zeitrahmens aktualisiert werden. Wir empfehlen die Kombination von `ImageNames` mit `ImageProviders`, um eine bessere Kontrolle und Spezifität zu gewährleisten. Durch die alleinige Verwendung von `ImageNames` kann ein AMI möglicherweise nicht eindeutig identifiziert werden.

3. Prüfen Sie, ob sich dies auf die zu erwartenden Geschäftsprozesse auswirkt

   Sie können die Konsole oder die CLI verwenden, um alle Instances zu identifizieren, mit AMIs denen gestartet wurde und die die angegebenen Kriterien nicht erfüllen. Diese Informationen können Ihnen bei der Entscheidung helfen, entweder Ihre Startkonfigurationen so zu aktualisieren, dass sie konform sind AMIs (z. B. indem Sie ein anderes AMI in einer Startvorlage angeben) oder Ihre Kriterien so anzupassen, dass sie dies zulassen AMIs.

   Konsole: Verwenden Sie die ec2- instance-launched-with-allowed AWS Config -ami-Regel, um zu überprüfen, ob laufende oder gestoppte Instances gestartet wurden AMIs , die Ihren Zulassungskriterien entsprechen. AMIs Die Regel lautet NON_COMPLIANT, wenn ein AMI die AMIs Zulassungskriterien nicht erfüllt, und COMPLIANT, falls dies der Fall ist. Die Regel funktioniert nur, wenn die AMIs Einstellung „Zugelassen“ auf „Aktiviert“ oder „Überwachungsmodus“ gesetzt ist.

   CLI: Führen Sie den describe-instance-image-metadataBefehl aus und filtern Sie die Antwort, um alle Instances zu identifizieren, AMIs die mit gestartet wurden und die die angegebenen Kriterien nicht erfüllen.

   Informationen zur Verwendung der Konsole und der CLI finden Sie unter Suchen Sie nach InstancesAMIs , die von dort aus gestartet wurden, die nicht erlaubt sind.

4. Zulässig aktivieren AMIs

   Sobald Sie bestätigt haben, dass sich die Kriterien nicht negativ auf die erwarteten Geschäftsprozesse auswirken, aktivieren Sie die Option Zulässig AMIs.

5. Instance-Starts überwachen

   Überwachen Sie weiterhin Instance-Starts AMIs in all Ihren Anwendungen und den von Ihnen verwendeten AWS verwalteten Services wie Amazon EMR, Amazon ECR, Amazon EKS und. AWS Elastic Beanstalk Suchen Sie nach unerwarteten Problemen und nehmen Sie die erforderlichen Anpassungen an den Zulassungskriterien vor. AMIs

6. Pilot neu AMIs

   Um Drittanbieter zu testen AMIs , die nicht Ihren aktuellen AMIs Einstellungen für „Zulässig“ entsprechen, AWS empfiehlt es sich, die folgenden Methoden anzuwenden:

   - Verwenden Sie ein separates Konto AWS-Konto: Erstellen Sie ein Konto ohne Zugriff auf Ihre geschäftskritischen Ressourcen. Stellen AMIs Sie sicher, dass die AMIs Einstellung Zulässig in

diesem Konto nicht aktiviert ist oder dass die zu testenden Daten ausdrücklich zugelassen sind, damit Sie sie testen können.

- Testen Sie in einem anderen AWS-Region: Verwenden Sie eine Region, in der Drittanbieter verfügbar AMIs sind, in der Sie die AMIs Einstellungen „Zulässig“ jedoch noch nicht aktiviert haben.

Diese Ansätze tragen dazu bei, dass Ihre geschäftskritischen Ressourcen geschützt bleiben, während Sie neue Ressourcen testen. AMIs

Erforderliche IAM-Berechtigungen

Um die AMIs Funktion „Zugelassen“ verwenden zu können, benötigen Sie die folgenden IAM-Berechtigungen:

- `GetAllowedImagesSettings`
- `EnableAllowedImagesSettings`
- `DisableAllowedImagesSettings`
- `ReplaceImageCriteriaInAllowedImagesSettings`

Verwalten Sie die Einstellungen für „Zugelassen“ AMIs

Sie können die Einstellungen für Zulässig verwalten AMIs. Diese Einstellungen gelten pro Region pro Konto.

Aufgaben

- Zulässig aktivieren AMIs
- Legen Sie die AMIs Kriterien für Zulässig fest
- Deaktivieren Sie Erlaubt AMIs
- Rufen Sie die AMIs Kriterien für „Zulässig
- Finden Sie heraus AMIs , dass diese erlaubt sind
- Suchen Sie nach InstancesAMIs , die von dort aus gestartet wurden, die nicht erlaubt sind

Zulässig aktivieren AMIs

Sie können „Zulässig“ aktivieren AMIs und die AMIs Kriterien „Zulässig“ angeben. Wir empfehlen, dass Sie im Überwachungsmodus beginnen, der Ihnen zeigt, welche Kriterien von den Kriterien betroffen AMIs wären, ohne den Zugriff tatsächlich einzuschränken.

Console

Um „Zugelassen“ zu aktivieren AMIs

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dashboard (Dashboard).
3. Wählen Sie unter Kontoattribute (oben rechts) die Option Zulässig aus AMIs.
4. Wählen Sie auf der AMIs Registerkarte Zulässig die Option Verwalten aus.
5. Wählen Sie für Zulässige AMIs Einstellungen die Option Überwachungsmodus oder Aktiviert aus. Es wird empfohlen, im Überwachungsmodus zu beginnen, die Kriterien zu testen und dann zu diesem Schritt zurückzukehren, um die Option Zulässig zu aktivieren AMIs.
6. (Optional) Geben Sie für AMI-Kriterien die Kriterien im JSON-Format ein.
7. Wählen Sie Aktualisieren aus.

AWS CLI

Um „Zugelassen“ zu aktivieren AMIs

Verwenden Sie den Befehl enable-allowed-images-settings.

```
aws ec2 enable-allowed-images-settings --allowed-images-settings-state enabled
```

Um stattdessen den Prüfmodus zu aktivieren, geben Sie `audit-mode` statt `enabled` an.

```
aws ec2 enable-allowed-images-settings --allowed-images-settings-state audit-mode
```

PowerShell

Um „Zugelassen“ zu aktivieren AMIs

Verwenden Sie das cmdlet Enable-EC2AllowedImagesSetting.

```
Enable-EC2AllowedImagesSetting -AllowedImagesSettingsState enabled
```

Um stattdessen den Prüfmodus zu aktivieren, geben Sie `audit-mode` statt `enabled` an.

```
Enable-EC2AllowedImagesSetting -AllowedImagesSettingsState audit-mode
```

Legen Sie die AMIs Kriterien für Zulässig fest

Nachdem Sie „Zugelassen“ aktiviert haben AMIs, können Sie die AMIs Kriterien „Zulässig“ festlegen oder ersetzen.

Die korrekte Konfiguration und gültige Werte finden Sie unter Zulässige AMIs Konfiguration und Zulässige AMIs Parameter.

Console

Um die AMIs Kriterien „Zulässig“ festzulegen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dashboard (Dashboard).
3. Wählen Sie unter Kontoattribute (oben rechts) die Option Zulässig aus AMIs.
4. Wählen Sie auf der AMIs Registerkarte Zulässig die Option Verwalten aus.
5. Geben Sie für AMI-Kriterien die Kriterien im JSON-Format ein.
6. Wählen Sie Aktualisieren aus.

AWS CLI

Um die AMIs Kriterien „Zulässig“ festzulegen

Verwenden Sie den allowed-images-settings Befehl replace-image-criteria-in- und geben Sie die JSON-Datei an, die die zulässigen AMIs Kriterien enthält.

```
aws ec2 replace-image-criteria-in-allowed-images-settings --cli-input-json
 file://file_name.json
```

PowerShell

Um die zulässigen AMIs Kriterien festzulegen

Verwenden Sie das Set-EC2ImageCriteriaInAllowedImagesSettingCmdlet und geben Sie die JSON-Datei an, die die Zulassungskriterien enthält. AMIs

```
$imageCriteria = Get-Content -Path .\file_name.json | ConvertFrom-Json
Set-EC2ImageCriteriaInAllowedImagesSetting -ImageCriterion $imageCriteria
```

Deaktivieren Sie Erlaubt AMIs

Sie können „Zulässig“ AMIs wie folgt deaktivieren.

Console

Um „Zugelassen“ zu deaktivieren AMIs

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dashboard (Dashboard).
3. Wählen Sie unter Kontoattribute (oben rechts) die Option Zulässig aus AMIs.
4. Wählen Sie auf der AMIs Registerkarte Zulässig die Option Verwalten aus.
5. Wählen Sie für Zulässige AMIs Einstellungen die Option Deaktiviert aus.
6. Wählen Sie Aktualisieren aus.

AWS CLI

Um „Zugelassen“ zu deaktivieren AMIs

Verwenden Sie den Befehl disable-allowed-images-settings.

```
aws ec2 disable-allowed-images-settings
```

PowerShell

Um „Zugelassen“ zu deaktivieren AMIs

Verwenden Sie das cmdlet Disable-EC2AllowedImagesSetting.

```
Disable-EC2AllowedImagesSetting
```

Rufen Sie die AMIs Kriterien für „Zulässig

Sie können den aktuellen Status der AMIs Einstellung Zulässig und der AMIs Kriterien Zulässig abrufen.

Console

Um den AMIs Status und die Kriterien „Zulässig“ abzurufen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dashboard (Dashboard).
3. Wählen Sie unter Kontoattribute (oben rechts) die Option Zulässig aus AMIs.
4. Auf der AMIs Registerkarte Zulässig ist die AMIs Einstellung Zulässige Einstellungen auf Aktiviert, Deaktiviert oder Überwachungsmodus gesetzt.
5. Wenn der Status von Allowed entweder Enabled oder Audit Mode AMIs lautet, werden AMI-Kriterien die AMI-Kriterien im JSON-Format angezeigt.

AWS CLI

Um den Status und die Kriterien „ AMIs Zugelassen“ abzurufen

Verwenden Sie den Befehl get-allowed-images-settings.

```
aws ec2 get-allowed-images-settings
```

In der folgenden Beispielausgabe ist der Status `audit-mode` und die Image-Kriterien sind im Konto festgelegt.

```
{
    "State": "audit-mode",
    "ImageCriteria": [
        {
            "MarketplaceProductCodes": [
                "abcdefg1234567890"
            ]
        },
        {
            "ImageProviders": [
                "123456789012",
```

```
                "123456789013"
            ],
            "CreationDateCondition": {
                "MaximumDaysSinceCreated": 300
            }
        },
        {
            "ImageProviders": [
                "123456789014"
            ],
            "ImageNames": [
                "golden-ami-*"
            ]
        },
        {
            "ImageProviders": [
                "amazon"
            ],
            "DeprecationTimeCondition": {
                "MaximumDaysSinceDeprecated": 0
            }
        }
    ],
    "ManagedBy": "account"
}
```

PowerShell

Um den AMIs Status und die Kriterien „Zulässig“ abzurufen

Verwenden Sie das cmdlet Get-EC2AllowedImagesSetting.

```
Get-EC2AllowedImagesSetting | Select-Object `
    State, `
    ManagedBy, `
    @{Name='ImageProviders'; Expression={($_.ImageCriteria.ImageProviders)}}, `
    @{Name='MarketplaceProductCodes';
 Expression={($_.ImageCriteria.MarketplaceProductCodes)}}, `
    @{Name='ImageNames'; Expression={($_.ImageCriteria.ImageNames)}}, `
    @{Name='MaximumDaysSinceCreated';
 Expression={($_.ImageCriteria.CreationDateCondition.MaximumDaysSinceCreated)}}, `
    @{Name='MaximumDaysSinceDeprecated';
 Expression={($_.ImageCriteria.DeprecationTimeCondition.MaximumDaysSinceDeprecated)}}
```

In der folgenden Beispielausgabe ist der Status `audit-mode` und die Image-Kriterien sind im Konto festgelegt.

```
State      : audit-mode
ManagedBy  : account
ImageProviders            : {123456789012, 123456789013, 123456789014, amazon}
MarketplaceProductCodes   : {abcdefg1234567890}
ImageNames                : {golden-ami-*}
MaximumDaysSinceCreated   : 300
MaximumDaysSinceDeprecated: 0
```

Finden Sie heraus AMIs , dass diese erlaubt sind

Sie können herausfinden AMIs , welche nach den aktuellen AMIs Zulassungskriterien zulässig oder nicht zulässig sind.

> **Note**
>
> AMIs Zulässig muss sich im Überwachungsmodus befinden.

Console

Um zu überprüfen, ob ein AMI die zulässigen AMIs Kriterien erfüllt

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich AMIs aus.
3. Wählen Sie das AMI aus.
4. Suchen Sie auf der Registerkarte Details (wenn Sie das Kontrollkästchen aktiviert haben) oder im Übersichtsbereich (wenn Sie die AMI-ID ausgewählt haben) das Feld Zulässiges AMI.
   - Ja — Das AMI erfüllt die zulässigen AMIs Kriterien. Dieses AMI steht Benutzern in Ihrem Konto zur Verfügung, nachdem Sie Allowed aktiviert habenAMIs.
   - Nein — Das AMI erfüllt nicht die zulässigen AMIs Kriterien.
5. Wählen Sie im Navigationsbereich die Option AMI-Katalog aus.

Ein AMI, das als Nicht zulässig markiert ist, weist auf ein AMI hin, das die AMIs Zulassungskriterien nicht erfüllt. Dieses AMI ist für Benutzer in Ihrem Konto nicht sichtbar oder verfügbar, wenn Zulässig aktiviert AMIs ist.

AWS CLI

Um zu überprüfen, ob ein AMI die zulässigen AMIs Kriterien erfüllt

Verwenden Sie den Befehl describe-images.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query Images[].ImageAllowed \
    --output text
```

Es folgt eine Beispielausgabe.

```
True
```

Um herauszufinden AMIs , ob sie die zulässigen AMIs Kriterien erfüllen

Verwenden Sie den Befehl describe-images.

```
aws ec2 describe-images \
    --filters "Name=image-allowed,Values=true" \
    --max-items 10 \
    --query Images[].ImageId
```

Es folgt eine Beispielausgabe.

```
ami-000eaaa8be2fd162a
ami-000f82db25e50de8e
ami-000fc21eb34c7a9a6
ami-0010b876f1287d7be
ami-0010b929226fe8eba
ami-0010957836340aead
ami-00112c992a47ba871
ami-00111759e194abcc1
ami-001112565ffcafa5e
```

```
ami-0011e45aaee9fba88
```

PowerShell

Um zu überprüfen, ob ein AMI die zulässigen AMIs Kriterien erfüllt

Verwenden Sie das cmdlet Get-EC2Image.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).ImageAllowed
```

Es folgt eine Beispielausgabe.

```
True
```

Um herauszufinden AMIs , ob sie die zulässigen AMIs Kriterien erfüllen

Verwenden Sie das cmdlet Get-EC2Image.

```
Get-EC2Image `
    -Filter @{Name="image-allows";Values="true"} `
    -MaxResult 10 | `
    Select ImageId
```

Es folgt eine Beispielausgabe.

```
ami-000eaaa8be2fd162a
ami-000f82db25e50de8e
ami-000fc21eb34c7a9a6
ami-0010b876f1287d7be
ami-0010b929226fe8eba
ami-0010957836340aead
ami-00112c992a47ba871
ami-00111759e194abcc1
ami-001112565ffcafa5e
ami-0011e45aaee9fba88
```

Suchen Sie nach InstancesAMIs , die von dort aus gestartet wurden, die nicht erlaubt sind

Sie können die Instances identifizieren, die mit einem AMI gestartet wurden, das die AMIs Zulassungskriterien nicht erfüllt.

Console

So überprüfen Sie, ob eine Instance mit einem nicht zulässigen AMI gestartet wurde

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.
4. Suchen Sie auf der Registerkarte Details unter Instance-Details Zulässiges Image.
   - Ja — Das AMI erfüllt die zulässigen AMIs Kriterien.
   - Nein — Das AMI erfüllt nicht die zulässigen AMIs Kriterien.

AWS CLI

So finden Sie Instances, die damit gestartet wurden AMIs , dass sie nicht erlaubt sind

Verwenden Sie den Befehl describe-instance-image-metadata mit dem Filter `image-allowed`.

```
aws ec2 describe-instance-image-metadata \
    --filters "Name=image-allowed,Values=false" \
    --query "InstanceImageMetadata[*].[InstanceId,ImageMetadata.ImageId]" \
    --output table
```

Es folgt eine Beispielausgabe.

```
-------------------------------------------------
|          DescribeInstanceImageMetadata         |
+----------------------+-------------------------+
|  i-08fd74f3f1595fdbd |  ami-09245d5773578a1d6  |
|  i-0b1bf24fd4f297ab9 |  ami-07cccf2bd80ed467f  |
|  i-026a2eb590b4f7234 |  ami-0c0ec0a3a3a4c34c0  |
|  i-006a6a4e8870c828f |  ami-0a70b9d193ae8a799  |
|  i-0781e91cfeca3179d |  ami-00c257e12d6828491  |
|  i-02b631e2a6ae7c2d9 |  ami-0bfddf4206f1fa7b9  |
+----------------------+-------------------------+
```

PowerShell

So finden Sie Instances, die damit gestartet wurden AMIs , dass sie nicht erlaubt sind

Verwenden Sie das cmdlet Get-EC2InstanceImageMetadata.

```
Get-EC2InstanceImageMetadata `
    -Filter @{Name="image-allowed";Values="false"} | `
    Select InstanceId, @{Name='ImageId'; Expression={($_.ImageMetadata.ImageId)}}
```

Es folgt eine Beispielausgabe.

```
InstanceId          ImageId
----------          -------
i-08fd74f3f1595fdbd ami-09245d5773578a1d6
i-0b1bf24fd4f297ab9 ami-07cccf2bd80ed467f
i-026a2eb590b4f7234 ami-0c0ec0a3a3a4c34c0
i-006a6a4e8870c828f ami-0a70b9d193ae8a799
i-0781e91cfeca3179d ami-00c257e12d6828491
i-02b631e2a6ae7c2d9 ami-0bfddf4206f1fa7b9
```

AWS Config

Sie können die ec2- instance-launched-with-allowed AWS Config -ami-Regel hinzufügen, sie für Ihre Anforderungen konfigurieren und sie dann zur Evaluierung Ihrer Instances verwenden.

Weitere Informationen finden Sie unter AWS Config Regeln hinzufügen und ec2- instance-launched-with-allowed -ami im Entwicklerhandbuch.AWS Config

Machen Sie Ihr AMI für die Verwendung in Amazon öffentlich verfügbar EC2

Sie können Ihr AMI öffentlich zugänglich machen, indem Sie es mit allen teilen AWS-Konten.

Wenn Sie verhindern möchten, dass Ihr Konto öffentlich geteilt wird AMIs, können Sie die Option Öffentlichen Zugriff sperren für aktivieren AMIs. Dadurch werden alle Versuche, ein AMI zu veröffentlichen, blockiert, was dazu beiträgt, unbefugten Zugriff und potenziellen Missbrauch von AMI-Daten zu verhindern. Beachten Sie, dass sich die Aktivierung des Blocks öffentlichen Zugriffs nicht auf Ihre AMIs bereits öffentlich verfügbaren Dateien auswirkt. Sie bleiben weiterhin öffentlich verfügbar. Weitere Informationen finden Sie unter Verstehen Sie, öffentlichen Zugriff sperren für AMIs.

Wenn Sie nur bestimmten Konten erlauben möchten, Ihr AMI zum Starten von Instances zu verwenden, lesen Sie Freigeben eines AMI für bestimmte AWS -Konten.

Inhalt

- Überlegungen
- Ein AMI mit allen AWS Konten teilen (öffentlich teilen)

Überlegungen

Beachten Sie Folgendes, bevor Sie ein AMI öffentlich machen.

- Eigentum — Um ein AMI zu veröffentlichen, AWS-Konto müssen Sie Eigentümer des AMI sein.
- Region — AMIs sind eine regionale Ressource. Wenn Sie ein AMI freigeben, ist es nur in der Region verfügbar, in der Sie es freigegeben haben. Um ein AMI in einer anderen Region verfügbar zu machen, kopieren Sie das AMI in die Region und geben Sie es dann frei. Weitere Informationen finden Sie unter Ein EC2 Amazon-AMI kopieren.
- Öffentlichen Zugriff blockieren — Um ein AMI öffentlich zu teilen, AMIs muss in jeder Region, in der das AMI öffentlich geteilt wird, die Sperrung des öffentlichen Zugriffs für deaktiviert sein. Nachdem Sie das AMI öffentlich geteilt haben, können Sie Block Public Access wieder aktivieren, AMIs um zu verhindern, dass Ihr AMIs AMI weiter öffentlich geteilt wird.
- Einige AMIs können nicht veröffentlicht werden — Wenn Ihr AMI eine der folgenden Komponenten enthält, können Sie es nicht veröffentlichen (aber Sie können das AMI mit bestimmten teilen AWS-Konten):
  - Verschlüsselte Volumes
  - Snapshots von verschlüsselten Volumes
  - Produkt-Codes
- Offenlegung sensibler Daten vermeiden: Damit beim Freigeben eines AMI keine sensiblen Daten offengelegt werden, lesen Sie die Sicherheitserwägungen in Empfehlungen für die Erstellung von gemeinsam genutztem Linux AMIs und folgen Sie den empfohlenen Verfahren.
- Nutzung: Wenn Sie ein AMI freigeben, können Benutzer Instances nur über das AMI starten. Sie können es nicht löschen, teilen oder ändern. Wenn die Benutzer jedoch eine Instance mit Ihrem AMI gestartet haben, können sie danach von der gestarteten Instance aus ein AMI erstellen.
- Automatische Deprecation — Standardmäßig AMIs ist das Verfallsdatum aller öffentlichen Inhalte auf zwei Jahre ab dem Erstellungsdatum des AMI festgelegt. Sie können das Veralterungsdatum auf weniger als zwei Jahre festlegen. Um das Verfallsdatum zu stornieren oder das Verfallsdatum auf ein späteres Datum zu verschieben, müssen Sie das AMI als privat kennzeichnen, indem Sie es nur mit bestimmten Personen teilen. AWS-Konten

- Obsolete entfernen AMIs — Wenn ein öffentliches AMI sein Verfallsdatum erreicht hat und sechs oder mehr Monate lang keine neuen Instances über das AMI gestartet wurden, wird AWS schließlich die öffentliche Freigabeeigenschaft entfernt, sodass veraltete Instanzen AMIs nicht in den öffentlichen AMI-Listen erscheinen.
- Abrechnung — Ihnen wird nichts in Rechnung gestellt, wenn Ihr AMI von anderen AWS-Konten zum Starten von Instances verwendet wird. Die Konten, die Instances mit dem AMI starten, werden für die Instances abgerechnet, die sie starten.

Ein AMI mit allen AWS Konten teilen (öffentlich teilen)

Nachdem Sie ein AMI veröffentlicht haben, ist es in der Community AMIs in der Konsole verfügbar, auf die Sie über den AMI-Katalog im linken Navigator der EC2 Konsole oder beim Starten einer Instance über die Konsole zugreifen können. Beachten Sie, dass es eine Weile dauern kann, bis ein AMI in der Community erscheint, AMIs nachdem Sie es veröffentlicht haben.

Console

Veröffentlichen eines AMI

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich AMIs aus.
3. Wählen Sie das AMI in der Liste aus und wählen Sie Aktionen, AMI-Berechtigungen bearbeiten aus.
4. Unter AMI-Verfügbarkeit wählen Sie Öffentlich aus.
5. Wählen Sie Änderungen speichern aus.

AWS CLI

Jedes AMI hat eine `launchPermission` Eigenschaft, die steuert AWS-Konten, welche außer denen des Besitzers dieses AMI zum Starten von Instances verwenden dürfen. Indem Sie die `launchPermission` Eigenschaft eines AMI ändern, können Sie das AMI öffentlich machen (wodurch allen Startberechtigungen gewährt werden AWS-Konten) oder es nur mit den von Ihnen angegebenen AWS-Konten Benutzern teilen.

Sie können ein Konto zur Liste der Konten hinzufügen oder IDs daraus entfernen, die Startberechtigungen für ein AMI haben. Um ein AMI zu veröffentlichen, geben Sie die `all`-Gruppe an. Sie können öffentliche und explizite Startberechtigungen angeben.

Veröffentlichen eines AMI

1. Verwenden Sie den Befehl modify-image-attribute wie folgt, um die `all`-Gruppe zur `launchPermission`-Liste für das angegebene AMI hinzuzufügen.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{Group=all}]"
```

2. Um die Startberechtigungen des AMI zu überprüfen, verwenden Sie den describe-image-attribute-Befehl.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

3. (Optional) Um das AMI erneut privat zu machen, entfernen Sie die `all`-Gruppe aus den Startberechtigungen. Hinweis: Der Besitzer des AMI hat immer Startberechtigungen und bleibt daher von dem Befehl unberührt.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{Group=all}]"
```

PowerShell

Jedes AMI hat eine `launchPermission` Eigenschaft, die steuert AWS-Konten, welche außer denen des Besitzers dieses AMI zum Starten von Instances verwenden dürfen. Indem Sie die `launchPermission` Eigenschaft eines AMI ändern, können Sie das AMI öffentlich machen (wodurch allen Startberechtigungen gewährt werden AWS-Konten) oder es nur mit den von Ihnen angegebenen AWS-Konten Benutzern teilen.

Sie können ein Konto zur Liste der Konten hinzufügen oder IDs daraus entfernen, die Startberechtigungen für ein AMI haben. Um ein AMI zu veröffentlichen, geben Sie die `all`-Gruppe an. Sie können öffentliche und explizite Startberechtigungen angeben.

Veröffentlichen eines AMI

1. Verwenden Sie den Befehl Edit-EC2ImageAttribute wie folgt, um die `all`-Gruppe zur `launchPermission`-Liste für das angegebene AMI hinzuzufügen.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType add `
    -UserGroup all
```

2. Um die Startberechtigungen des AMI zu überprüfen, verwenden Sie den folgenden Get-EC2ImageAttribute-Befehl.

```
Get-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission
```

3. (Optional) Um das AMI erneut privat zu machen, entfernen Sie die `all`-Gruppe aus den Startberechtigungen. Hinweis: Der Besitzer des AMI hat immer Startberechtigungen und bleibt daher von dem Befehl unberührt.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType remove `
    -UserGroup all
```

Verstehen Sie, öffentlichen Zugriff sperren für AMIs

Um zu verhindern, dass Ihre Inhalte öffentlich geteilt werden AMIs, können Sie die Option „Öffentlichen Zugriff sperren“ AMIs auf Kontoebene aktivieren.

Wenn Block Public Access aktiviert ist, wird jeder Versuch, ein AMI öffentlich zu machen, automatisch blockiert. Wenn Sie jedoch bereits öffentlich sind AMIs, bleiben sie weiterhin öffentlich verfügbar.

Um sie öffentlich zu teilen AMIs, müssen Sie den öffentlichen Zugriff blockieren deaktivieren. Wenn Sie mit dem Teilen fertig sind, empfiehlt es sich, die Option „Öffentlichen Zugriff sperren“ wieder zu aktivieren, um ein unbeabsichtigtes öffentliches Teilen Ihrer Inhalte zu verhindern. AMIs

> **Note**
>
> Diese Einstellung wird auf Kontoebene konfiguriert, entweder direkt im Konto oder mithilfe einer deklarativen Richtlinie. Es muss in allen Bereichen konfiguriert werden, in AWS-Region

denen Sie verhindern möchten, dass Ihre Inhalte öffentlich geteilt werden. AMIs Mithilfe einer deklarativen Richtlinie können Sie die Einstellung auf mehrere Regionen gleichzeitig sowie auf mehrere Konten gleichzeitig anwenden. Wenn eine deklarative Richtlinie verwendet wird, können Sie die Einstellung nicht direkt in einem Konto ändern. In diesem Thema wird beschrieben, wie Sie die Einstellung direkt in einem Konto konfigurieren. Informationen zur Verwendung deklarativer Richtlinien finden Sie unter Deklarative Richtlinien im AWS Organizations -Benutzerhandbuch.

Sie können die IAM-Berechtigungen auf Administratorbenutzer beschränken, sodass nur dieser den öffentlichen Zugriff aktivieren oder deaktivieren kann. AMIs

Themen

- Standardeinstellungen
- Verwalte die Einstellung „Öffentlichen Zugriff blockieren“ für AMIs

Standardeinstellungen

Die AMIs Einstellung „Öffentlichen Zugriff blockieren für“ ist standardmäßig entweder aktiviert oder deaktiviert, je nachdem, ob Ihr Konto neu oder bereits vorhanden ist und ob Sie über ein öffentliches AMIs Konto verfügen. In der folgenden Tabelle werden die Standardeinstellungen aufgeführt:

AWS Konto	Sperren Sie den öffentlichen Zugriff für die AMIs Standardeinstellung
Neue Konten	Aktiviert
Bestehende Konten ohne öffentliche Konten AMIs [1]	Aktiviert
Bestehende Konten mit einem oder mehreren öffentlichen Konten AMIs	Disabled

[1] Wenn Ihr Konto AMIs am oder nach dem 15. Juli 2023 über ein oder mehrere öffentliche Konten verfügte, AMIs ist die Option Öffentlichen Zugriff sperren für für Ihr Konto standardmäßig deaktiviert, auch wenn Sie anschließend alle Konten AMIs privat gemacht haben.

Verwalte die Einstellung „Öffentlichen Zugriff blockieren“ für AMIs

Sie können die Einstellung „Öffentlichen Zugriff blockieren“ so verwalten AMIs , dass Sie kontrollieren können, ob sie öffentlich geteilt werden können. Sie können den aktuellen Status des Blockierten öffentlichen Zugriffs für Sie aktivieren, deaktivieren oder anzeigen, AMIs indem Sie die EC2 Amazon-Konsole oder die verwenden AWS CLI.

Den Status des Blockierens des öffentlichen Zugriffs anzeigen für AMIs

Um zu sehen, ob das öffentliche Teilen von Ihnen in Ihrem Konto gesperrt AMIs ist, können Sie den Status für die Sperrung des öffentlichen Zugriffs einsehen AMIs. Sie müssen in jedem Bundesland, AWS-Region in dem Sie sehen möchten, ob das öffentliche Teilen Ihres Kontos gesperrt AMIs ist, einsehen.

Erforderliche Berechtigungen

Um die aktuelle Einstellung zum Sperren des öffentlichen Zugriffs für abzurufen AMIs, benötigen Sie die `GetImageBlockPublicAccessState` IAM-Berechtigung.

Console

Um den Status der Blockierung des öffentlichen Zugriffs AMIs in der angegebenen Region anzuzeigen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste (oben auf dem Bildschirm) die Region aus, für die der Status „Öffentlicher Zugriff gesperrt“ angezeigt werden soll AMIs.
3. Wenn das Dashboard nicht angezeigt wird, wählen Sie im Navigationsbereich EC2 Dashboard aus.
4. Wählen Sie unter Kontoattribute die Option Datenschutz und Sicherheit aus.
5. Aktivieren Sie unter Öffentlichen Zugriff sperren für AMIs das Feld Öffentlicher Zugriff. Der Wert lautet entweder Neues öffentliches Teilen blockiert oder Neues öffentliches Teilen erlaubt.

AWS CLI

Um den Status „Öffentlichen Zugriff blockieren“ abzurufen für AMIs

Verwenden Sie den Befehl get-image-block-public-access-state. Der Wert ist entweder `block-new-sharing` oder `unblocked`.

Beispiel: Für eine spezifische Region

```
aws ec2 get-image-block-public-access-state --region us-east-1
```

Das `ManagedBy`-Feld gibt die Entität an, die die Einstellung konfiguriert hat. `account` zeigt in diesem Beispiel an, dass die Einstellung direkt im Konto konfiguriert wurde. Ein Wert von `declarative-policy` würde bedeuten, dass die Einstellung durch eine deklarative Richtlinie konfiguriert wurde. Weitere Informationen finden Sie unter Deklarative Richtlinien im AWS Organizations -Benutzerhandbuch.

```
{
    "ImageBlockPublicAccessState": "block-new-sharing",
    "ManagedBy": "account"
}
```

Beispiel: Für all Regionen in Ihrem Konto

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 get-image-block-public-access-state \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Es folgt eine Beispielausgabe.

```
Region           Public Access State
--------------   ----------------------
ap-south-1       block-new-sharing
eu-north-1       unblocked
eu-west-3        block-new-sharing
...
```

PowerShell

Um den Status des Blockierens des öffentlichen Zugriffs für abzurufen AMIs

Verwenden Sie das cmdlet Get-EC2ImageBlockPublicAccessState. Der Wert ist entweder `block-new-sharing` oder `unblocked`.

Beispiel: Für eine spezifische Region

```
Get-EC2ImageBlockPublicAccessState -Region us-east-1
```

Es folgt eine Beispielausgabe.

```
block-new-sharing
```

Beispiel: Für all Regionen in Ihrem Konto

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
        [PSCustomObject]@{
            Region   = $_
            PublicAccessState = (Get-EC2ImageBlockPublicAccessState -Region $_)
        }
} | `
Format-Table -AutoSize
```

Es folgt eine Beispielausgabe.

```
Region         PublicAccessState
------         -----------------
ap-south-1     block-new-sharing
eu-north-1     block-new-sharing
eu-west-3      block-new-sharing
...
```

Aktivieren Sie „Öffentlichen Zugriff blockieren“ für AMIs

Um zu verhindern, dass Ihre Inhalte öffentlich geteilt werden AMIs, aktivieren Sie die Option Öffentlichen Zugriff sperren für AMIs auf Kontoebene. Sie müssen die Option „Öffentlichen Zugriff sperren“ für AMIs alle AWS-Region Bereiche aktivieren, in denen Sie das öffentliche Teilen Ihrer Daten verhindern möchten AMIs. Wenn Sie bereits öffentlich sind AMIs, bleiben sie weiterhin öffentlich verfügbar.

Erforderliche Berechtigungen

Um die Einstellung „Öffentlichen Zugriff blockieren“ für zu aktivieren AMIs, benötigen Sie die `EnableImageBlockPublicAccess` IAM-Berechtigung.

Überlegungen

- Es kann bis zu 10 Minuten dauern, diese Einstellung zu konfigurieren. Wenn Sie während dieser Zeit den Status des öffentlichen Zugriffs beschreiben, lautet die Antwort `unblocked`. Wenn die Konfiguration abgeschlossen ist, lautet die Antwort `block-new-sharing`.

Console

Um die Option „Öffentlichen Zugriff blockieren“ für die angegebene AMIs Region zu aktivieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste (oben auf dem Bildschirm) die Region aus, für die die Sperrung des öffentlichen Zugriffs aktiviert werden soll AMIs.
3. Wenn das Dashboard nicht angezeigt wird, wählen Sie im Navigationsbereich EC2 Dashboard aus.
4. Wählen Sie unter Kontoattribute die Option Datenschutz und Sicherheit aus.
5. Wählen Sie unter Öffentlichen Zugriff blockieren für AMIs die Option Verwalten aus.
6. Wählen Sie das Kontrollkästchen Öffentliche Freigabe blockieren und wählen Sie Aktualisieren.

AWS CLI

Um die Option „Öffentlichen Zugriff blockieren“ für zu aktivieren AMIs

Verwenden Sie den Befehl enable-image-block-public-access.

Beispiel: Für eine spezifische Region

```
aws ec2 enable-image-block-public-access \
--region us-east-1 \
--image-block-public-access-state block-new-sharing
```

Es folgt eine Beispielausgabe.

```
{
    "ImageBlockPublicAccessState": "block-new-sharing"
}
```

Beispiel: Für all Regionen in Ihrem Konto

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 enable-image-block-public-access \
            --region $region \
            --image-block-public-access-state block-new-sharing \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Es folgt eine Beispielausgabe.

```
Region           Public Access State
--------------   ----------------------
ap-south-1       block-new-sharing
eu-north-1       block-new-sharing
eu-west-3        block-new-sharing
...
```

PowerShell

Um den öffentlichen Zugriff blockieren für zu aktivieren AMIs

Verwenden Sie den Befehl Enable-EC2ImageBlockPublicAccess.

Beispiel: Für eine spezifische Region

```
Enable-EC2ImageBlockPublicAccess `
    -Region us-east-1 `
    -ImageBlockPublicAccessState block-new-sharing
```

Es folgt eine Beispielausgabe.

```
Value
-----
block-new-sharing
```

Beispiel: Für all Regionen in Ihrem Konto

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (
        Enable-EC2ImageBlockPublicAccess `
         -Region $_ `
         -ImageBlockPublicAccessState block-new-sharing)
    }
} | `
Format-Table -AutoSize
```

Es folgt eine Beispielausgabe.

```
Region         PublicAccessState
------         -----------------
ap-south-1     block-new-sharing
eu-north-1     block-new-sharing
eu-west-3      block-new-sharing
...
```

Deaktivieren Sie die Option „Öffentlichen Zugriff blockieren“ für AMIs

Damit die Nutzer in Ihrem Konto Ihr Konto öffentlich teilen können AMIs, deaktivieren Sie die Option „Öffentlichen Zugriff sperren“ auf Kontoebene. Sie müssen die Sperrung des öffentlichen Zugriffs für AMIs alle AWS-Region Bereiche deaktivieren, in denen Sie das öffentliche Teilen Ihrer Daten zulassen möchtenAMIs.

Erforderliche Berechtigungen

Um die Einstellung „Öffentlichen Zugriff blockieren“ für zu deaktivieren AMIs, benötigen Sie die `DisableImageBlockPublicAccess` IAM-Berechtigung.

Überlegungen

- Es kann bis zu 10 Minuten dauern, diese Einstellung zu konfigurieren. Wenn Sie während dieser Zeit den Status des öffentlichen Zugriffs beschreiben, lautet die Antwort `block-new-sharing`. Wenn die Konfiguration abgeschlossen ist, lautet die Antwort `unblocked`.

Console

Um den öffentlichen Zugriff blockieren für die angegebene AMIs Region zu deaktivieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste (oben auf dem Bildschirm) die Region aus, für die Sie die Sperrung des öffentlichen Zugriffs deaktivieren möchten AMIs.
3. Wenn das Dashboard nicht angezeigt wird, wählen Sie im Navigationsbereich EC2 Dashboard aus.
4. Wählen Sie unter Kontoattribute die Option Datenschutz und Sicherheit aus.
5. Wählen Sie unter Öffentlichen Zugriff blockieren für AMIs die Option Verwalten aus.
6. Wählen Sie das Kontrollkästchen Öffentliche Freigabe blockieren ab und wählen Sie Speichern.
7. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`confirm`** ein und wählen Sie dann Allow public sharing (Öffentliches Teilen zulassen) aus.

AWS CLI

Um den öffentlichen Zugriff blockieren für zu deaktivieren AMIs

Verwenden Sie den Befehl disable-image-block-public-access.

Beispiel: Für eine spezifische Region

```
aws ec2 disable-image-block-public-access --region us-east-1
```

Es folgt eine Beispielausgabe.

```
{
   "ImageBlockPublicAccessState": "unblocked"
}
```

Beispiel: Für all Regionen in Ihrem Konto

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 disable-image-block-public-access \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Es folgt eine Beispielausgabe.

```
Region           Public Access State
--------------   ----------------------
ap-south-1       unblocked
eu-north-1       unblocked
eu-west-3        unblocked
...
```

PowerShell

Um den öffentlichen Zugriff blockieren für zu deaktivieren AMIs

Verwenden Sie das cmdlet Disable-EC2ImageBlockPublicAccess.

Beispiel: Für eine spezifische Region

```
Disable-EC2ImageBlockPublicAccess -Region us-east-1
```

Es folgt eine Beispielausgabe.

```
Value
-----
unblocked
```

Beispiel: Für all Regionen in Ihrem Konto

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (Disable-EC2ImageBlockPublicAccess -Region $_)
    }
} | `
Format-Table -AutoSize
```

Es folgt eine Beispielausgabe.

```
Region         PublicAccessState
------         -----------------
ap-south-1     unblocked
eu-north-1     unblocked
eu-west-3      unblocked
...
```

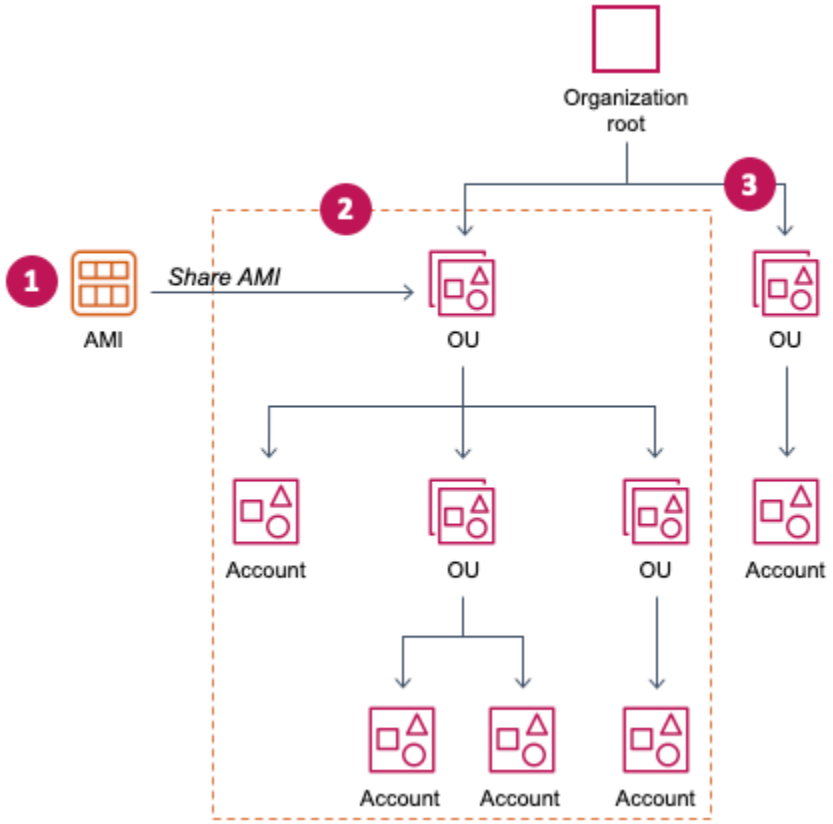
Ein AMI für bestimmte Organisationen oder Organisationseinheiten freigeben

AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie erstellen und zentral verwalten.

Sie können ein AMI zusätzlich zur Freigabe für bestimmte Konten für eine von Ihnen erstellte Organisation oder Organisationseinheit (OE) freigeben.

Eine Organisation ist eine juristische Stelle, die Sie erstellen, um Ihre AWS-Konten zu konsolidieren und zentral zu verwalten. Sie können die Konten in einer hierarchischen, Baumstruktur organisieren, mit einem Stamm an der Spitze und Organisationseinheiten, die unterhalb des Organisationsstamms angeordnet sind. Jedes Konto kann direkt zum Stammkonto hinzugefügt oder einem der Konten OUs in der Hierarchie zugeordnet werden. Weitere Informationen finden Sie unter AWS -Organizations – Terminologie und Konzepte im AWS Organizations -Benutzerhandbuch.

Wenn Sie ein AMI für eine Organisation oder eine OE freigeben, erhalten alle untergeordneten Konten Zugriff auf das AMI. Im folgenden Diagramm wird das AMI beispielsweise mit einer Organisationseinheit der obersten Ebene geteilt (durch den Pfeil bei der Nummer 1 angezeigt). Alle Konten OUs und, die sich unterhalb dieser Organisationseinheit der obersten Ebene befinden (gekennzeichnet durch die gepunktete Linie bei Nummer 2), haben ebenfalls Zugriff auf das AMI. Die Konten in der Organisation und OE außerhalb der gestrichelten Linie (gekennzeichnet durch die Zahl 3) haben keinen Zugriff auf das AMI, da sie der OE nicht untergeordnet sind, für die das AMI freigegeben ist.



Themen

- Überlegungen
- Den ARN einer Organisation oder Organisationseinheit abrufen
- Erlauben Sie Organisationen und OUs die Verwendung eines KMS-Schlüssels
- Gemeinsame Nutzung von AMI mit einer Organisation oder OU verwalten

Überlegungen

Beachten Sie bei der Weitergabe AMIs an bestimmte Organisationen oder Organisationseinheiten Folgendes.

- Eigentümerschaft – Um ein AMI freizugeben, muss Ihr AWS-Konto Besitzer des AMI sein.
- Freigabelimits — Der AMI-Besitzer kann ein AMI mit jeder Organisation oder Organisationseinheit teilen, auch mit Organisationen OUs , denen er nicht angehört.

  Die maximale Anzahl von Entitäten, für die ein AMI innerhalb einer Region gemeinsam genutzt werden kann, finden Sie in den EC2 Amazon-Servicekontingenten.
- Tags – Sie können keine benutzerdefinierten Tags (Tags, die Sie einem AMI anfügen) freigeben. Wenn Sie ein AMI teilen, sind Ihre benutzerdefinierten Tags für niemanden AWS-Konto in einer Organisation oder Organisationseinheit verfügbar, mit der das AMI geteilt wird.
- ARN-Format: Wenn Sie eine Organisation oder OE in einem Befehl angeben, achten Sie darauf, das richtige ARN-Format zu verwenden. Sie erhalten eine Fehlermeldung, wenn Sie nur die ID angeben, z. B. wenn Sie nur `o-123example` oder `ou-1234-5example` angeben.

  Richtige ARN-Formate:

  - ARN der Organisation: `arn:aws:organizations::`*`111122223333`*`:organization/`*`organization-id`*
  - OE-ARN: `arn:aws:organizations::`*`111122223333`*`:ou/`*`organization-id`*`/`*`ou-id`*

  Wobei Folgendes gilt:

  - *`111122223333`* ist ein Beispiel für die 12-stellige Konto-ID für das Verwaltungskonto. Wenn Sie die Verwaltungskontonummer nicht kennen, können Sie die Organisation oder die Organisationseinheit beschreiben, um den ARN zu erhalten, der die Verwaltungskontonummer enthält. Weitere Informationen finden Sie unter Den ARN einer Organisation oder Organisationseinheit abrufen.
  - *`organization-id`* ist die Organisations-ID, beispielsweise `o-123example`.
  - *`ou-id`* ist die ID der Organisationseinheit, beispielsweise `ou-1234-5example`.

Weitere Informationen zum Format von ARNs finden Sie unter Amazon Resource Names (ARNs) im IAM-Benutzerhandbuch.

- Verschlüsselung und Schlüssel — Sie können Daten teilen AMIs , die durch unverschlüsselte und verschlüsselte Snapshots gesichert sind.
  - Die verschlüsselten Snapshots müssen mit einem vom Kunden verwalteten Schlüssel verschlüsselt sein. Sie können keine Dateien teilenAMIs , die auf Snapshots basieren, die mit dem verwalteten AWS Standardschlüssel verschlüsselt wurden.
  - Wenn Sie ein AMI gemeinsam nutzen, das auf verschlüsselten Snapshots basiert, müssen Sie den Organisationen oder OUs der Verwendung der vom Kunden verwalteten Schlüssel, die zur Verschlüsselung der Snapshots verwendet wurden, gestatten. Weitere Informationen finden Sie unter Erlauben Sie Organisationen und OUs die Verwendung eines KMS-Schlüssels.
- Region — AMIs sind eine regionale Ressource. Wenn Sie ein AMI freigeben, ist es nur in der Region verfügbar, in der Sie es freigegeben haben. Um ein AMI in einer anderen Region verfügbar zu machen, kopieren Sie das AMI in die Region und geben Sie es dann frei. Weitere Informationen finden Sie unter Ein EC2 Amazon-AMI kopieren.
- Nutzung: Wenn Sie ein AMI freigeben, können Benutzer Instances nur über das AMI starten. Sie können es nicht löschen, teilen oder ändern. Wenn die Benutzer jedoch eine Instance mit Ihrem AMI gestartet haben, können sie danach von der gestarteten Instance aus ein AMI erstellen.
- Abrechnung — Ihnen wird nichts in Rechnung gestellt, wenn Ihr AMI von anderen AWS-Konten zum Starten von Instances verwendet wird. Die Konten, die Instances mit dem AMI starten, werden für die Instances abgerechnet, die sie starten.

Den ARN einer Organisation oder Organisationseinheit abrufen

Die Organisation und die Organisationseinheit ARNs enthalten die 12-stellige Verwaltungskontonummer. Wenn Sie die Verwaltungskontonummer nicht kennen, können Sie die Organisation und die Organisationseinheit beschreiben, um den jeweiligen ARN zu erhalten. In den folgenden Beispielen ist `123456789012` die Konto-ID des Verwaltungskontos.

Erforderliche Berechtigungen

Bevor Sie die erhalten können ARNs, müssen Sie über die Erlaubnis verfügen, Organisationen und Organisationseinheiten zu beschreiben. Die folgende Richtlinie bietet die erforderliche Berechtigung.

JSON

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

AWS CLI

So erhalten Sie den ARN einer Organisation

Verwenden Sie den Befehl describe-organization. Fügen Sie die Option `--query` hinzu, um nur den Organisations-ARN zurückzugeben.

```
aws organizations describe-organization --query 'Organization.Arn'
```

Es folgt eine Beispielausgabe.

```
"arn:aws:organizations::123456789012:organization/o-1234567abc"
```

So erhalten Sie den ARN einer Organisationseinheit

Verwenden Sie den Befehl describe-organizational-unit. Verwenden Sie den `--query`-Parameter, um nur den ARN der Organisationseinheit zurückzugeben.

```
aws organizations describe-organizational-unit \
    --organizational-unit-id ou-a123-b4567890 \
    --query 'OrganizationalUnit.Arn'
```

Es folgt eine Beispielausgabe.

```
"arn:aws:organizations::123456789012:ou/o-1234567abc/ou-a123-b4567890"
```

PowerShell

So erhalten Sie den ARN einer Organisation

Verwenden Sie das ORGOrganization Cmdlet Get-.

```
(Get-ORGOrganization).Arn
```

Es folgt eine Beispielausgabe.

```
arn:aws:organizations::123456789012:organization/o-1234567abc
```

So erhalten Sie den ARN einer Organisationseinheit

Verwenden Sie das Cmdlet Get- ORGOrganizational Unit.

```
(Get-ORGOrganizationalUnit -OrganizationalUnitId "ou-a123-b4567890").Arn
```

Es folgt eine Beispielausgabe.

```
arn:aws:organizations::123456789012:ou/o-1234567abc/ou-a123-b4567890
```

Erlauben Sie Organisationen und OUs die Verwendung eines KMS-Schlüssels

Wenn Sie ein AMI gemeinsam nutzen, das durch verschlüsselte Snapshots unterstützt wird, müssen Sie auch den Organisationen oder Organisationseinheiten (OUs) erlauben, die KMS-Schlüssel zu verwenden, die zum Verschlüsseln der Snapshots verwendet wurden.

> **Note**
>
> Die verschlüsselten Snapshots müssen mit einem vom Kunden verwalteten Schlüssel verschlüsselt sein. Sie können keine Dateien teilen AMIs , die auf Snapshots basieren, die mit dem verwalteten Standardschlüssel verschlüsselt sind. AWS

Um den Zugriff auf den KMS-Schlüssel zu steuern, können Sie in der Schlüsselrichtlinie die Bedingungsschlüssel `aws:PrincipalOrgID` und `aws:PrincipalOrgPaths` verwenden, um nur

bestimmten Prinzipalen Zugriff auf die angegebenen Aktionen zu gewähren. Ein Principal kann ein Benutzer, eine IAM-Rolle, ein Verbundbenutzer oder AWS-Konto ein Root-Benutzer sein.

Die Bedingungsschlüssel werden wie folgt verwendet:

- `aws:PrincipalOrgID` – Erlaubt jeden Prinzipal, der zu der Organisation gehört, die durch die angegebene ID repräsentiert wird.
- `aws:PrincipalOrgPaths`— Erlaubt jeden Prinzipal, der zu den durch die angegebenen Pfade OUs dargestellten gehört.

Um einer Organisation (einschließlich der zugehörigen Konten OUs und Konten) die Erlaubnis zur Verwendung eines KMS-Schlüssels zu erteilen, fügen Sie der Schlüsselrichtlinie die folgende Anweisung hinzu.

```
{
    "Sid": "Allow access for organization root",
    "Effect": "Allow",
    "Principal": "*",
    "Action": [
        "kms:Describe*",
        "kms:List*",
        "kms:Get*",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "o-123example"
        }
    }
}
```

Um bestimmten OUs (und den zugehörigen Konten) Berechtigungen zur Verwendung eines KMS-Schlüssels zu erteilen, können Sie eine Richtlinie verwenden, die dem folgenden Beispiel ähnelt.

```
{
```

```
        "Sid": "Allow access for specific OUs and their descendants",
        "Effect": "Allow",
        "Principal": "*",
        "Action": [
            "kms:Describe*",
            "kms:List*",
            "kms:Get*",
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:ReEncrypt*",
            "kms:GenerateDataKey*",
            "kms:CreateGrant"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": "o-123example"
            },
            "ForAnyValue:StringLike": {
                "aws:PrincipalOrgPaths": [
                    "o-123example/r-ab12/ou-ab12-33333333/*",
                    "o-123example/r-ab12/ou-ab12-22222222/*"
                ]
            }
        }
}
```

Weitere Beispiele für Bedingungsanweisungen finden Sie unter aws:PrincipalOrgID und aws:PrincipalOrgPaths im IAM-Benutzerhandbuch.

Weitere Informationen über kontoübergreifender Zugriff finden Sie im AWS Key Management Service -Entwicklerhandbuch unter Zulassen der Verwendung eines KMS-Schlüssels durch Benutzer in anderen Konten.

Gemeinsame Nutzung von AMI mit einer Organisation oder OU verwalten

Sie können die AMI-Sharing mit Organisationen und Organisationseinheiten (OU) verwalten, um zu kontrollieren, ob diese EC2 Amazon-Instances starten können.

Sehen Sie sich die Organisationen an, OUs mit denen ein AMI geteilt wird

Sie können die Organisationen finden, OUs mit denen Sie Ihr AMI geteilt haben.

Console

Um zu überprüfen, mit welchen Organisationen und OUs Sie Ihr AMI geteilt haben

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich AMIs aus.
3. Wählen Sie Ihr AMI in der Liste aus, wählen Sie den Tab Permissions und scrollen Sie nach unten zu Shared Organizations/ OUs.

   Informationen darüber AMIs , welche mit Ihnen geteilt wurden, finden Sie unter. Suchen Sie AMIs nach geteilten Dateien zur Verwendung für EC2 Amazon-Instances

AWS CLI

Um zu überprüfen, mit welchen Organisationen und OUs Sie Ihr AMI geteilt haben

Verwenden Sie den Befehl describe-image-attribute mit dem Attribut `launchPermission`.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

Nachfolgend finden Sie eine Beispielantwort.

```
{
    "ImageId": "ami-0abcdef1234567890",
    "LaunchPermissions": [
        {
            "OrganizationalUnitArn": "arn:aws:organizations::111122223333:ou/
o-123example/ou-1234-5example"
        }
    ]
}
```

PowerShell

Um zu überprüfen, mit welchen Organisationen und OUs Sie Ihr AMI geteilt haben

Verwenden Sie das cmdlet Get-EC2ImageAttribute.

```
Get-EC2ImageAttribute `
```

```
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission
```

Ein AMI für eine Organisation oder einer OE freigeben

Sie können ein AMI für eine Organisation oder einer OU freigeben

> **Note**
>
> Sie brauchen die Amazon-EBS-Snapshots, auf die ein AMI verweist, nicht zu teilen, um das AMI zu teilen. Nur das AMI selbst muss freigegeben werden. Das System stellt automatisch Instance-Zugriff auf die referenzierten EBS-Snapshots für den Start bereit. Sie müssen jedoch die KMS-Schlüssel freigeben, die zum Verschlüsseln von Snapshots verwendet werden, auf die das AMI verweist. Weitere Informationen finden Sie unter Erlauben Sie Organisationen und OUs die Verwendung eines KMS-Schlüssels.

Console

So geben Sie ein AMI für eine Organisation oder einer OE frei

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich AMIs aus.
3. Wählen Sie das AMI in der Liste aus und wählen Sie dann Aktionen, AMI-Berechtigungen bearbeiten aus.
4. Unter AMI-Verfügbarkeit wählen Sie Privat aus.
5. Wählen Sie neben Gemeinsam genutzte Organisationen/ die Option OUs ARN hinzufügen organization/OU aus.
6. Geben Sie für Organization/OU ARN (ARN der Organisation/OE) den ARN der Organisation oder OE ein, für den Sie das AMI freigeben möchten, und wählen Sie dann Share AMI (AMI freigeben) aus. Beachten Sie, dass Sie den vollständigen ARN angeben müssen, nicht nur die ID.

   Um dieses AMI mit mehreren Organisationen zu teilen oder wiederholen Sie diesen Schritt OUs, bis Sie alle erforderlichen Organisationen hinzugefügt haben oder OUs.
7. Wählen Sie abschließend Save changes (Änderungen speichern) aus.

8. (Optional) Um die Organisationen anzuzeigen oder OUs mit denen Sie das AMI geteilt haben, wählen Sie das AMI in der Liste aus, klicken Sie auf die Registerkarte Berechtigungen und scrollen Sie nach unten zu Gemeinsam genutzte Organisationen/ OUs. Informationen darüber AMIs , welche mit Ihnen geteilt wurden, finden Sie unter. Suchen Sie AMIs nach geteilten Dateien zur Verwendung für EC2 Amazon-Instances

AWS CLI

So geben Sie ein AMI für eine Organisation frei

Verwenden Sie den Befehl modify-image-attribute, um der angegebenen Organisation Startberechtigungen für das angegebene AMI zu erteilen.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

So geben Sie ein AMI für eine OE frei

Der modify-image-attributeBefehl gewährt der angegebenen Organisationseinheit Startberechtigungen für das angegebene AMI. Beachten Sie, dass Sie den vollständigen ARN angeben müssen, nicht nur die ID.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationalUnitArn=arn:aws:organizations::123456789012:ou/o-123example/
ou-1234-5example}]"
```

PowerShell

Verwenden Sie den Edit-EC2ImageAttributeBefehl (Tools für Windows PowerShell), um ein AMI gemeinsam zu nutzen, wie in den folgenden Beispielen gezeigt.

So geben Sie ein AMI für eine Organisation oder einer OE frei

Der folgende Befehl erteilt der angegebenen Organisation Startberechtigungen für das angegebene AMI.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType add `
    -OrganizationArn "arn:aws:organizations::123456789012:organization/o-123example"
```

So beenden Sie die Freigabe eines AMI für eine Organisation oder OE

Der folgende Befehl entfernt Startberechtigungen für das angegebene AMI von der angegebenen Organisation:

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType remove `
    -OrganizationArn "arn:aws:organizations::123456789012:organization/o-123example"
```

Um die gemeinsame Nutzung eines AMI mit allen Organisationen zu beenden OUs, und AWS-Konten

Der folgende Befehl entfernt alle öffentlichen und expliziten Startberechtigungen vom angegebenen AMI. Hinweis: Der Besitzer des AMI hat immer Startberechtigungen und bleibt daher von dem Befehl unberührt.

```
Reset-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission
```

So beenden Sie die Freigabe eines AMI für eine Organisation oder OU

Sie können die Freigabe eines AMI für eine Organisation oder OU beenden.

> **Note**
>
> Sie können die Freigabe eines AMI für ein bestimmtes Konto nicht beenden, wenn es sich in einer Organisation oder OE befindet, für die ein AMI freigegeben ist. Wenn Sie versuchen, die gemeinsame Nutzung des AMI zu beenden, indem Sie die Startberechtigungen für das Konto entfernen, EC2 gibt Amazon eine Erfolgsmeldung zurück. Das AMI ist jedoch weiterhin für das Konto freigegeben.

Console

So beenden Sie die Freigabe eines AMI für eine Organisation oder OE

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich AMIs aus.
3. Wählen Sie das AMI in der Liste aus und wählen Sie dann Aktionen, AMI-Berechtigungen bearbeiten aus.
4. Wählen Sie unter Gemeinsam genutzte Organisationen/ die Organisationen ausOUs, für die Sie das AMI nicht mehr teilen möchten, und wählen Sie dann Ausgewählte entfernen aus. OUs
5. Wählen Sie abschließend Save changes (Änderungen speichern) aus.
6. (Optional) Um zu bestätigen, dass Sie das AMI nicht mehr mit den Organisationen teilenOUs, oder wählen Sie das AMI in der Liste aus, wählen Sie die Registerkarte Berechtigungen und scrollen Sie nach unten zu Gemeinsam genutzte Organisationen/ OUs.

AWS CLI

So beenden Sie die Freigabe eines AMI für eine Organisation oder OE

Verwenden Sie den Befehl modify-image-attribute. Dieses Beispiel entfernt Startberechtigungen für das angegebene AMI von der angegebenen Organisation.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Remove=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

Um die gemeinsame Nutzung eines AMI mit allen Organisationen zu beenden OUs, und AWS-Konten

Verwenden Sie den Befehl reset-image-attribute. Dieses Beispiel entfernt alle öffentlichen und expliziten Startberechtigungen vom angegebenen AMI. Hinweis: Der Besitzer des AMI hat immer Startberechtigungen und bleibt daher von dem Befehl unberührt.

```
aws ec2 reset-image-attribute \
    --image-id ami-0abcdef1234567890 \
```

```
    --attribute launchPermission
```

PowerShell

So beenden Sie die Freigabe eines AMI für eine Organisation oder OE

Verwenden Sie das cmdlet Edit-EC2ImageAttribute. Dieses Beispiel entfernt Startberechtigungen für das angegebene AMI von der angegebenen Organisation.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType remove `
    -OrganizationArn "arn:aws:organizations::123456789012:organization/o-123example"
```

Um die gemeinsame Nutzung eines AMI mit allen Organisationen zu beenden OUs, und AWS-Konten

Verwenden Sie das cmdlet Reset-EC2ImageAttribute. Dieses Beispiel entfernt alle öffentlichen und expliziten Startberechtigungen vom angegebenen AMI. Hinweis: Der Besitzer des AMI hat immer Startberechtigungen und bleibt daher von dem Befehl unberührt.

```
Reset-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute LaunchPermission
```

Freigeben eines AMI für bestimmte AWS -Konten

Sie können ein AMI mit bestimmten Personen teilen, AWS-Konten ohne das AMI zu veröffentlichen. Alles was Sie brauchen ist die AWS-Konto IDs.

Eine AWS-Konto ID ist eine 12-stellige Zahl`012345678901`, die z. B. eine AWS-Konto eindeutig identifiziert. Weitere Informationen finden Sie unter AWS-Konto -Kennungen anzeigen im Referenzleitfaden für AWS -Kontenverwaltung .

Überlegungen

Beachten Sie beim Teilen AMIs mit bestimmten AWS-Konten Personen Folgendes.

- Eigentümerschaft – Um ein AMI freizugeben, muss Ihr AWS-Konto Besitzer des AMI sein.
- Freigabebeschränkungen — Die maximale Anzahl von Entitäten, für die ein AMI innerhalb einer Region gemeinsam genutzt werden kann, finden Sie in den Amazon EC2 Service-Kontingenten.
- Tags – Sie können keine benutzerdefinierten Tags (Tags, die Sie einem AMI anfügen) freigeben. Wenn Sie ein AMI teilen, sind Ihre benutzerdefinierten Tags für niemanden verfügbar, mit dem AWS-Konto das AMI geteilt wird.
- Snapshots – Sie müssen die Amazon-EBS-Snapshots, auf die ein AMI verweist, nicht freigeben, um das AMI freizugeben. Sie können nur das AMI selbst freigeben. Das System stellt automatisch Instance-Zugriff auf die referenzierten EBS-Snapshots für den Start bereit. Sie müssen jedoch sämtliche KMS-Schlüssel freigeben, die zum Verschlüsseln von Snapshots verwendet werden, auf die ein AMI verweist. Weitere Informationen finden Sie unter Amazon-EBS-Snapshot freigeben im Amazon-EBS-Benutzerhandbuch.
- Verschlüsselung und Schlüssel — Sie können diese Daten teilen AMIs , die durch unverschlüsselte und verschlüsselte Snapshots gesichert sind.
  - Die verschlüsselten Snapshots müssen mit einem KMS-Schlüssel verschlüsselt werden. Sie können keine Dateien teilen AMIs , die auf Snapshots basieren, die mit dem verwalteten AWS Standardschlüssel verschlüsselt wurden.
  - Wenn Sie ein AMI teilen, das von verschlüsselten Snapshots unterstützt wird, müssen Sie zulassen, dass die AWS-Konten KMS-Schlüssel verwendet werden, die zum Verschlüsseln der Snapshots verwendet wurden. Weitere Informationen finden Sie unter Erlauben Sie Organisationen und OUs die Verwendung eines KMS-Schlüssels. Informationen zur Einrichtung der Schlüsselrichtlinie, die Sie zum Starten von Amazon EC2 Auto Scaling Scaling-Instances benötigen, wenn Sie einen vom Kunden verwalteten Schlüssel für die Verschlüsselung verwenden, finden Sie unter Erforderliche AWS KMS key Richtlinie für die Verwendung mit verschlüsselten Volumes im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.
- Region — AMIs sind eine regionale Ressource. Wenn Sie ein AMI freigeben, ist es nur in der entsprechenden Region verfügbar. Um ein AMI in einer anderen Region verfügbar zu machen, kopieren Sie das AMI in die Region und geben Sie es dann frei. Weitere Informationen finden Sie unter Ein EC2 Amazon-AMI kopieren.
- Nutzung: Wenn Sie ein AMI freigeben, können Benutzer Instances nur über das AMI starten. Sie können es nicht löschen, teilen oder ändern. Nachdem sie jedoch eine Instance mit Ihrem AMI gestartet haben, können sie dann ein AMI aus ihrer eigenen Instance erstellen.
- Geteiltes kopieren AMIs — Wenn Benutzer in einem anderen Konto ein gemeinsam genutztes AMI kopieren möchten, müssen Sie ihnen Leseberechtigungen für den Speicher gewähren, der das AMI unterstützt. Weitere Informationen finden Sie unter Kontoübergreifendes Kopieren.

- Abrechnung — Ihnen wird nichts in Rechnung gestellt, wenn Ihr AMI von anderen AWS-Konten zum Starten von Instances verwendet wird. Die Konten, die Instances mit dem AMI starten, werden für die Instances abgerechnet, die sie starten.

Console

Erteilen expliziter Startberechtigungen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich AMIs aus.
3. Wählen Sie das AMI in der Liste aus und wählen Sie dann Aktionen, AMI-Berechtigungen bearbeiten aus.
4. Wählen Sie Private (Privat) aus.
5. Wählen Sie unter Freigegebene Konten die Option Konto-ID hinzufügen aus.
6. Geben Sie unter AWS-Konto ID die AWS-Konto ID ein, mit der Sie das AMI teilen möchten, und wählen Sie dann Share AMI aus.

   Um dieses AMI mit mehreren Konten zu teilen, wiederholen Sie die Schritte 5 und 6, bis Sie alle erforderlichen Konten hinzugefügt haben IDs.
7. Wählen Sie abschließend Änderungen speichern aus.
8. (Optional) Um das zu sehen, AWS-Konto IDs mit dem Sie das AMI geteilt haben, wählen Sie das AMI in der Liste aus und klicken Sie dann auf die Registerkarte Berechtigungen. Informationen darüber AMIs , welche mit Ihnen geteilt wurden, finden Sie unterSuchen Sie AMIs nach geteilten Dateien zur Verwendung für EC2 Amazon-Instances.

AWS CLI

Verwenden Sie den Befehl modify-image-attribute, um ein AMI wie in den folgenden Beispielen gezeigt freizugeben.

Erteilen expliziter Startberechtigungen

Das folgende Beispiel erteilt Startberechtigungen für das angegebene AMI an das angegebene AWS-Konto.

```
aws ec2 modify-image-attribute \
```

```
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{UserId=123456789012}]"
```

Entfernen von Startberechtigungen für ein Konto

Das folgende Beispiel entfernt Startberechtigungen für das angegebene AMI vom angegebenen AWS-Konto.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{UserId=123456789012}]"
```

Entfernen aller Startberechtigungen

Das folgende Beispiel entfernt alle öffentlichen und expliziten Startberechtigungen vom angegebenen AMI. Hinweis: Der Besitzer des AMI hat immer Startberechtigungen und bleibt daher von dem Befehl unberührt.

```
aws ec2 reset-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

PowerShell

Verwenden Sie den Edit-EC2ImageAttributeBefehl (Tools für Windows PowerShell), um ein AMI gemeinsam zu nutzen, wie in den folgenden Beispielen gezeigt.

Erteilen expliziter Startberechtigungen

Das folgende Beispiel erteilt Startberechtigungen für das angegebene AMI an das angegebene AWS-Konto.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission `
    -OperationType add `
    -UserId "123456789012"
```

Entfernen von Startberechtigungen für ein Konto

Das folgende Beispiel entfernt Startberechtigungen für das angegebene AMI vom angegebenen AWS-Konto.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission -OperationType remove `
    -UserId "123456789012"
```

Entfernen aller Startberechtigungen

Das folgende Beispiel entfernt alle öffentlichen und expliziten Startberechtigungen vom angegebenen AMI. Hinweis: Der Besitzer des AMI hat immer Startberechtigungen und bleibt daher von dem Befehl unberührt.

```
Reset-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute launchPermission
```

Kündigen Sie die gemeinsame Nutzung eines AMI mit Ihrem AWS-Konto

Ein Amazon Machine Image (AMI) kann für bestimmte AWS-Konten freigegeben werden, indem die Konten zu den Startberechtigungen des AMI hinzugefügt werden. Wenn ein AMI mit Ihrem geteilt wurde AWS-Konto und Sie nicht mehr möchten, dass es mit Ihrem Konto geteilt wird, können Sie Ihr Konto aus den Startberechtigungen des AMI entfernen. Sie tun dies, indem Sie den `cancel-image-launch-permission` AWS CLI Befehl ausführen. Wenn Sie diesen Befehl ausführen, werden Ihnen AWS-Konto die Startberechtigungen für das angegebene AMI entzogen. Informationen zu den Dateien AMIs , die mit Ihrem geteilt wurden AWS-Konto, finden Sie unterSuchen Sie AMIs nach geteilten Dateien zur Verwendung für EC2 Amazon-Instances.

Sie können beispielsweise die Freigabe eines AMI für Ihr Konto aufheben, um die Wahrscheinlichkeit zu verringern, dass eine Instance mit einem ungenutzten oder veralteten AMI gestartet wird, das für Sie freigegeben wurde. Wenn Sie kündigen, dass ein AMI mit Ihrem Konto geteilt wird, erscheint es nicht mehr in den AMI-Listen in der EC2 Konsole oder in der Ausgabe für Describe-Images.

Themen

- Einschränkungen
- Aufheben der Freigabe eines AMI für Ihr Konto

Einschränkungen

- Sie können Ihr Konto aus den Startberechtigungen eines AMI entfernen, das AWS-Konto nur mit Ihnen geteilt wird. Sie können es nicht verwenden`cancel-image-launch-permission`, um Ihr Konto aus den Startberechtigungen eines AMI zu entfernen, das mit einer Organisation oder Organisationseinheit (OU) geteilt wurde, oder um den Zugriff auf die Öffentlichkeit zu entfernen AMIs.
- Sie können Ihr Konto nicht dauerhaft aus den Startberechtigungen eines AMI entfernen. Ein AMI-Besitzer kann ein AMI wieder mit Ihrem -Konto teilen.
- AMIs sind eine regionale Ressource. Beim Ausführen von `cancel-image-launch-permission` müssen Sie die Region angeben, in der sich das AMI befindet. Geben Sie entweder die Region im Befehl an, oder verwenden Sie die AWS_DEFAULT_REGION Umgebungsvariable.
- Nur das AWS CLI und SDKs unterstützt das Entfernen Ihres Kontos aus den Startberechtigungen eines AMI. Die EC2 Konsole unterstützt diese Aktion derzeit nicht.

Aufheben der Freigabe eines AMI für Ihr Konto

> **Note**
>
> Nachdem Sie die Freigabe eines AMI für Ihr Konto aufgehoben haben, können Sie dies nicht mehr rückgängig machen.. Um wieder Zugriff auf das AMI zu erhalten, muss der AMI-Besitzer es für Ihr Konto freigeben.

AWS CLI

So heben Sie die Freigabe eines AMI für Ihr Konto auf

Verwenden Sie den Befehl cancel-image-launch-permission.

```
aws ec2 cancel-image-launch-permission \
    --image-id ami-0abcdef1234567890 \
    --region us-east-1
```

PowerShell

So heben Sie die Freigabe eines AMI für Ihr Konto auf

Verwenden Sie das cmdlet Stop-EC2ImageLaunchPermission.

```
Stop-EC2ImageLaunchPermission `
    -ImageId ami-0abcdef1234567890 `
    -Region us-east-1
```

Empfehlungen für die Erstellung von gemeinsam genutztem Linux AMIs

Verwenden Sie die folgenden Richtlinien, um die Angriffsfläche zu reduzieren und die Zuverlässigkeit der von AMIs Ihnen erstellten Dateien zu verbessern.

> **Important**
>
> Die Liste der Sicherheitsrichtlinien kann sehr umfassend sein. Erstellen Sie Ihre geteilten Daten AMIs sorgfältig und nehmen Sie sich Zeit, um zu überlegen, wo Sie sensible Daten preisgeben könnten.

Inhalt

- Deaktivieren von passwortbasierten Fernanmeldungen für den Stammbenutzer
- Deaktivieren des lokalen Root-Zugriffs
- Entfernen von SSH-Host-Schlüsselpaaren
- Installieren von Anmeldeinformationen für öffentliche Schlüssel
- SSHD-DNS-Prüfungen deaktivieren (optional)
- Sensible Daten entfernen

Wenn Sie AMIs dafür bauen AWS Marketplace, finden Sie AMIs im AWS Marketplace Verkäuferleitfaden unter Bewährte Methoden für das Bauen Richtlinien, Richtlinien und bewährte Methoden.

Deaktivieren von passwortbasierten Fernanmeldungen für den Stammbenutzer

Die Verwendung fester Root-Passwörter für öffentliche AMIs ist ein Sicherheitsrisiko, das schnell bekannt werden kann. Wenn die Benutzer bei der ersten Anmeldung zum Ändern des Passworts aufgefordert werden, bietet sich hierbei eine potenzielle Möglichkeit des Missbrauchs.

Um das Problem zu beheben, deaktivieren Sie die Passwort-basierte Remoteanmeldung für den Root-Benutzer.

Deaktivieren von passwortbasierten Fernanmeldungen für den Stammbenutzer

1. Öffnen Sie die Datei `/etc/ssh/sshd_config` in einem Textbearbeitungsprogramm und suchen Sie nach folgender Zeile:

   ```
   #PermitRootLogin yes
   ```

2. Ändern Sie die Zeile folgendermaßen:

   ```
   PermitRootLogin without-password
   ```

   Der Speicherort dieser Konfigurationsdatei weicht von Ihrer Verteilung ggf. ab. Das ist auch der Fall, wenn Sie nicht OpenSSH verwenden. Ist dies der Fall, schlagen Sie in der entsprechenden Dokumentation nach.

Deaktivieren des lokalen Root-Zugriffs

Wenn Sie mit Shared arbeiten AMIs, ist es eine bewährte Methode, direkte Root-Logins zu deaktivieren. Melden Sie sich hierfür in der ausgeführten Instance an und geben Sie den folgenden Befehl aus:

```
[ec2-user ~]$ sudo passwd -l root
```

> **Note**
>
> Der Befehl beeinträchtigt nicht die Verwendung von `sudo`.

Entfernen von SSH-Host-Schlüsselpaaren

Wenn Sie ein von einem öffentlichen AMI abgeleitetes AMI teilen möchten, entfernen Sie die bestehenden SSH-Host-Schlüsselpaare in `/etc/ssh`. Dadurch wird SSH gezwungen, neue eindeutige SSH-Schlüsselpaare zu generieren, wenn jemand eine Instance mit Ihrem AMI startet, wodurch die Sicherheit verbessert und die Wahrscheinlichkeit von "man-in-the-middle" -Angriffen verringert wird.

Entfernen Sie die folgenden Schlüsseldateien aus Ihrem System.

- ssh_host_dsa_key

- ssh_host_dsa_key.pub
- ssh_host_key
- ssh_host_key.pub
- ssh_host_rsa_key
- ssh_host_rsa_key.pub
- ssh_host_ecdsa_key
- ssh_host_ecdsa_key.pub
- ssh_host_ed25519_key
- ssh_host_ed25519_key.pub

Sie können all diese Dateien mit folgendem Befehl sicher entfernen.

```
[ec2-user ~]$ sudo shred -u /etc/ssh/*_key /etc/ssh/*_key.pub
```

Warning

Hilfsprogramme zum sicheren Entfernen wie shred entfernen möglicherweise nicht alle Kopien einer Datei vom Speichermedium. Journaling-Dateisysteme (u. a. Amazon Linux default ext4), Snapshots, Sicherungen, RAID und temporäres Caching erstellen möglicherweise versteckte Kopien von Dateien. Weitere Informationen finden Sie in der shred-Dokumentation.

Important

Wenn Sie die bestehenden SSH-Host-Schlüsselpaare nicht aus dem öffentlichen AMI entfernen, benachrichtigt unser routinemäßiger Prüfprozess Sie und alle Kunden, die Instances des AMI ausführen, über potenzielle Sicherheitsrisiken. Nach einer kurzen Übergangsfrist wird das AMI als privat markiert.

Installieren von Anmeldeinformationen für öffentliche Schlüssel

Wenn Sie das AMI so konfigurieren, dass keine Passwortanmeldung möglich ist, müssen Sie eine anderen Anmeldemethode für die Benutzer bereitstellen.

Amazon EC2 ermöglicht es Benutzern, beim Starten einer Instance einen Namen für ein öffentlich-privates key pair anzugeben. Wenn ein gültiger Schlüsselpaarname für den `RunInstances` API-Aufruf (oder über die Befehlszeilen-API-Tools) bereitgestellt wird, wird der öffentliche Schlüssel (der Teil des key pair, den Amazon nach einem Aufruf von `CreateKeyPair` oder auf dem Server EC2 aufbewahrt`ImportKeyPair`) der Instance durch eine HTTP-Abfrage der Instance-Metadaten zur Verfügung gestellt.

Wenn Sie sich via SSH anmelden möchten, muss das AMI den Schlüsselwert beim Starten abrufen und `/root/.ssh/authorized_keys` (oder der entsprechenden Datei für das entsprechende Benutzerkonto im AMI) anhängen. Benutzer können Instances des AMI mit einem Schlüsselpaar starten und sich ohne Root-Passwort anmelden.

Viele Verteilungen, u. a. Amazon Linux und Ubuntu, verwenden das `cloud-init`-Paket zum Einfügen von Anmeldeinformationen für öffentliche Schlüssel für einen konfigurierten Benutzer. Wenn die Verteilung `cloud-init` nicht unterstützt, fügen Sie dem System-Startup-Skript (z. B. `/etc/rc.local`) den folgenden Code hinzu, um den öffentlichen Schlüssel abzurufen, den Sie beim Start für den Root-Benutzer angegeben haben.

> **Note**
>
> Im folgenden Beispiel ist die IP-Adresse http://169.254.169.254/ eine lokale (link-local) Adresse und nur von der Instance aus gültig.

IMDSv2

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

IMDSv1

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

Dies kann auf jeden Benutzer angewendet werden. Sie müssen es nicht auf den `root`-Benutzer beschränken.

> **Note**
>
> Beim erneuten Bündeln einer Instance basierend auf dem AMI wird der Schlüssel eingebunden, mit dem es gestartet wurde. Damit der Schlüssel nicht eingebunden wird, löschen (oder entfernen) Sie die `authorized_keys`-Datei oder schließen Sie diese Datei vom erneuten Bündeln aus.

SSHD-DNS-Prüfungen deaktivieren (optional)

Durch das Deaktivieren von sshd-DNS-Prüfungen wird die sshd-Sicherheit beeinträchtigt. Wenn bei der DNS-Auflösung allerdings ein Fehler auftritt, funktioniert die SSH-Anmeldung weiterhin. Wenn Sie die sshd-Prüfungen nicht deaktivieren, wird die Anmeldung durch Fehler bei der DNS-Auflösung verhindert.

Deaktivieren von sshd-DNS-Prüfungen

1. Öffnen Sie die Datei `/etc/ssh/sshd_config` in einem Textbearbeitungsprogramm und suchen Sie nach folgender Zeile:

   ```
   #UseDNS yes
   ```

2. Ändern Sie die Zeile folgendermaßen:

```
UseDNS no
```

> **Note**
>
> Der Speicherort dieser Konfigurationsdatei kann von Ihrer Verteilung abweichen. Das ist auch der Fall, wenn Sie nicht OpenSSH verwenden. Ist dies der Fall, schlagen Sie in der entsprechenden Dokumentation nach.

Sensible Daten entfernen

Wir empfehlen, keine empfindlichen Daten oder empfindliche Software auf AMIs zu speichern, die Sie teilen. Benutzer, die ein gemeinsames AMI starten, könnten es erneut bündeln und als ihr eigenes registrieren. Gehen Sie folgendermaßen vor, um keine Sicherheitsrisiken zu übersehen:

- Wir empfehlen, die `--exclude` *`directory`*-Option für `ec2-bundle-vol` zu verwenden, um die Verzeichnisse und Unterverzeichnisse zu überspringen, die geheime Informationen enthalten. Schließen Sie insbesondere alle benutzereigenen public/private SSH-Schlüsselpaare und `authorized_keys` SSH-Dateien aus, wenn Sie das Image bündeln. Amazon Public AMIs speichert diese `/root/.ssh` für den Root-Benutzer und `/home/`*`user_name`*`/.ssh/` für normale Benutzer. Weitere Informationen finden Sie unter ec2-bundle-vol.
- Löschen Sie vor dem Bündeln immer den Shell-Verlauf. Wenn Sie versuchen, mehr als einen Bundle-Upload im selben AMI durchzuführen, enthält der Shell-Verlauf Ihren Zugriffsschlüssel. Das folgende Beispiel muss der letzte ausgeführte Befehl vor dem Bündeln in einer Instance sein.

```
[ec2-user ~]$ shred -u ~/.*history
```

> **Warning**
>
> Die in der Warnung oben beschriebenen Einschränkungen von shred gelten auch hier. Hinweis: Bash schreibt den Verlauf der aktuellen Sitzung beim Beenden auf den Datenträger. Wenn Sie sich nach dem Löschen von `~/.bash_history` von der Instance ab- und anschließend wieder anmelden, werden Sie feststellen, dass die `~/.bash_history`-Datei neu erstellt wurde und alle Befehle enthält, die während der vorherigen Sitzung ausgeführt wurden.

Neben Bash schreiben auch andere Programme Verlaufsdaten auf den Datenträger. Seien Sie vorsichtig und entfernen Sie unnötige DOT-Dateien und -Verzeichnisse.

- Zum Bündeln einer ausgeführten Instance sind Ihr privater Schlüssel und das X.509-Zertifikat erforderlich. Legen Sie diese Daten und anderen Anmeldeinformationen an einem Speicherort ab, der nicht gebündelt wird (z. B. den Instance-Speicher).

Überwachen Sie AMI-Ereignisse mit Amazon EventBridge

Wenn sich der Status eines Amazon Machine Image (AMI) ändert, EC2 generiert Amazon ein Ereignis, das an Amazon gesendet wird EventBridge (früher bekannt als Amazon CloudWatch Events). Die Ereignisse werden im JSON-Format an den EventBridge Standard-Event-Bus gesendet. Sie können Amazon verwenden EventBridge , um diese Ereignisse zu erkennen und darauf zu reagieren. Sie tun dies, indem Sie Regeln erstellen EventBridge , die als Reaktion auf ein Ereignis eine Aktion auslösen. Sie können beispielsweise eine EventBridge Regel erstellen, die erkennt, wann der AMI-Erstellungsprozess abgeschlossen ist, und dann ein Amazon SNS SNS-Thema aufruft, um Ihnen eine E-Mail-Benachrichtigung zu senden.

Amazon EC2 generiert ein `EC2 AMI State Change` Ereignis, wenn ein AMI in einen der folgenden Zustände eintritt:

- `available`
- `failed`
- `deregistered`
- `disabled`

Ereignisse werden auf bestmögliche Weise ausgegeben.

In der folgenden Tabelle sind die AMI-Vorgänge und die Zustände aufgeführt, in die ein AMI übergehen kann. In der Tabelle gibt Ja die Zustände an, in die das AMI übergehen kann, wenn der entsprechende Vorgang ausgeführt wird.

AMI-Vorgänge	available	failed	deregistered	disabled
CopyImage	Ja	Ja		
CreateImage	Ja	Ja		

AMI-Vorgänge	available	failed	deregistered	disabled
CreateRestoreImageTask	Ja	Ja		
DeregisterImage			Ja	
DisableImage				Ja
EnableImage	Ja			
RegisterImage	Ja	Ja		

EC2 AMI State Change-Ereignisse

- Ereignisdetails
- available-Ereignisse
- failed-Ereignisse
- deregistered-Ereignisse
- disabled-Ereignisse

Ereignisdetails

Die folgenden Felder des Ereignisses können verwendet werden, um Regeln zu erstellen, die eine Aktion auslösen:

`"source": "aws.ec2"`

Identifiziert, dass das Ereignis von Amazon stammt EC2.

`"detail-type": "EC2 AMI State Change"`

Identifiziert den Ereignisnamen.

`"detail": { "ImageId": "ami-0abcdef1234567890", "State": "available", }`

Stellt die AMI-ID und den Status des AMI (`available`, `failed`, `deregistered` oder `disabled`) bereit.

Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch:

- EventBridge Amazon-Veranstaltungen
- EventBridge Amazon-Ereignismuster
- EventBridge Amazon-Regeln

Ein Tutorial zum Erstellen einer Lambda-Funktion und einer EventBridge Regel, die die Lambda-Funktion ausführt, finden Sie unter Tutorial: Den Status einer EC2 Amazon-Instance mithilfe protokollieren EventBridge im AWS Lambda Developer Guide.

available-Ereignisse

Das Folgende ist ein Beispiel für ein Ereignis, das Amazon EC2 generiert, wenn das AMI nach einem erfolgreichen `EnableImage` Vorgang`CreateImage`,, `CopyImage` `RegisterImage``CreateRestoreImageTask`, oder in den `available` Status wechselt.

`"State": "available"` zeigt an, dass der Vorgang erfolgreich war.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0abcdef1234567890"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0abcdef1234567890",
        "State": "available",
        "ErrorMessage": ""
    }
}
```

failed-Ereignisse

Das Folgende ist ein Beispiel für ein Ereignis, das Amazon EC2 generiert, wenn das AMI nach einem fehlgeschlagenen`CreateImage`, `CopyImage``RegisterImage`, oder `CreateRestoreImageTask` Vorgang in den `failed` Status wechselt.

Die folgenden Felder enthalten relevante Informationen:

- `"State": "failed"` – Gibt an, dass ein Vorgang fehlgeschlagen ist.
- `"ErrorMessage": ""` – Gibt den Grund für den fehlgeschlagenen Vorgang an.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0abcdef1234567890"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0abcdef1234567890",
        "State": "failed",
        "ErrorMessage": "Description of failure"
    }
}
```

deregistered-Ereignisse

Das Folgende ist ein Beispiel für ein Ereignis, das Amazon EC2 generiert, wenn das AMI nach einem erfolgreichen `DeregisterImage` Vorgang in den `deregistered` Status wechselt. Wenn der Vorgang fehlschlägt, wird kein Ereignis generiert. Jeder Fehler ist sofort bekannt, da `DeregisterImage` ein synchroner Vorgang ist.

`"State": "deregistered"` zeigt an, dass der `DeregisterImage`-Vorgang erfolgreich war.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0abcdef1234567890"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0abcdef1234567890",
```

```
        "State": "deregistered",
        "ErrorMessage": ""
    }
}
```

disabled-Ereignisse

Das Folgende ist ein Beispiel für ein Ereignis, das Amazon EC2 generiert, wenn das AMI nach einem erfolgreichen `DisableImage` Vorgang in den `disabled` Status wechselt. Wenn der Vorgang fehlschlägt, wird kein Ereignis generiert. Jeder Fehler ist sofort bekannt, da `DisableImage` ein synchroner Vorgang ist.

`"State": "disabled"` zeigt an, dass der `DisableImage`-Vorgang erfolgreich war.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0abcdef1234567890"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0abcdef1234567890",
        "State": "disabled",
        "ErrorMessage": ""
    }
}
```

Verstehen von AMI-Fakturierungsdaten

Beim Start Ihrer Instances stehen viele Amazon Machine Images (AMIs) zur Auswahl, und sie unterstützen eine Vielzahl von Betriebssystemplattformen und -features. Um zu verstehen, wie sich das AMI, das Sie beim Start Ihrer Instance auswählen, auf das Endergebnis Ihrer AWS-Rechnung wirkt, können Sie die zugehörige Betriebssystemplattform und die Fakturierungsdaten untersuchen. Tun Sie dies, bevor Sie On-Demand oder Spot-Instances starten oder Reserved Instance kaufen.

Hier sind zwei Beispiele dafür, wie die Untersuchung Ihres AMI im Voraus bei der Auswahl des AMI helfen kann, das Ihren Anforderungen am besten entspricht:

- Für Spot-Instances können Sie anhand der AMI-Plattformdetails bestätigen, dass das AMI für Spot-Instances unterstützt wird.
- Beim Kauf eines Reserved Instance können Sie sicherstellen, dass Sie die Betriebssystemplattform (Plattform) auswählen, die den AMI-Plattformdetails zugeordnet ist.

Weitere Informationen zu den Preisen für Instances erhalten Sie unter Amazon EC2 – Preise.

Inhalt

- Felder für AMI-Fakturierungsdaten
- Informationen zur AMI-Fakturierung und Verwendung finden
- Überprüfen Sie die AMI-Gebühren auf Ihrer Rechnung

Felder für AMI-Fakturierungsdaten

Die folgenden Felder enthalten Fakturierungsdaten, die einem AMI zugeordnet sind:

Plattformdetails

Die Plattformdetails, die mit dem Fakturierungscode des AMI verknüpft sind. Beispiel, `Red Hat Enterprise Linux`.

Verwendungsvorgang

Der Betrieb der Amazon-EC2-Instance und der mit dem AMI verknüpfte Abrechnungscode. Beispiel, `RunInstances:0010`. Usage operation (Verwendungsvorgang) entspricht der Spalte lineitem/Operation in Ihrem AWS-Kosten- und Nutzungsbericht und in der AWS-Preislisten-API.

Sie können diese Felder auf der Seite Instances oder AMIs in der Amazon-EC2-Konsole anzeigen, oder in der Antwort, die vom Befehl describe-images oder Get-EC2Image zurückgegeben wird.

Beispieldaten: Verwendungsvorgang nach Plattform

In der folgenden Tabelle sind einige der Werte für Plattformdetails und Nutzungsvorgänge aufgeführt, die auf der Seite Instances oder AMIs in der Amazon-EC2-Konsole oder in der Antwort angezeigt werden können, die vom Befehl describe-images oder Get-EC2Image zurückgegeben wird.

Plattformdetails	Verwendungsvorgang [2]

Plattformdetails	Verwendungsvorgang [2]
Linux/UNIX	RunInstances
Red Hat BYOL Linux	RunInstances:00g0 [3]
Red Hat Enterprise Linux	RunInstances:0010
Red Hat Enterprise Linux with HA	RunInstances:1010
Red Hat Enterprise Linux with SQL Server Standard and HA	RunInstances:1014
Red Hat Enterprise Linux with SQL Server Enterprise and HA	RunInstances:1110
Red Hat Enterprise Linux with SQL Server Standard	RunInstances:0014
Red Hat Enterprise Linux with SQL Server Web	RunInstances:0210
Red Hat Enterprise Linux with SQL Server Enterprise	RunInstances:0110
SQL Server Enterprise	RunInstances:0100
SQL Server Standard	RunInstances:0004
SQL Server Web	RunInstances:0200
SUSE Linux	RunInstances:000g
Ubuntu Pro	RunInstances:0g00
Windows	RunInstances:0002

Plattformdetails	Verwendungsvorgang [2]
Windows BYOL	RunInstances:0800
Windows with SQL Server Enterprise [1]	RunInstances:0102
Windows with SQL Server Standard [1]	RunInstances:0006
Windows with SQL Server Web [1]	RunInstances:0202

[1] Wenn zwei Softwarelizenzen mit einem AMI verknüpft sind, werden im Feld Plattformdetails beide angezeigt.

[2] Wenn Sie Spot Instances ausführen, kann der lineitem/Operation in Ihrem AWS-Kosten- und Nutzungsbericht von dem hier aufgeführten Wert für Verwendungsvorgang abweichen. Wenn `lineitem/Operation` beispielsweise `RunInstances:0010:SV006` anzeigt, bedeutet dies, dass Amazon EC2 eine Stunde Red Hat Enterprise Linux Spot Instance in der Region USA Ost (Nord-Virginia) in der VPC-Zone 6 ausführt.

[3] Dies wird wie RunInstances (Linux/UNIX) in Ihren Nutzungsberichten angezeigt.

Informationen zur AMI-Fakturierung und Verwendung finden

Die folgenden Eigenschaften können Ihnen helfen, AMI-Gebühren auf Ihrer Rechnung zu überprüfen:

- Plattformdetails
- Verwendungsvorgang
- AMI-ID

Console

So suchen Sie AMI-Fakturierungsdaten für ein AMI

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.

3. Wählen Sie das AMI aus.
4. Suchen Sie auf der Registerkarte Details die Optionen Plattformdetails und Nutzungsvorgang.

So suchen Sie AMI-Fakturierungsdaten für eine Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.
4. Erweitern Sie auf der Registerkarte Details die Instance-Details und suchen Sie nach Plattformdetails und Nutzungsvorgang.

AWS CLI

So suchen Sie AMI-Fakturierungsdaten für ein AMI

Verwenden Sie den Befehl describe-images.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query "Images[].
{PlatformDetails:PlatformDetails,UsageOperation:UsageOperation}"
```

Nachstehend finden Sie eine Beispielausgabe für ein Linux-AMI.

```
[
    {
        "PlatformDetails": "Linux/UNIX",
        "UsageOperation": "RunInstances"
    }
]
```

So suchen Sie AMI-Fakturierungsdaten für eine Instance

Verwenden Sie den Befehl describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[].Instances[].
{PlatformDetails:PlatformDetails,UsageOperation:UsageOperation}"
```

Nachstehend finden Sie eine Beispielausgabe für eine Windows-Instance.

```
[
    {
        "PlatformDetails": "Windows",
        "UsageOperation": "RunInstances:0002"
    }
]
```

PowerShell

So suchen Sie AMI-Fakturierungsdaten für ein AMI

Verwenden Sie das cmdlet Get-EC2Image.

```
Get-EC2Image `
    -ImageId ami-0abcdef1234567890 | `
    Format-List PlatformDetails, UsageOperation
```

Nachstehend finden Sie eine Beispielausgabe für ein Linux-AMI.

```
PlatformDetails : Linux/UNIX
UsageOperation  : RunInstances
```

So suchen Sie AMI-Fakturierungsdaten für eine Instance

Verwenden Sie das cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances | `
    Format-List PlatformDetails, UsageOperation
```

Nachstehend finden Sie eine Beispielausgabe für eine Windows-Instance.

```
PlatformDetails : Windows
UsageOperation  : RunInstances:0002
```

Überprüfen Sie die AMI-Gebühren auf Ihrer Rechnung

Um sicherzustellen, dass Sie keine ungeplanten Kosten anfallen, können Sie bestätigen, dass die Fakturierungsdaten für eine Instance in Ihrem AWS-Kosten- und Nutzungsbericht mit den Fakturierungsdaten übereinstimmen, die mit dem AMI verknüpft sind, mit dem Sie die Instance gestartet haben.

Um die Fakturierungsdaten zu bestätigen, suchen Sie die Instance-ID in Ihrem CUR und überprüfen Sie den entsprechenden Wert in der Spalte `lineitem/Operation`. Der Wert sollte mit dem Wert für Usage operation (Verwendungsvorgang) übereinstimmen, der dem AMI zugeordnet ist.

Zum Beispiel hat das AMI `ami-0123456789EXAMPLE` die folgenden Fakturierungsdaten:

- Plattformdetails = `Red Hat Enterprise Linux`
- Verwendungsvorgang = `RunInstances:0010`

Wenn Sie eine Instance mit diesem AMI gestartet haben, können Sie die Instance-ID in Ihrem CUR finden und den entsprechenden Wert in der Spalte `lineitem/Operation` überprüfen. In diesem Beispiel sollte der Wert sei `RunInstances:0010`.

AMI-Kontingente in Amazon EC2

Die folgenden Kontingente gelten für das Erstellen und Freigeben von AMIs. Die Kontingente gelten pro AWS-Region.

Kontingentname	Beschreibung	Standardkontingent pro Region
AMIs	Die maximal zulässige Anzahl öffentlicher und privater AMIs pro Region. Dazu gehören verfügbare, ausstehende und deaktivierte AMIs sowie AMIs im Papierkorb.	50 000
Öffentliche AMIs	Die maximal zulässige Anzahl öffentlicher AMIs, einschlie	5

Kontingentname	Beschreibung	Standardkontingent pro Region
	ßlich öffentlicher AMIs im Papierkorb, pro Region.	
Freigeben von AMIs	Die maximale Anzahl von Entitäten (Organisationen, Organisationseinheiten (OUs) und Konten), mit denen ein AMI in einer Region gemeinsam genutzt werden kann. Beachten Sie, dass bei Freigabe eines AMI für eine Organisation oder Organisat ionseinheit die Anzahl der Konten in der Organisation oder Organisationseinhe it nicht auf das Kontingent angerechnet wird.	1.000

Wenn Sie Ihre Kontingente überschreiten und weitere AMIs erstellen oder freigeben möchten, können Sie Folgendes tun:

- Wenn Sie Ihr Gesamtkontingent an AMIs oder öffentlichen AMIs überschreiten, sollten Sie erwägen, nicht verwendete Images abzumelden.
- Wenn Sie Ihr Kontingent an öffentlichen AMIs überschreiten, sollten Sie eine oder mehrere öffentliche AMIs als privat einstufen.
- Wenn Sie Ihr AMI-Freigabekontingent überschreiten, sollten Sie erwägen, Ihre AMIs für eine Organisation oder Organisationseinheit anstelle von separaten Konten freizugeben.
- Beantragen Sie eine Kontingenterhöhung für AMIs.

Beantragung einer Kontingenterhöhung für AMIs

Wenn Sie mehr als das standardmäßige Kontingent für AMIs benötigen, können Sie eine Kontingenterhöhung beantragen.

So beantragen Sie eine Kontingenterhöhung für AMIs

1. Öffnen Sie die Service-Quotas-Konsole unter https://console.aws.amazon.com/servicequotas/.
2. Wählen Sie im Navigationsbereich AWS-Services.
3. Wählen Sie Amazon Elastic Compute Cloud (Amazon EC2) aus der Liste aus oder geben Sie den Namen des Service in das Suchfeld ein.
4. Wählen Sie das AMI-Kontingent, um eine Erhöhung zu beantragen. Sie können folgende AMI-Kontingente auswählen:

   - AMIs
   - Öffentliche AMIs
   - Freigeben von AMIs
5. Wählen Sie Kontingenterhöhung anfordern.
6. Geben Sie unter Change quota value (Kontingentwert ändern) den neuen Kontingentwert ein und wählen Sie dann Request (Anforderung) aus.

Um ausstehende oder kürzlich genehmigte Anfragen anzuzeigen, wählen Sie im Navigationsbereich die Option Dashboard . Wählen Sie für ausstehende Anfragen den Status der Anfrage, um die Anfrage zu öffnen. Der Anfangsstatus einer Anfrage ist Pending (Ausstehend). Nachdem sich der Status in Quota requested (Kontingent beantragt) geändert hat, wird Ihnen die Fallnummer unter Support Center case number (Support-Center-Fallnummer) angezeigt. Wählen Sie die Fallnummer, um das Ticket für Ihre Anfrage zu öffnen.

Nachdem die Anfrage genehmigt wurde, wird Applied quota value (Angewandter Kontingentwert) für das Kontingent auf den neuen Wert eingestellt.

Weitere Informationen zu diesem Service finden Sie im Benutzerhandbuch für Service Quotas.

Amazon EC2-Instances

Eine Amazon-EC2-Instance ist ein virtueller Server in der AWS Cloud. Sie haben die volle Kontrolle über Ihre Instance, und zwar von dem Zeitpunkt an, an dem Sie sie zum ersten Mal starten (als Starten einer Instance bezeichnet), bis Sie sie löschen (das als Beenden einer Instance bezeichnet). Sie können beim Start Ihrer Instance aus einer Vielzahl von Betriebssystemen auswählen. Sie können eine Verbindung mit Ihrer Instance herstellen und sie für Ihre Anforderungen anpassen. Sie können beispielsweise das Betriebssystem konfigurieren, Betriebssystem-Updates installieren und Anwendungen auf Ihrer Instance installieren.

Amazon EC2 bietet eine breite Auswahl an Instance-Typen. Sie können einen Instance-Typ auswählen, der die Anforderungen Ihrer Anwendungen an Rechenleistung, Arbeitsspeicher, Speicher und Netzwerkleistung erfüllt.

Mit Amazon EC2 zahlen Sie nur das, was Sie tatsächlich nutzen. Die Abrechnung für Ihre Instance beginnt, wenn Sie Ihre Instance starten, und sie in den Status „Wird ausgeführt“ wechselt. Die Abrechnung endet, wenn Sie Ihre Instance beenden, und wird wieder aufgenommen, wenn Sie Ihre Instance starten. Wenn Sie Ihre Instance beenden, wird die Abrechnung beendet, wenn sie in den Status „Herunterfahren“ übergeht.

Amazon EC2 bietet Feature, die Sie zur Optimierung der Leistung und Kosten Ihrer Instances verwenden können. Sie können beispielsweise Amazon-EC2-Flotte oder Amazon EC2 Auto Scaling verwenden, um Ihre Kapazität zu erhöhen oder zu verringern, wenn sich Ihre Instance-Nutzung ändert. Sie können die Kosten für Ihre Instances mithilfe von Spot Instances oder Savings Plans reduzieren.

Eine verwaltete Instance wird von einem Serviceanbieter wie Amazon EKS Auto Mode verwaltet. Sie können die Einstellungen einer verwalteten Instance nicht direkt ändern. Verwaltete Instances werden durch den Wert Wahr im Feld Verwaltet identifiziert. Weitere Informationen finden Sie unter Verwaltete Amazon-EC2-Instances.

Feature und Aufgaben

- EC2 Amazon-Instance-Typen
- Verwaltete Amazon-EC2-Instances
- EC2 Abrechnungs- und Kaufoptionen von Amazon
- Instance-Startparameter in EC2 Amazon-Startvorlagen speichern

- Starten Sie eine EC2 Amazon-Instance
- Connect zu Ihrer EC2 Instance her
- Amazon-EC2-Instance-Statusänderungen
- Automatische Instance-Wiederherstellung
- Verwenden Sie Instanz-Metadaten, um Ihre EC2 Instanz zu verwalten
- Ermitteln, ob es sich bei einem Host um eine EC2-Instance handelt
- Instance-Identitätsdokumente für Amazon-EC2-Instances
- STIG-Compliance für Ihre EC2-Instance
- Präzise Uhr- und Zeitsynchronisierung auf Ihrer EC2-Instance
- EC2 Capacity Manager
- Gerätetreiber für Ihre EC2 Instanz verwalten
- Ihre Amazon-EC2-Instance konfigurieren
- EC2–Windows-Instance auf eine neuere Version von Windows Server aktualisieren
- Tutorial: Verbinden einer Amazon-EC2-Instance mit einer Amazon-RDS-Datenbank

EC2 Amazon-Instance-Typen

Wenn Sie eine Instance starten, bestimmt der von Ihnen angegebene Instance-Typ die Hardware der Host-Computer für die Instance. Jeder Instance-Typ bietet unterschiedliche Rechenleistung, Arbeitsspeicher- und Speicher-Kapazität und wird abhängig von diesen Eigenschaften in Instance-Familien eingeordnet. Wählen Sie einen Instance-Typ den Anforderungen der Anwendung oder Software entsprechend aus, die Sie in Ihrer Instance ausführen möchten. Weitere Informationen zu Funktionen und Anwendungsfällen finden Sie unter EC2 Amazon-Instanztypen.

Amazon EC2 weist einige Ressourcen des Host-Computers, wie CPU, Arbeitsspeicher und Instance-Speicher, einer bestimmten Instance zu. Amazon EC2 teilt andere Ressourcen des Host-Computers, wie das Netzwerk und das Festplattensubsystem, zwischen den Instances. Wenn die Instances eines Host-Computers jeweils möglichst viele Ressourcen nutzen möchten, wird die Ressource gleichmäßig aufgeteilt. Wenn eine Ressource jedoch nicht voll ausgelastet ist, kann eine Instance einen höheren Anteil der verfügbaren Ressource nutzen.

Jeder Instance-Typ stellt Leistung von einer gemeinsamen Ressource je nach Anforderung bereit. Beispielsweise weisen Instance-Typen mit hoher I/O Leistung eine größere Anzahl gemeinsam genutzter Ressourcen auf. Durch die Zuweisung eines größeren Anteils gemeinsam genutzter

Ressourcen wird auch die Varianz der I/O Leistung verringert. Für die meisten Anwendungen ist eine moderate I/O Leistung mehr als ausreichend. Für Anwendungen, die eine höhere oder konsistentere I/O Leistung erfordern, sollten Sie jedoch einen Instance-Typ mit höherer I/O Leistung in Betracht ziehen.

Inhalt

- Verfügbare Instance-Typen
- Hardwarespezifikationen
- Hypervisor-typ
- AMI-Virtualisierungstypen
- Prozessoren
- Suchen eines Amazon EC2-Instance-Typs
- Holen Sie sich Empfehlungen vom EC2-Instance-Typ-Finder
- EC2-Instance-Empfehlungen von Compute Optimizer abrufen
- Änderungen des EC2 Amazon-Instanztyps
- Burstable Performance Instances
- Leistungsbeschleunigung mit GPU-Instances
- Amazon EC2 Mac-Instanzen
- Für Amazon EBS optimierte Instance-Typen
- CPU-Optionen für EC2 Amazon-Instances
- AMD SEV-SNP für Amazon-EC2-Instances
- Kontrolle des Prozessorstatus für Amazon EC2 Linux-Instances

Verfügbare Instance-Typen

Amazon EC2 bietet eine große Auswahl an Instance-Typen, die für unterschiedliche Anwendungsfälle optimiert sind. Die Instance-Typen umfassen unterschiedliche Kombinationen von CPU-, Arbeitsspeicher-, Speicher- und Netzwerkkapazitäten und geben Ihnen die nötige Flexibilität, um die richtige Mischung von Ressourcen für Ihre Anwendungen zu wählen. Jeder Instance-Typ umfasst eine oder mehrere Instance-Größen, so dass Sie Ihre Ressourcen an die Anforderungen Ihrer Ziel-Workloads anpassen können.

Namenskonvention für Instance-Typen

Die Namen basieren auf der Instance-Familie, der Generation, der Prozessorfamilie, den Fähigkeiten und der Größe. Weitere Informationen finden Sie unter Namenskonventionen im Amazon EC2 Instance Types Guide.

Suchen eines -Instance-Typs

Informationen darüber, welche Instance-Typen Ihren Anforderungen entsprechen, wie z. B. unterstützte Regionen, Rechenressourcen oder Speicherressourcen, finden Sie unter Suchen eines Amazon EC2-Instance-Typs und die Spezifikationen für EC2 Amazon-Instance-Typen im Amazon EC2 Instance Types Guide.

Hardwarespezifikationen

Detaillierte Spezifikationen für Instance-Typen finden Sie unter Spezifikationen im Amazon EC2 Instance Types Guide. Preisinformationen finden Sie unter Amazon EC2 On-Demand-Preise.

Um die richtigen Instance-Typen für Ihre Anforderungen zu bestimmen, empfehlen wir, eine Instance zu starten und Ihre eigene Benchmarkanwendung zu verwenden. Da Instances pro Sekunde abgerechnet werden, können Sie mehrere Instance-Typen bequem und ohne großen Kostenaufwand testen, bevor Sie eine Entscheidung treffen. Falls sich Ihre Anforderungen ändern, können Sie selbst nach der Entscheidung den Instance-Typ anpassen. Weitere Informationen finden Sie unter Änderungen des EC2 Amazon-Instanztyps.

Hypervisor-typ

Amazon EC2 unterstützt die folgenden Hypervisoren: Xen und Nitro.

Nitro-basierte Instances

- Allzweck: M5 | M5a | M5ad | M5d | M5dn | M5n | M5zn | M6a | M6g | M6gd | M6i | M6id | M6idn | M6in | M7a | M7g | M7gd | M7i | M7i-flex | M8a | M8g | M8gd | M8i | M8i-flex | T3 | T3a | T4g
- Für Rechenleistung optimiert: C5 | C5a | C5ad | C5d | C5n | C6a | C6g | C6GD | C6Gn | C6i | C6id | C6in | C7a | C7g | C7gd | C7gn | C7i | C7i-Flex | C8a | C8g | C8GB | C8GD | C8gn | C8i | C8i-Flex
- Speicheroptimiert: R5 | R5a | R5ad | R5b | R5d | R5dn | R5n | R6a | R6g | R6gd | R6i | R6id | R6idn | R6in | R7a | R7g | R7g | R7gd | R7i | R7iz | R8a | R8g | R8GB | R8i | R8i-Flex | U-3 TB | U-6 TB | U-9 TB | U-12 TB | U-12 TB | U-18 TB1 | U-24 TB | U7i-6 TB | U7i-8 TB | U7i-12 TB | U7i-12 TB | U7in-16 TB | U7in-24 TB | U7in-32 TB | U7in-32 TB | x2GD | x2IDN | x2IDN | x2IDN | x2IDN | x2ieZN | x8G | x8ADZ | z1d
- Speicheroptimiert: D3 | D3en | I3en | I4g | I4i | I7i | I7ie | I8g | I8ge | Im4gn | Is4gen

- Beschleunigtes Rechnen: DL1 DL2q | | F2 | G4ad | G4dn | G5 | G5g | G6 | G6e | G6f | Gr6 | Gr6f | Inf1 | Inf2 | P4d | P4de | P5 | P5e | P5en | P6-B200 | P6-B300 | GB2 P6e-00 | Trn1 | Trn1n | Trn2 | Trn2 | Trn2 N2u | VT1
- Hochleistungs-Datenverarbeitung: Hpc6a | Hpc6id | Hpc7a | Hpc7g
- Vorherige Generation: A1 | P3dn

Weitere Informationen zu den unterstützten Versionen von Nitro Hypervisor finden Sie unter Unterstützung von Netzwerkfunktionen im Amazon EC2 Instance Types Guide.

Xen-based Instances

- Allgemeine Zwecke: M1 | M2 | M3 | M4 | T1 | T2
- Für Datenverarbeitung optimiert: C1 | C3 | C4
- Arbeitsspeicheroptimiert:: R3 | R4 | X1 | X1e
- Speicheroptimiert: D2 | H1 | I2 | I3
- Beschleunigte Datenverarbeitung:: F1 | G3 | P2 | P3

AMI-Virtualisierungstypen

Der Virtualisierungstyp Ihrer Instance wird durch das AMI bestimmt, das zum Starten der Instance verwendet wird. Instance-Typen der aktuellen Generation unterstützen nur eine Hardware Virtual Machine (HVM). Einige Instance-Typen der vorherigen Generation unterstützen paravirtual (PV) und einige AWS Regionen unterstützen PV-Instances. Weitere Informationen finden Sie unter Virtualisierungstypen.

Um optimale Leistung zu erzielen, empfehlen wir die Verwendung eines HVM-AMI. Darüber hinaus müssen HVM AMIs die Vorteile verbesserter Netzwerke nutzen. Die HVM-Virtualisierung nutzt die von der Plattform bereitgestellte hardwaregestützte Technologie. AWS Mit HVM-Virtualisierung kann die VM wie auf einer nativen Hardwareplattform ausgeführt werden. Es werden jedoch weiterhin PV-Netzwerk- und Speicher-Treiber für bestmögliche Leistung eingesetzt.

Prozessoren

EC2 Instanzen unterstützen eine Vielzahl von Prozessoren.

Prozessoren

- Intel-Prozessoren
- AMD-Prozessoren
- AWS Graviton-Prozessoren
- AWS Trainium
- AWS Inferenz

Intel-Prozessoren

EC2 Amazon-Instances, die auf Intel-Prozessoren ausgeführt werden, können die folgenden Prozessorfunktionen enthalten. Nicht alle Instances, die auf Intel-Prozessoren laufen, unterstützen alle diese Prozessor-Feature. Informationen darüber, welche Funktionen für die einzelnen Instance-Typen verfügbar sind, finden Sie unter EC2 Amazon-Instance-Typen.

- Intel AES New Instructions (AES-NI) – Der Befehlssatz für Intel AES-NI-Verschlüsselung verbessert den Originalalgorithmus Advanced Encryption Standard (AES) in Hinblick auf schnelleren Datenschutz und bessere Sicherheit. Alle EC2 Instances der aktuellen Generation unterstützen diese Prozessorfunktion.
- Intel Advanced Vector Extensions (Intel AVX AVX2, Intel und Intel AVX-512) — Intel AVX und Intel AVX2 sind 256-Bit, und Intel AVX-512 ist eine 512-Bit-Befehlssatzerweiterung, die für Floating Point (FP) -intensive Anwendungen entwickelt wurde. Intel AVX-Befehle verbessern die Leistung für Anwendungen wie Bild- und audio/video Bildverarbeitung, wissenschaftliche Simulationen, Finanzanalysen sowie 3D-Modellierung und -Analyse. Diese Funktionen sind nur auf Instances verfügbar, die mit HVM AMIs gestartet wurden.
- Intel Turbo Boost Technology — Prozessoren der Intel Turbo Boost Technology führen Kerne automatisch schneller als die Basisbetriebsfrequenz aus.
- Intel Deep Learning Boost (Intel DL Boost) — beschleunigt KI-Deep-Learning-Anwendungsfälle. Die skalierbaren Intel Xeon Prozessoren der zweiten Generation erweitern den Intel AVX-512 um neue Vector Neural Network Instruction (VNNI/INT8) that significantly increases deep learning inference performance over previous generation Intel Xeon Scalable processors (with FP32) for image recognition/segmentation, Objekterkennung, Spracherkennung, Sprachübersetzung, Empfehlungssysteme, Verstärkungslernen und mehr). VNNI ist möglicherweise nicht mit allen Linux-Distributionen kompatibel.

  Die folgenden Instances unterstützen VNNI: `M5n`, `R5n`, `M5dn`, `M5zn`, `R5b`, `R5dn`, `D3`, `D3en` und `C6i`. Die Instances `C5` und `C5d` unterstützen VNNI nur für `12xlarge`-, `24xlarge`- und `metal`-Instances.

Die branchenüblichen Benennungskonventionen für 64-Bit können zu Verwirrung führen. CPUs Prozessorhersteller Advanced Micro Devices (AMD) stellte die erste kommerziell erfolgreiche 64-Bit-Architektur basierend auf dem x86-Befehlssatz von Intel vor. Folglich wird die Architektur allgemein als AMD64 unabhängig vom Chiphersteller bezeichnet. Windows und diverse Linux-Distributionen folgen dieser Konvention. Dies erklärt, warum die internen Systeminformationen einer Instanz, auf der Ubuntu oder Windows ausgeführt wird, die CPU-Architektur so AMD64 anzeigen, als ob die Instanzen auf Intel-Hardware laufen.

AMD-Prozessoren

EC2 Amazon-Instances, die auf AMD EPYC-Prozessoren ausgeführt werden, können Ihnen helfen, sowohl Kosten als auch Leistung für Ihre Workloads zu optimieren. Diese Instances unterstützen möglicherweise die folgenden Prozessor-Feature. Nicht alle Instances, die auf Intel-Prozessoren laufen, unterstützen alle diese Prozessor-Feature. Informationen darüber, welche Funktionen für die einzelnen Instance-Typen verfügbar sind, finden Sie unter EC2 Amazon-Instance-Typen.

- AMD Secure Memory Encryption (SME)
- AMD Transparent Single Key Memory Encryption (TSME)
- AMD Advanced Vector Extensions (AVX)
- Sichere verschlüsselte AMD-Virtualisierung – Sicheres verschachteltes Paging (SEV-SNP)
- Vector Neural Network Instructions (VNNI)
- BFloat16

AWS Graviton-Prozessoren

AWS Graviton ist eine Prozessorfamilie, die darauf ausgelegt ist, das beste Preis-Leistungs-Verhältnis für Ihre Workloads zu bieten, die auf EC2 Amazon-Instances ausgeführt werden.

Weitere Informationen finden Sie unter Erste Schritte mit Graviton.

AWS Trainium

Die von AWS Trainium angetriebenen Instances wurden speziell für ein leistungsstarkes und kostengünstiges Deep-Learning-Training entwickelt. Sie können diese Instances verwenden, um die Verarbeitung natürlicher Sprache, Computer Vision und Empfehlungsmodelle zu trainieren, die in einer Vielzahl von Anwendungen verwendet werden, z. B. Spracherkennung, Empfehlung, Betrugserkennung sowie Image- und Videoklassifizierung. Verwenden Sie Ihre vorhandenen Workflows in gängigen ML-Frameworks wie PyTorch und. TensorFlow

AWS Inferenz

Von AWS Inferentia betriebene Instances wurden entwickelt, um Machine Learning zu beschleunigen. Sie bieten hohe Leistung und niedrige Latenzzeiten für Machine-Learning-Inferenzen. Diese Instances sind für die Bereitstellung von Deep-Learning-(DL)-Modellen für Anwendungen wie natürliche Sprachverarbeitung, Objekterkennung und -klassifizierung, Inhaltspersonalisierung und -filterung sowie Spracherkennung optimiert.

Es gibt eine Vielzahl von Möglichkeiten für den Einstieg:

- Verwenden Sie SageMaker KI, einen vollständig verwalteten Service, der der einfachste Weg ist, mit Modellen für maschinelles Lernen zu beginnen. Weitere Informationen finden Sie unter Erste Schritte mit SageMaker KI im Amazon SageMaker AI Developer Guide.
- Starten Sie eine Inf1- oder Inf2-Instance mit dem Deep-Learning-AMI. Weitere Informationen finden Sie unter AWS Inferentia with DLAMI im AWS Deep Learning AMIs -Developer-Handbuch.
- Starten Sie eine Inf1- oder Inf2-Instance mit Ihrem eigenen AMI und installieren Sie den AWS Neuron SDK, mit dem Sie Deep-Learning-Modelle für AWS Inferentia kompilieren, ausführen und profilieren können.
- Starten Sie eine Container-Instance mit einer Inf1- oder Inf2-Instance und einem Amazon-ECS-optimierten AMI. Weitere Informationen finden Sie unter Amazon Linux 2 (Inferentia) AMIs im Amazon Elastic Container Service Developer Guide.
- Erstellen Sie einen Amazon EKS-Cluster mit Knoten, auf denen Inf1-Instances ausgeführt werden. Weitere Informationen finden Sie unter Inferentia-Support im Amazon EKS-Benutzerhandbuch.

Suchen eines Amazon EC2-Instance-Typs

Bevor Sie eine Instance starten können, müssen Sie einen Instance-Typ auswählen, der verwendet werden soll. Der von Ihnen gewählte Instance-Typ hängt unter Umständen von den Ressourcen ab, die Ihre Workload benötigt, z. B. Computing-, Speicher- oder Storage-Ressourcen. Es kann von Vorteil sein, mehrere Instance-Typen zu identifizieren, die zu Ihrer Workload passen, und deren Leistung in einer Testumgebung zu bewerten. Es gibt keinen Ersatz für die Messung der Leistung Ihrer Anwendung unter Last.

Vorschläge und Anleitungen für EC2-Instance-Typen erhalten Sie mit dem EC2-Instance-Typ-Finder. Weitere Informationen finden Sie unter the section called “EC2-Instance-Typ-Finder”.

Wenn Sie bereits EC2-Instances ausgeführt haben, können Sie AWS Compute Optimizer für Empfehlungen zu den Instance-Typen nutzen, die Sie verwenden sollten, um die Leistung zu

verbessern, Kosten zu sparen oder beides. Weitere Informationen finden Sie unter the section called “Empfehlungen zu Compute Optimizer”.

Aufgaben

- Suchen eines Instance-Typs mithilfe der Konsole
- Eine Instance-Typs mithilfe der AWS CLI beschreiben
- Suchen eines Instance-Typs mithilfe der AWS CLI
- Einen Instance-Typ mit den Tools für PowerShell suchen

Suchen eines Instance-Typs mithilfe der Konsole

Mit der Amazon EC2-Konsole finden Sie einen Instance-Typ, der Ihren Anforderungen entspricht.

So suchen Sie einen Instance-Typ mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste die Region aus, in der Sie Ihre Instances starten möchten. Sie können unabhängig von Ihrem Standort jede verfügbare Region auswählen.
3. Wählen Sie im Navigationsbereich Instance Types (Instance-Typen) aus.
4. (Optional) Wählen Sie das Einstellungssymbol (Zahnrad) aus, um festzulegen, welche Attribute des Instance-Typs angezeigt werden sollen (z. B. On-Demand-Linux-Preise), und wählen Sie dann Bestätigen aus. Wählen Sie alternativ den Namen eines Instance-Typs, um die Detailseite zu öffnen und alle über die Konsole verfügbaren Attribute anzuzeigen. Die Konsole zeigt nicht alle Attribute an, die über die API oder die Befehlszeile verfügbar sind.
5. Verwenden Sie die Instance-Typ-Attribute, um die Liste der angezeigten Instance-Typen nur nach den Instance-Typen zu filtern, die Ihren Anforderungen entsprechen. Sie können beispielsweise nach den folgenden Attributen filtern:

   - Availability Zone – Der Name der Availability Zone, der lokalen Zone oder der Wavelength-Zone. Weitere Informationen finden Sie unter the section called “Regionen und Zonen”.
   - vCPUs oder Kerne – Die Anzahl an vCPUs oder Kernen.
   - Arbeitsspeicher (GiB) – Die Speichergröße in GiB
   - Netzwerkleistung – Die Netzwerkleistung in Gigabit.
   - Lokaler Instance-Speicher – Gibt an, ob der Instance-Typ über lokalen Instance-Speicher verfügt (`true` | `false`).

6. (Optional) Aktivieren Sie das Kontrollkästchen für mehrere Instance-Typen, um einen Vergleich anzuzeigen. Der Vergleich wird unten auf dem Bildschirm angezeigt.
7. (Optional) Um die Liste der Instance-Typen zur weiteren Überprüfung in einer CSV-Datei zu speichern, wählen Sie Actions (Aktionen), Download List CSV (Liste als CSV herunterladen). Die Datei enthält alle Instance-Typen, die den von Ihnen festgelegten Filtern entsprechen.
8. (Optional) Um Instances mit einem Instance-Typ zu starten, der Ihren Anforderungen entspricht, aktivieren Sie das Kontrollkästchen für den Instance-Typ und wählen Sie Actions (Aktionen), Launch Instance (Instance starten). Weitere Informationen finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten.

Eine Instance-Typs mithilfe der AWS CLI beschreiben

Sie können den Befehl describe-instance-types verwenden, um einen bestimmten Instance-Typ zu beschreiben.

Einen Instance-Typ vollständig beschreiben

Der folgende Befehl zeigt alle verfügbaren Details für den angegebenen Instance-Typ an. Die Ausgabe ist langwierig, weshalb sie hier weggelassen wird.

```
aws ec2 describe-instance-types \
    --instance-types t2.micro \
    --region us-east-2
```

Einen Instance-Typ beschreiben und die Ausgabe filtern

Der folgende Befehl zeigt die Details für den angegebenen Instance-Typ an.

```
aws ec2 describe-instance-types \
    --instance-types t2.micro \
    --region us-east-2 \
    --query "InstanceTypes[].NetworkInfo"
```

Es folgt eine Beispielausgabe.

```
[
    {
        "NetworkPerformance": "Low to Moderate",
```

```
        "MaximumNetworkInterfaces": 2,
        "MaximumNetworkCards": 1,
        "DefaultNetworkCardIndex": 0,
        "NetworkCards": [
            {
                "NetworkCardIndex": 0,
                "NetworkPerformance": "Low to Moderate",
                "MaximumNetworkInterfaces": 2,
                "BaselineBandwidthInGbps": 0.064,
                "PeakBandwidthInGbps": 1.024
            }
        ],
        "Ipv4AddressesPerInterface": 2,
        "Ipv6AddressesPerInterface": 2,
        "Ipv6Supported": true,
        "EnaSupport": "unsupported",
        "EfaSupported": false,
        "EncryptionInTransitSupported": false,
        "EnaSrdSupported": false
    }
]
```

Mit dem folgenden Befehl wird der verfügbare Arbeitsspeicher für den angegebenen Instance-Typ angezeigt.

```
aws ec2 describe-instance-types \
    --instance-types t2.micro \
    --region us-east-2 \
    --query "InstanceTypes[].MemoryInfo"
```

Es folgt eine Beispielausgabe.

```
[
    {
        "SizeInMiB": 1024
    }
]
```

Suchen eines Instance-Typs mithilfe der AWS CLI

Sie können die Befehle describe-instance-types und describe-instance-type-offerings verwenden, um die Instance-Typen zu finden, die Ihren Anforderungen entsprechen.

Beispiele

- Beispiel 1: Einen Instance-Typ anhand der Availability Zone finden
- Beispiel 2: Einen Instance-Typ anhand der verfügbaren Speichergröße finden
- Beispiel 3: Einen Instance-Typ anhand des verfügbaren Instance-Speichers finden
- Beispiel 4: Einen Instance-Typ finden, der den Ruhezustand unterstützt

Beispiel 1: Einen Instance-Typ anhand der Availability Zone finden

Im folgenden Beispiel werden nur die Instance-Typen angezeigt, die in der angegebenen Availability Zone angeboten werden.

```
aws ec2 describe-instance-type-offerings \
    --location-type "availability-zone" \
    --filters "Name=location,Values=us-east-2a" \
    --region us-east-2 \
    --query "InstanceTypeOfferings[*].[InstanceType]" --output text | sort
```

Die Ausgabe ist eine alphabetisch sortierte Liste von Instance-Typen. Das folgende Beispiel zeigt nur den Anfang der Ausgabe.

```
a1.2xlarge
a1.4xlarge
a1.large
a1.medium
a1.metal
a1.xlarge
c4.2xlarge
   ...
```

Beispiel 2: Einen Instance-Typ anhand der verfügbaren Speichergröße finden

Sie können beispielsweise den folgenden Befehl verwenden, um nur Instance-Typen der aktuellen Generation mit 64 GiB (65 536 MiB) Speicher anzuzeigen.

```
aws ec2 describe-instance-types \
    --filters "Name=current-generation,Values=true" "Name=memory-info.size-in-
mib,Values=65536" \
    --region us-east-2 \
    --query "InstanceTypes[*].[InstanceType]" --output text | sort
```

Die Ausgabe ist eine alphabetisch sortierte Liste von Instance-Typen. Das folgende Beispiel zeigt nur den Anfang der Ausgabe.

```
c5a.8xlarge
c5ad.8xlarge
c6a.8xlarge
c6g.8xlarge
c6gd.8xlarge
c6gn.8xlarge
c6i.8xlarge
c6id.8xlarge
c6in.8xlarge
   ...
```

Beispiel 3: Einen Instance-Typ anhand des verfügbaren Instance-Speichers finden

Im folgenden Beispiel wird die Gesamtgröße des Instance-Speichers für alle R7-Instances mit Instance-Speicher-Volumes angezeigt.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r7*" "Name=instance-storage-
supported,Values=true" \
    --region us-east-2 \
    --query "InstanceTypes[].[InstanceType, InstanceStorageInfo.TotalSizeInGB]" \
    --output table
```

Es folgt eine Beispielausgabe.

```
----------------------------
|  DescribeInstanceTypes   |
+----------------+---------+
|  r7gd.xlarge   |  237    |
|  r7gd.8xlarge  |  1900   |
|  r7gd.16xlarge |  3800   |
|  r7gd.medium   |  59     |
|  r7gd.4xlarge  |  950    |
|  r7gd.2xlarge  |  474    |
|  r7gd.metal    |  3800   |
|  r7gd.large    |  118    |
|  r7gd.12xlarge |  2850   |
+----------------+---------+
```

Beispiel 4: Einen Instance-Typ finden, der den Ruhezustand unterstützt

Im folgenden Beispiel werden die Instance-Typen aufgeführt, die den Ruhezustand unterstützen.

```
aws ec2 describe-instance-types \
    --filters "Name=hibernation-supported,Values=true" \
    --region us-east-2 \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

Die Ausgabe ist eine alphabetisch sortierte Liste von Instance-Typen. Das folgende Beispiel zeigt nur den Anfang der Ausgabe.

```
c4.2xlarge
c4.4xlarge
c4.8xlarge
c4.large
c4.xlarge
c5.12xlarge
c5.18xlarge
c5.2xlarge
c5.4xlarge
c5.9xlarge
...
```

Einen Instance-Typ mit den Tools für PowerShell suchen

Sie können die cmdlets Get-EC2InstanceType und Get-EC2InstanceTypeOffering verwenden, um die Instance-Typen zu suchen, die Ihren Anforderungen entsprechen.

Beispiele

- Finden Sie einen Instance-Typ anhand der Availability Zone
- Finden eines Instance-Typs anhand der verfügbaren Arbeitsspeichergröße
- Finden eines Instance-Typs anhand des verfügbaren Instance-Speichers
- Finden Sie einen Instance-Typ, der den Ruhezustand unterstützt

Finden Sie einen Instance-Typ anhand der Availability Zone

Im folgenden Beispiel werden nur die Instance-Typen angezeigt, die in der angegebenen Availability Zone angeboten werden.

```
(Get-EC2InstanceTypeOffering `
    -LocationType "availability-zone" `
    -Region us-east-2 `
    -Filter @{Name="location"; Values="us-east-2a"}).InstanceType | Sort-Object `
```

Finden eines Instance-Typs anhand der verfügbaren Arbeitsspeichergröße

Sie können beispielsweise den folgenden Befehl verwenden, um nur Instance-Typen der aktuellen Generation mit 64 GiB (65 536 MiB) Speicher anzuzeigen.

```
(Get-EC2InstanceType `
    -Filter @{Name="current-generation"; Values="true"},
            @{Name="memory-info.size-in-mib"; Values="65536"}).InstanceType | Sort-
Object
```

Finden eines Instance-Typs anhand des verfügbaren Instance-Speichers

Im folgenden Beispiel wird die Gesamtgröße des Instance-Speichers für alle R7-Instances mit Instance-Speicher-Volumes angezeigt.

```
Get-EC2InstanceType `
    -Filter @{Name="instance-type"; Values="r7*"},
            @{Name="instance-storage-supported"; Values="true"} | `
     Select InstanceType, @{Name="TotalSizeInGB";
 Expression={($_.InstanceStorageInfo.TotalSizeInGB)}}
```

Es folgt eine Beispielausgabe.

```
InstanceType  TotalSizeInGB
------------  -------------
r7gd.8xlarge           1900
r7gd.16xlarge          3800
r7gd.xlarge             237
r7gd.4xlarge            950
r7gd.medium              59
r7gd.2xlarge            474
r7gd.large              118
r7gd.metal             3800
r7gd.12xlarge          2850
```

Finden Sie einen Instance-Typ, der den Ruhezustand unterstützt

Im folgenden Beispiel werden die Instance-Typen aufgeführt, die den Ruhezustand unterstützen.

```
(Get-EC2InstanceType `
    -Filter @{Name="hibernation-supported"; Values="true"}).InstanceType | Sort-Object
```

Holen Sie sich Empfehlungen vom EC2-Instance-Typ-Finder

EC2-Instance-Typ-Finder berücksichtigt Ihren Anwendungsfall, Ihren Workload-Typ und die Präferenz des CPU-Herstellers und die Art und Weise, wie Sie Preis und Leistung priorisieren sowie weitere Parameter, die Sie angeben können. Anschließend werden diese Daten verwendet, um Anleitungen und Vorschläge für Amazon-EC2-Instance-Typen bereitzustellen, die für Ihre neuen Workloads am besten geeignet sind.

Da so viele Instance-Typen verfügbar sind, kann es zeitaufwendig sein, die richtigen Instance-Typen für Ihren Workload zu finden. Mithilfe des EC2-Instance-Typ-Finders können Sie über die neuesten Instance-Typen auf dem Laufenden bleiben und das beste Preis-Leistungs-Verhältnis für Ihre Workloads erzielen.

Sie können Vorschläge und Anleitungen für EC2-Instance-Typen mit der Amazon-EC2-Konsole erhalten. Sie können auch direkt zu Amazon Q gehen, um eine Beratung zu Instance-Typen zu erhalten. Weitere Informationen finden Sie im Benutzerhandbuch für Amazon Q Developer.

Wenn Sie nach Empfehlungen zum Instance-Typ für einen bestehenden Workload suchen, verwenden Sie AWS Compute Optimizer. Weitere Informationen finden Sie unter EC2-Instance-Empfehlungen von Compute Optimizer abrufen.

EC2-Instance-Typ-Finder verwenden

In der Amazon-EC2-Konsole können Sie Vorschläge zu Instance-Typen über den EC2-Instance-Typ-Finder im Launch Instance Wizard, beim Erstellen einer Startvorlage oder auf der Seite Instance-Typen abrufen.

Verwenden Sie die folgenden Anweisungen, um mithilfe des EC2-Instance-Typ-Finders in der Amazon-EC2-Konsole Anleitungen und Vorschläge für EC2-Instance-Typen zu erhalten. Eine Animation dieser Schritte finden Sie unter Animation anzeigen: Mithilfe des EC2-Instance-Typ-Finders erhalten Sie Vorschläge für Instance-Typen.

Erhalten Sie mithilfe von EC2-Instance-Typ-Finder Vorschläge für Instance-Typen

1. Starten Sie Ihren Prozess mit einer der folgenden Optionen:

   - Befolgen Sie das Verfahren zum Starten einer Instance. Wählen Sie neben Instance-Typ die Verknüpfung Tipps einholen.
   - Gehen Sie folgendermaßen vor, um eine Startvorlage zu erstellen. Wählen Sie neben Instance-Typ die Verknüpfung Tipps einholen.
   - Wählen Sie im Navigationsbereich die Option Instance-Typen und anschließend die Schaltfläche für Instance-Typ-Finder aus.

2. Gehen Sie auf dem Bildschirm Tipps zur Auswahl des Instance-Typs erhalten wie folgt vor:

   a. Geben Sie Ihre Anforderungen an den Instance-Typ an, indem Sie Optionen für Workload-Typ, Anwendungsfall, Priorität und CPU-Hersteller auswählen.

   b. (Optional) Um detailliertere Anforderungen für Ihren Workload anzugeben, gehen Sie wie folgt vor:

      i. Erweitern Sie Erweiterte Parameter.

      ii. Um einen Parameter hinzuzufügen, wählen Sie einen Parameter aus, klicken Sie auf Hinzufügen und geben Sie einen Wert für den Parameter an. Wiederholen Sie den Vorgang für jeden zusätzlichen Parameter, den Sie hinzufügen möchten. Wenn Sie keinen Mindest- oder Höchstwert angeben wollen, lassen Sie das Feld leer.

      iii. Um einen Parameter nach dem Hinzufügen zu entfernen, wählen Sie das X neben dem Parameter aus.

   c. Wählen Sie Tipps zu Instance-Typen einholen.

      Amazon EC2 bietet Ihnen Vorschläge für Instance-Familien, die Ihren spezifischen Anforderungen entsprechen.

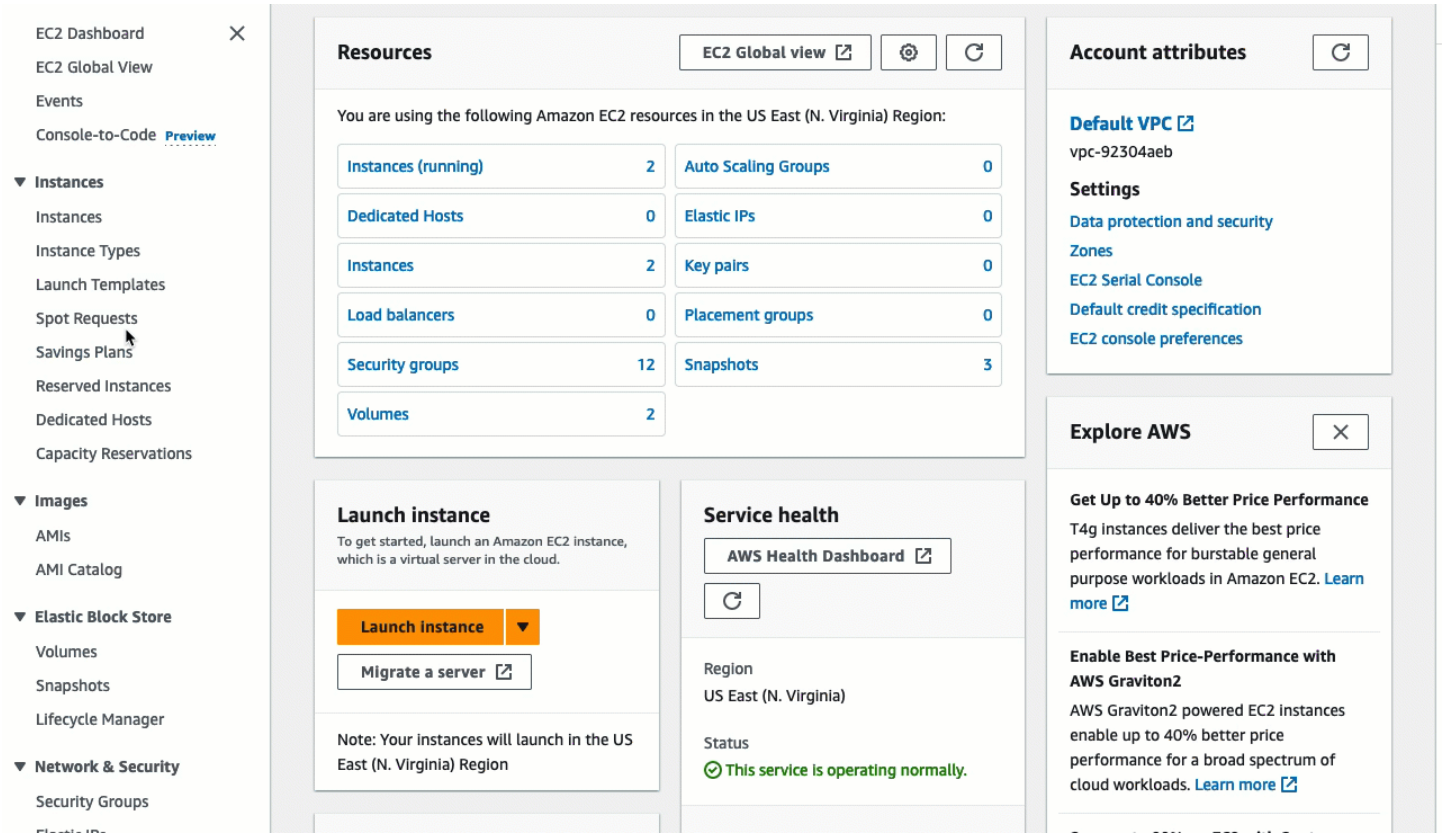
3. Um die Details der einzelnen Instance-Typen innerhalb der vorgeschlagenen Instanc-Familien anzuzeigen, wählen Sie Empfohlene Instance-Familiendetails anzeigen.

4. Wählen Sie einen Instance-Typ aus, der Ihren Anforderungen entspricht, und wählen Sie dann Aktionen, Instance starten oder Aktionen, Startvorlage erstellen.

   Wenn Sie den Vorgang alternativ im Launch Instance Wizard oder auf der Startvorlagenseite gestartet haben und lieber zu Ihrem ursprünglichen Flow zurückkehren möchten, notieren Sie sich den Instance-Typ, den Sie verwenden möchten. Dann wählen Sie im Launch Instance

Wizard oder in der Startvorlage für Instance-Typ den Instance-Typ aus und schließen Sie den Vorgang ab, um eine Instance zu starten oder eine Startvorlage zu erstellen.

Animation anzeigen: Mithilfe des EC2-Instance-Typ-Finders erhalten Sie Vorschläge für Instance-Typen



EC2-Instance-Empfehlungen von Compute Optimizer abrufen

AWS Compute Optimizer bietet Empfehlungen für Amazon EC2, die Ihnen helfen, die Leistung zu verbessern, Geld zu sparen oder beides. Sie können diese Empfehlungen nutzen, um zu entscheiden, ob Sie zu einem neuen Instance-Typ wechseln wollen.

Zur Abgabe von Empfehlungen analysiert Compute Optimizer Ihre vorhandenen Instance-Spezifikationen und Auslastungsmetriken. Die kompilierten Daten werden dann für die Empfehlung verwendet, welche Amazon EC2-Instance-Typen den vorhandenen Workload am besten bewältigen können. Empfehlungen werden zusammen mit den Preisen der Instance pro Stunde zurückgegeben. Weitere Informationen finden Sie unter Amazon-EC2-Instance-Metriken im Benutzerhandbuch für AWS Compute Optimizer.

Inhalt

- Voraussetzungen
- Klassifizierungen finden
- Anzeigen von Empfehlungen
- Überlegungen zur Bewertung von Empfehlungen

Voraussetzungen

Um Empfehlungen von Compute Optimizer zu erhalten, müssen Sie sich zunächst bei Compute Optimizer anmelden. Weitere Informationen finden Sie unter Erste Schritte in AWS Compute Optimizer im AWS Compute Optimizer-Benutzerhandbuch.

Compute Optimizer generiert Empfehlungen für einige, aber nicht für alle Instance-Typen. Wenn Sie einen Instancetyp verwenden, der nicht unterstützt wird, generiert Compute Optimizer keine Empfehlungen. Eine Liste der unterstützten Instance-Typen finden Sie unter Amazon-EC2-Instance-Anforderungen im Benutzerhandbuch für AWS Compute Optimizer.

Klassifizierungen finden

Compute Optimizer klassifiziert seine Ergebnisse für EC2-Instances wie folgt:

- Unterdimensioniert– Eine EC2-Instance gilt als unterdimensioniert, wenn mindestens eine Spezifikation Ihrer Instance, z. B. CPU, Arbeitsspeicher oder Netzwerk, die Leistungsanforderungen für Ihre Verarbeitungslast (Workload) nicht erfüllt. Unterdimensionierte EC2-Instances führen möglicherweise zu einer schlechten Anwendungsleistung.
- Überdimensioniert – Eine EC2-Instance gilt als überdimensioniert, wenn mindestens eine Spezifikation Ihrer Instance, z. B. CPU, Arbeitsspeicher oder Netzwerk, verringert werden kann und dabei nach wie vor die Leistungsanforderungen für Ihr Workload erfüllt werden und wenn keine Spezifikation mangelhaft erfüllt wird. Überdimensionierte EC2-Instances können zu überflüssigen Infrastrukturkosten führen.
- Optimiert– Eine EC2-Instance gilt als optimiert, wenn alle Spezifikationen Ihrer Instance, z. B. CPU, Arbeitsspeicher und Netzwerk, die Leistungsanforderungen für Ihr Workload erfüllen und die Instance nicht überdimensioniert wird. Eine optimierte EC2-Instance führt Ihre Workloads mit optimalen Leistungs- und Infrastrukturkosten aus. Für optimierte Instances empfiehlt Compute Optimizer mitunter einen Instance-Typ einer neuen Generation.
- Keine– Für diese Instance liegen keine Empfehlungen vor. Dies kann vorkommen, wenn Sie bei Compute Optimizer weniger als 12 Stunden angemeldet waren oder die Instance weniger als

30 Stunden ausgeführt wurde oder wenn der Instance-Typ von Compute Optimizer nicht unterstützt wird.

Anzeigen von Empfehlungen

Nachdem Sie sich bei Compute Optimizer angemeldet haben, können Sie die Erkenntnisse, die Compute Optimizer für Ihre EC2-Instances generiert, in der Amazon-EC2-Konsole anzeigen. Anschließend können Sie auf die Compute Optimizer-Konsole zugreifen, um die Empfehlungen anzuzeigen. Wenn Sie sich vor kurzem angemeldet haben, werden die Ergebnisse möglicherweise bis zu 12 Stunden lang nicht in der EC2-Konsole angezeigt.

Empfehlungen für eine Instance mit der Amazon-EC2-Konsole anzeigen lassen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance-ID, um die Instance-Detailseite zu öffnen.
4. Suchen Sie auf der Detailseite der Instance im oberen Bereich der Zusammenfassung AWS Compute Optimizer-Erkenntnis. Wenn es eine Erkenntnis gibt, zeigen wir die Klassifizierung der Erkenntnis und einen Link zur Ansicht der Details an. Andernfalls wird die Meldung Keine Empfehlungen für diese Instance verfügbar angezeigt.
5. Wenn es eine Erkenntnis gibt, wählen Sie Detail anzeigen. Dadurch wird die Seite Empfehlungen für EC2-Instances in der Compute-Optimizer-Konsole geöffnet. Der aktuelle Instance-Typ trägt die Bezeichnung Aktuell. Es werden bis zu drei verschiedene Empfehlungen für Instance-Typen gegeben, die als Option 1, Option 2 und Option 3 bezeichnet werden. Auf dieser Seite werden auch aktuelle CloudWatch-Metrikdaten für die Instance angezeigt.

So zeigen Sie Empfehlungen für alle Instances in allen Regionen an

In der Compute-Optimizer-Konsole können Sie sich Empfehlungen für all Ihre Amazon-EC2-Instances in allen Regionen ansehen. Weitere Informationen finden Sie unter Empfehlungen für EC2-Instances anzeigen und EC2-Instance-Details anzeigen im Benutzerhandbuch für AWS Compute Optimizer.

Überlegungen zur Bewertung von Empfehlungen

Wenn Sie eine Empfehlung erhalten, müssen Sie entscheiden, ob darauf reagiert werden soll. Bevor Sie einen Instance-Typ ändern, sollten Sie Folgendes beachten:

- Die Empfehlungen prognostizieren nicht Ihre Nutzung. Die Empfehlungen basieren auf Ihrer bisherigen Nutzung während des letzten 14-Tage-Zeitraums. Stellen Sie sicher, dass Sie einen Instance-Typ auswählen, der Ihren künftigen Ressourcenanforderungen entspricht.
- Konzentrieren Sie sich auf die grafisch dargestellten Metriken, um zu ermitteln, ob die tatsächliche Nutzung geringer als die Instance-Kapazität ist. Sie können sich die Metrikdaten (Durchschnitt, Höchstlast, Perzentil) auch in CloudWatch anzeigen lassen, um weitere Erkenntnisse aus Ihrer Empfehlungen für EC2-Instances zu erlangen. Beachten Sie zum Beispiel, wie sich die prozentualen CPU-Prozentsatzmetriken im Laufe des Tages verändern und ob es Datenverkehrsspitzen gibt, die berücksichtigt werden müssen. Weitere Informationen finden Sie unter Viewing Available Metrics (Anzeigen der verfügbaren Metriken) im Amazon CloudWatch-Benutzerhandbuch.
- Compute Optimizer bietet möglicherweise Empfehlungen für Instances mit Spitzenlastleistung, bei denen es sich um T3-, T3a- und T2-Instances handelt. Wenn Sie regelmäßig über die Basisleistung hinausgehen, stellen Sie sicher, dass Sie dies weiterhin auf der Grundlage der vCPUs des neuen Instance-Typs tun können. Weitere Informationen finden Sie unter Schlüsselkonzepte und Definitionen für Instances mit Spitzenlastleistung.
- Wenn Sie eine Reserved Instance erworben haben, wird Ihnen Ihre On-Demand-Instance möglicherweise als Reserved Instance in Rechnung gestellt. Bevor Sie den aktuellen Instance-Typ ändern, sollten Sie zunächst die Auswirkungen auf die Nutzung und Abdeckung der Reserved Instance bewerten.
- Ziehen Sie nach Möglichkeit einen Umstieg auf Instances der neueren Generation in Betracht.
- Bei der Migration auf eine andere Instance-Familie ist darauf zu achten, dass der aktuelle Instance-Typ und der neue Instance-Typ miteinander kompatibel sind, z. B. in Bezug auf Virtualisierung, Architektur oder Netzwerktyp. Weitere Informationen finden Sie unter Kompatibilität zum Ändern des Instance-Typs.
- Berücksichtigen Sie abschließend die Bewertung des Leistungsrisikos, die für jede Empfehlung angegeben ist. Das Leistungsrisiko gibt den Aufwand an, den Sie möglicherweise aufwenden müssen, um zu überprüfen, ob der empfohlene Instance-Typ den Leistungsanforderungen Ihrem Workload entspricht. Darüber hinaus empfehlen wir, vor und nach jeder Änderung Last- und Leistungstests durchzuführen.

Änderungen des EC2 Amazon-Instanztyps

Wenn sich Ihre Anforderungen ändern, wird Ihre Instance möglicherweise überlastet (der Instance-Typ ist zu klein) oder wird nicht voll ausgelastet (der Instance-Typ ist zu groß). In diesem Fall können

Sie die Größe Ihrer Instance ändern, indem Sie ihren Instance-Typ ändern. Beispiel: Wenn Ihre `t2.micro`-Instance zu klein für den Workload ist, können Sie die Größe erhöhen, indem Sie sie in einen größeren T2-Instance-Typ ändern, z. B. `t2.large`. Oder Sie ändern sie in einen anderen Instance-Typ wie z. B. `m5.large`. Möglicherweise möchten Sie auch von einem Instance-Typ der vorherigen Generation zu einem Instance-Typ der aktuellen Generation wechseln, um einige Funktionen nutzen zu können, z. B. die Unterstützung für IPv6.

Wenn Sie eine Empfehlung für einen Instance-Typ wünschen, der Ihren vorhandenen Workload am besten verarbeiten kann, können Sie AWS Compute Optimizer nutzen. Weitere Informationen finden Sie unter EC2-Instance-Empfehlungen von Compute Optimizer abrufen.

Wenn Sie den Instance-Typ ändern, zahlen Sie ab dann den Tarif des neuen Instance-Typs. Die On-Demand-Tarife aller Instance-Typen finden Sie unter Amazon EC2 On-Demand-Preise.

Um Ihrer Instance zusätzlichen Speicherplatz hinzuzufügen, ohne den Instance-Typ zu ändern, fügen Sie der Instance ein EBS-Volume hinzu. Weitere Informationen finden Sie unter Anfügen eines Amazon-EBS-Volumes an eine Instance im Amazon-EBS-Benutzerhandbuch.

Welche Anweisungen müssen Sie befolgen?

Zum Ändern des Instance-Typs sind verschiedene Anweisungen verfügbar. Die zu verwendenden Anweisungen hängen vom Root-Volume der Instance ab und davon, ob der Instance-Typ mit der aktuellen Konfiguration der Instance kompatibel ist. Weitere Informationen zur Bestimmung der Kompatibilität finden Sie unter Kompatibilität zum Ändern des Instance-Typs.

Bestimmen Sie anhand der nachstehenden Tabelle, welche Anweisungen zu befolgen sind.

Root-Volume	Kompatibilität	Diese Anweisungen befolgen
EBS	Kompatibel	Ändern des Instance-Typs
EBS	Nicht kompatibel	Zu einem größeren Instance-Typ migrieren
Instance-Speicher	Nicht zutreffend	Zu einem größeren Instance-Typ migrieren

Kompatibilität zum Ändern des Instance-Typs

Sie können den Instance-Typ nur ändern, wenn die aktuelle Konfiguration der Instance mit dem gewünschten Instance-Typ kompatibel ist. Wenn der gewünschte Instance-Typ nicht mit der aktuellen

Konfiguration der Instance kompatibel ist, müssen Sie eine neue Instance mit einer Konfiguration starten, die mit dem Instance-Typ kompatibel ist, und dann Ihre Anwendung auf die neue Instance migrieren.

Die Kompatibilität wird folgendermaßen ermittelt:

Virtualisierungstyp

Linux AMIs verwendet eine von zwei Arten der Virtualisierung: paravirtuelle (PV) oder virtuelle Hardware-Maschine (HVM). Wenn eine Instance von einem PV-AMI gestartet wurde, können Sie nicht zu einem Instance-Typ wechseln, der nur HVM ist. Weitere Informationen finden Sie unter Virtualisierungstypen. Um den Virtualisierungstyp Ihrer Instance zu überprüfen, überprüfen Sie den Virtualisierungswert im Detailbereich des Bildschirms Instances in der EC2 Amazon-Konsole.

Architektur

AMIs sind spezifisch für die Architektur des Prozessors, daher müssen Sie einen Instance-Typ mit derselben Prozessorarchitektur wie der aktuelle Instance-Typ auswählen. Zum Beispiel:

- Wenn der aktuelle Instance-Typ einen auf der ARM-Architektur basierenden Prozessor hat, sind Sie auf die Instance-Typen beschränkt, die einen auf der ARM-Architektur basierenden Prozessor unterstützen, z. B. C6g und M6g.
- Die folgenden Instance-Typen sind die einzigen Instance-Typen, die 32-Bit- AMIs unterstützen: `t2.nano`, `t2.micro`, `t2.small`, `t2.medium`, `c3.large`, `t1.micro`, `m1.small`, `m1.medium` und `c1.medium`. Wenn Sie den Instance-Typ einer 32-Bit-Instance ändern, sind Sie auf diese Instance-Typen beschränkt.

Netzwerkadapter

Wenn Sie von einem Treiber für einen Netzwerkadapter zu einem anderen wechseln, werden die Netzwerkadaptereinstellungen zurückgesetzt, wenn das Betriebssystem den neuen Adapter erstellt. Um die Einstellungen neu zu konfigurieren, benötigen Sie möglicherweise Zugriff auf ein lokales Konto mit Administratorberechtigungen. Nachfolgend finden Sie Beispiele für den Wechsel von einem Netzwerkadapter zu einem anderen:

- AWS PV (T2-Instances) auf Intel 82599 VF (M4-Instances)
- Intel 82599 VF (die meisten M4-Instances) zu ENA (M5-Instances)
- ENA (M5-Instances) zu ENA mit hoher Bandbreite (M5n-Instances)

Enhanced Networking

Instance-Typen, die Enhanced Networking unterstützen, erfordern die Installation der notwendigen Treiber. Nitro-basierte Instances erfordern beispielsweise EBS-gestützte Instances,

AMIs bei denen die Elastic Network Adapter (ENA) -Treiber installiert sind. Um von einem Instance-Typ, der Enhanced Networking nicht unterstützt, zu einem Instance-Typ zu wechseln, der es unterstützt, müssen Sie die ENA-Treiber oder ixgbevf-Treiber entsprechend auf der Instance installieren.

> **Note**
>
> Wenn Sie die Größe einer Instance ändern, bei der ENA Express aktiviert ist, muss der neue Instance-Typ auch ENA Express unterstützen. Eine Liste mit Instance-Typen, die ENA Express unterstützen, finden Sie unter Unterstützte Instance-Typen für ENA Express.
> Wenn Sie von einem Instance-Typ, der ENA Express unterstützt, zu einem Instance-Typ wechseln möchten, der ENA Express nicht unterstützt, stellen Sie sicher, dass ENA Express nicht aktiviert ist, bevor Sie die Größe der Instance ändern.

NVMe

EBS-Volumes werden auf Nitro-basierten Instances als NVMe Blockgeräte verfügbar gemacht. Wenn Sie von einem Instance-Typ, der dies nicht unterstützt, NVMe zu einem Instance-Typ wechseln, der dies unterstützt NVMe, müssen Sie zuerst die NVMe Treiber auf Ihrer Instance installieren. Außerdem werden die Gerätenamen für Geräte, die Sie in der Blockgerätezuordnung angeben, mithilfe von NVMe Gerätenamen (`/dev/nvme[0-26]n1`) umbenannt.

[Linux-Instanzen] Um Dateisysteme beim Booten mithilfe von zu mounten`/etc/fstab`, müssen Sie daher Gerätenamen UUID/Label anstelle von Gerätenamen verwenden.

Volume-Limit

Die maximale Anzahl von Amazon-EBS-Volumes, die Sie einer Instance anfügen können, hängt vom Instance-Typ und der Instance-Größe ab. Weitere Informationen finden Sie unter Amazon EBS-Volumenlimits für Amazon-Instances EC2 .

Sie können nur zu einem Instance-Typ oder einer Instance-Größe wechseln, der/die dieselbe oder eine größere Anzahl von Volumes unterstützt, als derzeit an die Instance angefügt ist. Wenn Sie zu einem Instance-Typ oder einer Instance-Größe wechseln, die die Anzahl der aktuell angefügten Volumes nicht unterstützt, schlägt die Anfrage fehl. Wenn Sie beispielsweise von einer `m7i.4xlarge`-Instance mit 32 angefügten Volumes zu einer `m6i.4xlarge`-Instance wechseln, die maximal 27 Volumes unterstützt, schlägt die Anfrage fehl.

NitroTPM

Wenn Sie die Instance mit einem AMI mit aktiviertem NitroTPM und einem Instance-Typ gestartet haben, wird die Instance mit aktiviertem NitroTPM gestartet. Sie können nur zu einem Instance-Typ wechseln, der ebenfalls NitroTPM unterstützt.

Ändern Sie den Instance-Typ für Ihre EC2 Amazon-Instance

Verwenden Sie die folgenden Anweisungen, um den Instance-Typ einer Amazon-EBS-gestützten Instance zu ändern, wenn der gewünschte Instance-Typ mit der aktuellen Konfiguration der Instance kompatibel ist. Weitere Informationen finden Sie unter the section called “Kompatibilität”.

Überlegungen

- Sie müssen Ihre Instance anhalten, bevor Sie ihren Instance-Typ ändern können. Planen Sie Stillstandzeiten ein, während Ihre Instance angehalten ist. Das Anhalten der Instance und die Änderung des Instance-Typs können ein paar Minuten dauern. Der Neustart Ihrer Instance kann je nach den Startup-Skripten Ihrer Anwendung unterschiedlich lange dauern. Weitere Informationen finden Sie unter Stoppen und starten Sie EC2 Amazon-Instances.
- Wenn Sie eine Instance anhalten und wieder starten, wird sie auf neue Hardware verschoben. Wenn Ihre Instance eine öffentliche IPv4 Adresse hat, bei der es sich nicht um eine Elastic IP handelt, geben wir die Adresse frei und geben Ihrer Instance eine neue öffentliche IPv4 Adresse. Weitere Informationen zum Verhalten von IP-Adressen während des gesamten Lebenszyklus einer Instance finden Sie unter Unterschiede zwischen Instance-Status.
- Sie können den Instance-Typ einer Spot-Instance nicht ändern.
- [Windows-Instanzen] Wir empfehlen, dass Sie das AWS PV-Treiberpaket aktualisieren, bevor Sie den Instance-Typ ändern. Weitere Informationen finden Sie unter the section called “Upgrade für PV-Treiber”.
- Wenn sich Ihre Instance in einer Amazon EC2 Auto Scaling-Gruppe befindet, markiert der Amazon EC2 Auto Scaling-Service die gestoppte Instance als fehlerhaft und beendet sie möglicherweise und startet eine Ersatz-Instance. Um dies zu verhindern, können Sie die Skalierungsprozesse für die Gruppe anhalten, während Sie den Instance-Typ ändern. Weitere Informationen finden Sie unter Einen Prozess für eine Amazon EC2 Auto Scaling Scaling-Gruppe aussetzen und wieder aufnehmen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.
- Wenn Sie den Instance-Typ einer NVMe Instance mit Instance-Speicher-Volumes ändern, verfügt die aktualisierte Instance möglicherweise über zusätzliche Instance-Speicher-Volumes, da alle

NVMe Instance-Speicher-Volumes verfügbar sind, auch wenn sie nicht in der AMI- oder Instance-Block-Gerätezuordnung angegeben sind. Anderenfalls weist die aktualisierte Instance die gleiche Anzahl von Instance-Speicher-Volumes auf, die Sie beim Starten der ursprünglichen Instance angegeben haben.

- Die maximale Anzahl von Amazon-EBS-Volumes, die Sie einer Instance anfügen können, hängt vom Instance-Typ und der Instance-Größe ab. Sie können nicht zu einem Instance-Typ oder einer Instance-Größe wechseln, die nicht die Anzahl der Volumes unterstützt, die bereits an Ihre Instance angefügt sind. Weitere Informationen finden Sie unter Amazon EBS-Volumenlimits für Amazon-Instances EC2 .
- [Linux-Instances] Sie können das `AWSSupport-MigrateXenToNitroLinux`-Runbook verwenden, um kompatible Instances von einem Xen-Instance-Typ zu einem Nitro-Instance-Typ zu migrieren. Weitere Informationen finden Sie unter AWSSupport-MigrateXenToNitroLinux runbook in der Referenz zum AWS Systems Manager -Automation-Runbook.
- [Windows-Instances] Weitere Hinweise zur Migration kompatibler Windows-Instances von einem Xen-Instance-Typ zu einem Nitro-Instance-Typ finden Sie unter Zu Instance-Typen der letzten Generation migrieren.

So ändern Sie den Instance-Typ einer Amazon-EBS-gestützten Instance

1. (Optional) Wenn für den neuen Instance-Typ Treiber erforderlich sind, die nicht auf der vorhandenen Instance installiert sind, müssen Sie eine Verbindung zu Ihrer Instance einrichten und zuerst die Treiber installieren. Weitere Informationen finden Sie unter Kompatibilität zum Ändern des Instance-Typs.
2. [Windows-Instances] Wenn Sie Ihre Windows-Instance so konfiguriert haben, dass sie statische IP-Adressen verwendet, und Sie von einem Instance-Typ, der kein erweitertes Netzwerk unterstützt, zu einem Instance-Typ wechseln, der ein erweitertes Netzwerk unterstützt, erhalten Sie möglicherweise eine Warnung über einen potenziellen IP-Adressenkonflikt, wenn Sie erneut statische IP-Adressen konfigurieren. Sie können das verhindern, indem Sie DHCP für die Netzwerkschnittstelle der Instance aktivieren, bevor Sie den Instance-Typ ändern. Öffnen Sie in Ihrer Instance das Network and Sharing Center, öffnen Sie die Eigenschaften von Internet Protocol Version 4 (TCP/IPv4) für die Netzwerkschnittstelle und wählen Sie IP-Adresse automatisch beziehen aus. Ändern Sie den Instance-Typ und konfigurieren Sie die statische IP-Adresszuweisung für die Netzwerkschnittstelle neu.
3. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
4. Wählen Sie im Navigationsbereich Instances aus.

5. Wählen Sie die Instance und dann Instance-Status, Instance anhalten aus. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Stop aus. Das Anhalten der Instance kann einige Minuten dauern.
6. Während die Instance noch ausgewählt ist, wählen Sie Aktionen, Instance-Einstellungen, Instance-Typ ändern aus. Diese Option ist deaktiviert, wenn der Status der Instance nicht lautet `stopped`.
7. Gehen Sie auf der Seite Ändern des Instance-Typs wie folgt vor:

   a. Wählen Sie unter Instance-Typ den gewünschten Instance-Typ aus.

      Wenn der Instance-Typ nicht in der Liste enthalten ist, ist er nicht mit der Konfiguration Ihrer Instance kompatibel. Befolgen Sie stattdessen die nachstehenden Anweisungen: Migrieren Sie zu einem neuen Instanztyp, indem Sie eine neue EC2 Instanz starten.

   b. (Optional) Wenn der ausgewählte Instance-Typ EBS-Optimierung unterstützt, wählen Sie EBS-optimiert aus, um die EBS-Optimierung zu aktivieren oder löschen Sie EBS-optimiert, um die Optimierung zu deaktivieren.

      Wenn der ausgewählte Instance-Typ standardmäßig EBS-optimiert ist, ist die Option EBS-optimiert bereits ausgewählt und Sie können sie nicht deaktivieren.

   c. (Optional) vCPU-Optionen für den neuen Instance-Typ konfigurieren.

      Wenn Sie den Instance-Typ einer vorhandenen Instance ändern, EC2 wendet Amazon nach Möglichkeit die CPU-Optionseinstellungen der vorhandenen Instance auf die neue Instance an. Wenn der neue Instance-Typ diese Einstellungen nicht unterstützt, werden die CPU-Optionen auf Keine zurückgesetzt. Diese Option verwendet die Standardzahl v CPUs für den neuen Instance-Typ.

      Wenn der von Ihnen ausgewählte Instance-Typ die vCPU-Konfiguration unterstützt, wählen Sie im Bereich Erweiterte Details die Option CPU-Optionen angeben aus, um v CPUs für Ihren neuen Instance-Typ zu konfigurieren.

   d. Wählen Sie Ändern, um die neuen Einstellungen zu übernehmen.
8. Um die Instance zu starten, wählen Sie die Instance aus und wählen Sie Instance state (Instance-Status), Start instance (Instance starten). Es kann einige Minuten dauern, bis die Instance in den Zustand `running` übergeht. Wenn Ihre Instance nicht startet, finden Sie weitere Informationen unter Problembehandlung beim Ändern des Instance-Typs.
9. [Windows-Instanzen] Wenn auf Ihrer Instanz Windows Server 2016 oder Windows Server 2019 mit EC2 Launch v1 ausgeführt wird, stellen Sie eine Verbindung zu Ihrer Windows-Instanz her

und führen Sie das folgende EC2 PowerShell Startskript aus, um die Instanz zu konfigurieren, nachdem der Instanztyp geändert wurde.

> **Important**
>
> Das Administratorkennwort wird zurückgesetzt, wenn Sie das EC2 Startskript für die Initialisierung der Instanz aktivieren. Sie können die Konfigurationsdatei bearbeiten, um das Zurücksetzen des Administratorpassworts zu deaktivieren, indem Sie es in den Einstellungen für die Initialisierungsaufgaben festlegen. Schritte zum Deaktivieren des Kennwortzurücksetzens finden Sie unter Initialisierungsaufgaben konfigurieren (EC2Launch) oder Einstellungen ändern (EC2Launch v2).

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

Migrieren Sie zu einem neuen Instanztyp, indem Sie eine neue EC2 Instanz starten

Sie können den Instance-Typ einer EC2 Instance nur ändern, wenn es sich um eine EBS-gestützte Instance mit einer Konfiguration handelt, die mit dem gewünschten neuen Instance-Typ kompatibel ist. Andernfalls, wenn die Konfiguration oder Ihre Instance nicht mit dem neuen Instance-Typ kompatibel ist oder es sich um eine Instance handelt, die im Instance-Speicher ist, müssen Sie eine Ersatz-Instance starten, die mit dem gewünschten Instance-Typ kompatibel ist. Weitere Informationen, wie die Kompatibilität bestimmt wird, finden Sie unter Kompatibilität zum Ändern des Instance-Typs.

Übersicht über den Migrationsprozess

- Sichern Sie die Daten Ihrer ursprünglichen Instance.
- Starten Sie eine neue Instance mit einer Konfiguration, die mit dem neuen Instance-Typ kompatibel ist, und fügen Sie alle EBS-Volumes an, die an Ihre ursprüngliche Instance angehängt waren.
- Installieren Sie Ihre Anwendung auf Ihrer neuen Instance.
- Stellen Sie alle Daten wieder her.
- Wenn Ihre ursprüngliche Instance über eine elastische IP-Adresse verfügt und Sie sicherstellen möchten, dass die Benutzer die Anwendungen auf Ihrer neuen Instance weiterhin ohne

Unterbrechung verwenden können, müssen Sie die elastische IP-Adresse Ihrer neuen Instance zuordnen.

Eine Instance zu einer neuen Instance migrieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Sichern Sie alle Daten, die Sie weiter benötigen, wie folgt:
   - Stellen Sie eine Verbindung zu Ihrer Instance her und kopieren Sie die Daten auf Ihren Instance-Speicher-Volumes in den persistenten Speicher.
   - Erstellen Sie Snapshots Ihrer EBS-Volumes, damit Sie neue Volumes mit denselben Daten erstellen können, oder lösen Sie die Volumes von der ursprünglichen Instance, damit Sie sie an die neue Instance anhängen können.
3. Wählen Sie im Navigationsbereich Instances aus.
4. Wählen Sie Launch Instances aus. Gehen Sie beim Konfigurieren der Instance wie folgt vor:
   a. Wählen Sie ein AMI aus, das den von Ihnen gewünschten Instance-Typ unterstützt. Beispielsweise müssen Sie ein AMI auswählen, das den Prozessortyp des neuen Instance-Typs unterstützt. Außerdem erfordern die Instances der aktuellen Generation ein HVM-AMI.
   b. Wählen Sie den neuen Instance-Typ aus, den Sie starten möchten. Wenn der gewünschte Instance-Typ nicht verfügbar ist, ist er nicht mit der Konfiguration des ausgewählten AMI kompatibel.
   c. Wenn Sie erlauben wollen, dass der gleiche Datenverkehr die neue Instance erreicht, wählen Sie die Sicherheitsgruppe aus, die der ursprünglichen Instance zugeordnet ist.
   d. Wenn Sie mit der Konfiguration Ihrer neuen Instance fertig sind, wählen Sie ein Schlüsselpaar aus und starten Sie Ihre Instance. Es kann einige Minuten dauern, bis die Instance in den Zustand `running` übergeht.
5. Wenn Sie Daten auf einem EBS-Snapshot gesichert haben, erstellen Sie aus dem Snapshot ein Volume und fügen Sie das Volume dann der neuen Instance hinzu.

   Um ein EBS-Volume von der ursprünglichen Instance auf die neue Instance zu verschieben, trennen Sie das Volume von der ursprünglichen Instance und fügen Sie das Volume dann der neuen Instance hinzu.
6. Installieren Sie Ihre Anwendung und benötigte Software auf der neuen Instance.

7. Stellen Sie alle Daten wieder her, die Sie von den Instance-Speicher-Volumes der ursprünglichen Instance gesichert haben.
8. Wenn die ursprüngliche Instance über eine zugeordnete Elastic-IP-Adresse verfügt, sollten Sie sie der neuen Instance wie folgt zuordnen:

   a. Wählen Sie im Navigationsbereich Elastic aus IPs.
   b. Wählen Sie die Elastic IP-Adresse aus, die der ursprünglichen Instance zugeordnet ist, und wählen Sie dann Aktionen, Elastic IP-Adresszuordnung aufheben aus. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Zuordnung aufheben.
   c. Wählen Sie bei noch ausgewählter Elastic IP-Adresse Aktionen, Elastic IP-Adresse zuordnen aus.
   d. Wählen Sie für Resource type (Ressourcentyp) die Option Instance aus.
   e. Wählen Sie für Instance die neue Instance aus.
   f. (Optional) Geben Sie für Private IP address (Private IP-Adresse) eine private IP-Adresse an, mit der die Elastic IP-Adresse verknüpft werden soll.
   g. Wählen Sie Associate aus.
9. (Optional) Sie können die ursprüngliche Instance beenden, wenn sie nicht länger benötigt wird. Wählen Sie die Instance aus, stellen Sie sicher, dass Sie im Begriff sind, die ursprüngliche Instance und nicht die neue Instance zu beenden (überprüfen Sie beispielsweise den Namen oder die Startzeit), und wählen Sie dann Instance-Status, Instance beenden aus.

Problembehandlung beim Ändern des Instance-Typs

Verwenden Sie die folgenden Informationen, um Probleme zu diagnostizieren und zu beheben, die beim Ändern des Instance-Typs auftreten können.

Die Instance startet nach dem Ändern des Instance-Typs nicht

Mögliche Ursache: Anforderungen für neuen Instance-Typ nicht erfüllt

Wenn Ihre Instance nicht startet, ist es möglich, dass eine der Anforderungen für den neuen Instance-Typ nicht erfüllt wurde. Weitere Informationen finden Sie unter Warum startet meine Linux-Instance nicht, nachdem ich ihren Typ geändert habe?

Mögliche Ursache: AMI unterstützt den Instance-Typ nicht

Wenn Sie die EC2 Konsole verwenden, um den Instance-Typ zu ändern, sind nur die Instance-Typen verfügbar, die vom ausgewählten AMI unterstützt werden. Wenn Sie jedoch die verwenden,

AWS CLI um eine Instance zu starten, können Sie ein inkompatibles AMI und einen Instance-Typ angeben. Wenn das AMI und der Instance-Typ nicht kompatibel sind, kann die Instance nicht gestartet werden. Weitere Informationen finden Sie unter Kompatibilität zum Ändern des Instance-Typs.

Mögliche Ursache: Instance befindet sich in Cluster-Placement-Gruppe

Wenn sich Ihre Instance in einer Cluster-Placement-Gruppe befindet und die Instance nach dem Ändern des Instance-Typs nicht startet, versuchen Sie Folgendes:

1. Beenden Sie alle Instances in der Cluster-Placement-Gruppe.
2. Ändern Sie den Instance-Typ der betroffenen Instance.
3. Starten Sie alle Instances in der Cluster-Placement-Gruppe.

Anwendung oder Website nach Änderung des Instance-Typs nicht aus dem Internet erreichbar

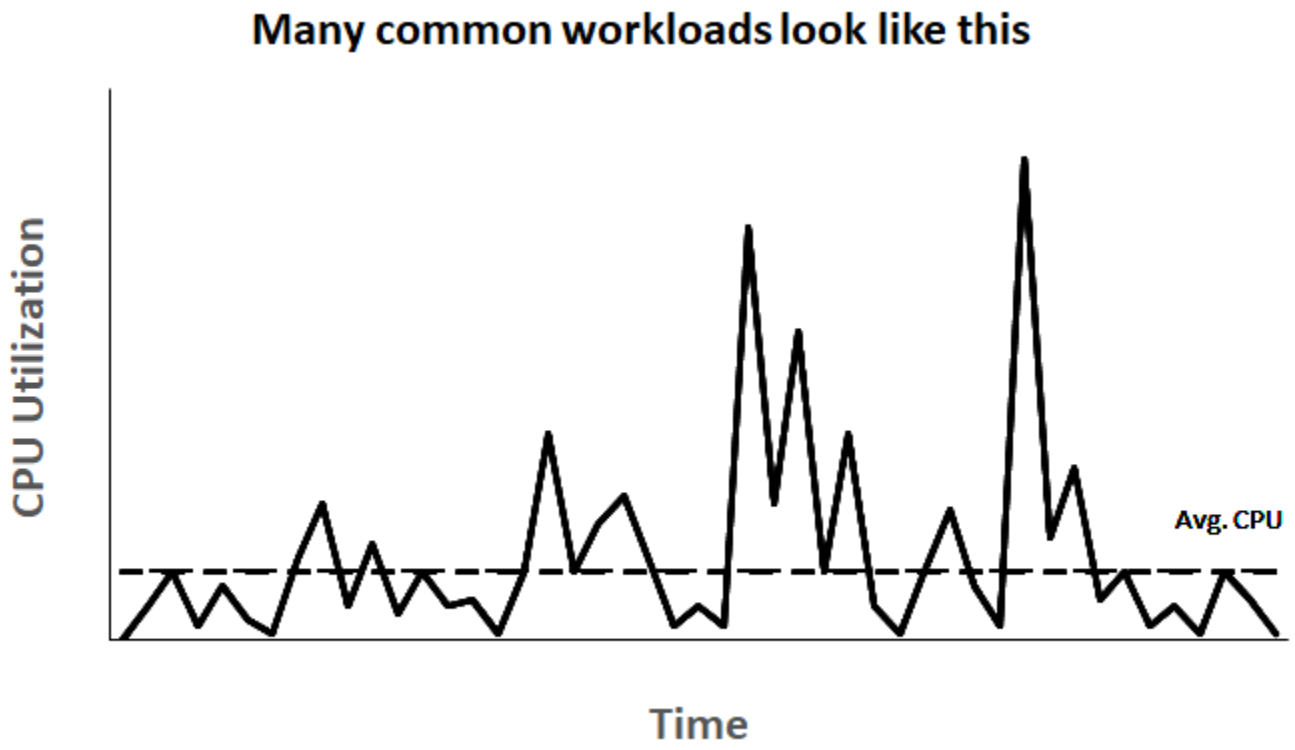
Mögliche Ursache: IPv4 Die öffentliche Adresse wurde veröffentlicht

Wenn Sie den Instance-Typ ändern, müssen Sie zuerst die Instance beenden. Wenn Sie eine Instance beenden, geben wir die öffentliche IPv4 Adresse frei und geben Ihrer Instance eine neue öffentliche IPv4 Adresse.

Um die öffentliche IPv4 Adresse zwischen den Stopps und Starts der Instance beizubehalten, empfehlen wir Ihnen, eine Elastic IP-Adresse ohne zusätzliche Kosten zu verwenden, sofern Ihre Instance läuft. Weitere Informationen finden Sie unter Elastic-IP-Adressen.

Burstable Performance Instances

Viele allgemeine Workloads sind im Durchschnitt nicht ausgelastet und erfordern keine hohe anhaltende CPU-Leistung. Die folgende Grafik veranschaulicht die CPU-Auslastung für viele gängige Workloads, die Kunden heute in der AWS Cloud ausführen.



Diese low-to-moderate CPU-Auslastung führt zu einer Verschwendung von CPU-Zyklen, sodass Sie für mehr bezahlen, als Sie nutzen. Um dies zu überwinden, können Sie die kostengünstigen universellen Burstable-Instances, die T-Instances, nutzen.

Die T-Instance-Familie bietet eine Baseline-CPU-Leistung mit der Möglichkeit, jederzeit und so lange wie erforderlich über die Baseline zu springen. Die Baseline-CPU ist so definiert, dass sie die Anforderungen der meisten universellen Workloads erfüllt, einschließlich großer Mikrodienste, Webserver, kleiner und mittlerer Datenbanken, Datenprotokollierung, Code-Repositorys, virtueller Desktops, Entwicklungs- und Testumgebungen sowie Geschäfts-kritische Anwendungen. Die T-Instances bieten ein ausgewogenes Verhältnis von Rechen-, Arbeitsspeicher- und Netzwerkressourcen und bieten Ihnen die kostengünstigste Möglichkeit, ein breites Spektrum an Allzweckanwendungen mit low-to-moderate CPU-Auslastung auszuführen. Sie können Ihnen im Vergleich zu M-Instances bis zu 15% an Kosten sparen und mit kleineren, wirtschaftlicheren Instance-Größen, die nur 2 V CPUs und 0,5 GiB Arbeitsspeicher bieten, zu noch mehr Kosteneinsparungen führen. Die kleineren T-Instance-Größen wie Nano, Micro, Small und Medium eignen sich gut für Workloads, die wenig Arbeitsspeicher benötigen und keine hohe CPU-Auslastung erwarten.

> **Note**
>
> In diesem Thema wird die Burst-fähige CPU beschrieben. Informationen zu Burst-fähiger Netzwerkleistung finden Sie unter Netzwerkbandbreite der EC2 Amazon-Instance.

EC2 Burstable-Instance-Typen

Die EC2 Burstable-Instances bestehen aus den Instance-Typen T4g, T3a und T3 sowie den T2-Instance-Typen der vorherigen Generation.

Die T4G-Instance-Typen sind die neueste Generation von Burstable-Instances. Sie bieten das beste Preis-Leistungs-Verhältnis und bieten Ihnen die niedrigsten Kosten aller Instance-Typen. EC2 Die T4G-Instance-Typen werden von ARM-basierten AWS Graviton2-Prozessoren angetrieben und bieten umfassende Ökosystemunterstützung durch Betriebssystemanbieter, unabhängige Softwareanbieter und beliebte Dienste und Anwendungen. AWS

Die folgende Tabelle fasst die wichtigsten Unterschiede zwischen den Burstable-Instance-Typen zusammen.

Typ	Beschreibung	Prozessorfamilie
Neueste Generation		
T4g	Der kostengünstigste EC2 Instance-Typ mit bis zu 40% höheren price/performance und 20% niedrigeren Kosten als T3	AWS Graviton2-Prozessoren mit Arm Neoverse N1-Kernen
T3a	Kostengünstigste x86-basierte Instances mit 10 % geringere n Kosten im Vergleich zu T3-Instances	AMD-EPYC-Prozessoren der 1. Generation
T3	Beste Spitzenleistung price/ performance für x86-Workl oads mit bis zu 30% weniger als bei T2-Instances der	Intel Xeon Scalable (Skylake, Cascade-Lake-Prozessoren)

Typ	Beschreibung	Prozessorfamilie
	vorherigen Generation price/ performance	
Vorherige Generation		
T2	Burstable-Instances der vorherigen Generation	Intel-Xeon-Prozessoren

Informationen zu Instance-Preisen und zusätzlichen Spezifikationen finden Sie unter EC2 Amazon-Preise und EC2 Amazon-Instance-Typen. Informationen zu Burst-fähiger Netzwerkleistung finden Sie unter Netzwerkbandbreite der EC2 Amazon-Instance.

Wenn Sie Ihre AWS-Konto vor dem 15. Juli 2025 erstellt haben und sie weniger als 12 Monate alt ist, können Sie eine `t2.micro` Instance innerhalb bestimmter Nutzungslimits kostenlos nutzen (oder eine `t3.micro` Instance in Regionen, in denen sie nicht verfügbar `t2.micro` ist). Wenn du deine Instance-Typen AWS-Konto am oder nach dem 15. Juli 2025 erstellt hast, kannst dut`3.micro`,`t3.small`,`t4g.micro`, `t4g.small` Instance-Typen 6 Monate lang verwenden oder bis dein Guthaben aufgebraucht ist. Weitere Informationen finden Sie unter Kostenloses AWS-Kontingent.

Unterstützte Kaufoptionen für T-Instances

- On-Demand Instances
- Reserved Instances
- Dedicated Instances (nur T3)
- Dedicated Hosts (nur T3, nur in `standard`-Modus)
- Spot Instances

Weitere Informationen finden Sie unter EC2 Abrechnungs- und Kaufoptionen von Amazon.

Inhalt

- Bewährte Methoden
- Schlüsselkonzepte und Definitionen für Instances mit Spitzenlastleistung
- Unbegrenzter Modus für Burstable Performance Instances

- Standardmodus für Instances mit Spitzenlastleistung
- Instances mit Spitzenlastleistung konfigurieren
- CPU-Guthaben auf Instances mit Spitzenlastleistung überwachen

Bewährte Methoden

Folgen Sie diesen bewährten Methoden, um Burstable Performance Instances mit größtmöglichem Nutzen zu verwenden.

- Stellen Sie sicher, dass die gewählte Größe der Instance die Speicher-Mindestanforderungen Ihres Betriebssystems und Ihrer Anwendungen erfüllt. Betriebssysteme mit grafischen Benutzeroberflächen, die deutlich mehr Speicher und CPU-Ressourcen verbrauchen (z. B. Windows), erfordern möglicherweise eine `t3.micro`- oder eine noch größere Instance-Größe für viele Anwendungsfälle. Da die Speicher- und CPU-Anforderungen Ihrer Workload im Laufe der Zeit wachsen, haben Sie mit den T-Instances die Flexibilität, auf größere Instance-Größen desselben Instance-Typs zu skalieren oder einen anderen Instance-Typ auszuwählen.
- Aktivieren Sie AWS Compute Optimizer für Ihr Konto und überprüfen Sie die Compute-Optimizer-Empfehlungen für Ihre Workload. Compute Optimizer kann bei der Beurteilung helfen, ob Instances zur Verbesserung der Leistung vergrößert oder zur Kosteneinsparung verkleinert werden sollten. Compute Optimizer empfiehlt möglicherweise auch einen anderen Instance-Typ basierend auf Ihrem Szenario. Weitere Informationen finden Sie im AWS Compute Optimizer Benutzerhandbuch unter EC2Instanzempfehlungen anzeigen.

Schlüsselkonzepte und Definitionen für Instances mit Spitzenlastleistung

Herkömmliche EC2 Amazon-Instance-Typen bieten feste CPU-Ressourcen, während Instances mit hoher Leistung eine grundlegende CPU-Auslastung bieten und die Möglichkeit bieten, die CPU-Auslastung über dem Basisniveau zu erhöhen. Dadurch wird sichergestellt, dass Sie nur für die Basis-CPU zuzüglich einer zusätzlichen Burst-CPU-Nutzung zahlen, was zu geringeren Rechenkosten führt. Die Basisauslastung und die Steigerbarkeit werden über das CPU-Guthaben verwaltet. Burstable Performance Instances sind die einzigen Instance-Typen, die CPU-Guthaben für die CPU-Nutzung verwenden.

Jede Burstable Performance Instance erhält kontinuierlich Guthaben, wenn sie unter der CPU-Baseline bleibt, und gibt kontinuierlich Guthaben aus, wenn sie über der Baseline liegt. Die Höhe des verdienten oder ausgegebenen Guthabens hängt von der CPU-Auslastung der Instance ab:

- Wenn die CPU-Auslastung unter dem Ausgangswert liegt, sind die verdienten Guthaben höher als die ausgegebenen Guthaben.
- Wenn die CPU-Auslastung der Baseline entspricht, entsprechen die verdienten Guthaben den ausgegebenen Guthaben.
- Wenn die CPU-Auslastung höher als der Basiswert ist, sind die ausgegebenen Guthaben höher als die verdienten Guthaben

Wenn das verdiente Guthaben höher ist als das ausgegebene Guthaben, wird die Differenz als aufgelaufenes Guthaben bezeichnet, das später verwendet werden kann, um die CPU-Basisauslastung zu überschreiten. Wenn das ausgegebene Guthaben höher ist als das verdiente Guthaben, hängt das Verhalten der Instance ebenfalls vom Guthaben-Konfigurationsmodus ab – Standardmodus oder unbegrenzter Modus.

Wenn im Standardmodus das ausgegebene Guthaben höher ist als das verdiente Guthaben, verwendet die Instance das angesammelte Guthaben, um die CPU-Basisauslastung zu überschreiten. Wenn keine angesammelten Guthaben mehr vorhanden sind, sinkt die Instance allmählich auf die Baseline-CPU-Auslastung und kann nicht über die Baseline hinausgehen, bis mehr Guthaben angesammelt wird.

Wenn die Instance im unbegrenzten Modus über die Baseline-CPU-Auslastung hinausgeht, verwendet die Instance zuerst die aufgelaufenen Guthaben für das Burst. Wenn keine angesammelten Guthaben übrig sind, gibt die Instance das überschüssige Guthaben für das Burst aus. Wenn ihre CPU-Nutzung die Baseline unterschreitet, verwendet sie die verdienten CPU-Guthaben, um die zuvor verbrauchten überzähligen Guthaben wieder zurückzuzahlen. Durch die Möglichkeit, CPU-Guthaben zu sammeln, um überschüssige Credits zurückzuzahlen EC2 , kann Amazon die durchschnittliche CPU-Auslastung einer Instance über einen Zeitraum von 24 Stunden ermitteln. Wenn die durchschnittliche CPU-Auslastung über einen Zeitraum von 24 Stunden die Grundkapazität übersteigt, wird der Instance die zusätzliche Nutzung zu einer pauschalen Zusatzgebühr pro vCPU-Stunde in Rechnung gestellt.

Inhalt

- Die wichtigsten Konzepte und Definitionen
- Verdienen von CPU-Guthaben
- Erwerbsrate von CPU-Guthaben
- Limit für die Ansammlung von CPU-Guthaben
- Lebensdauer des angefallenen CPU-Guthabens

- Basisauslastung

Die wichtigsten Konzepte und Definitionen

Die folgenden Schlüsselkonzepte und Definitionen gelten für Burstable Performance Instances.

CPU-Auslastung

Die CPU-Auslastung ist der Prozentsatz der zugewiesenen EC2 Recheneinheiten, die derzeit auf der Instance verwendet werden. Diese Metrik misst den Prozentsatz der zugewiesenen CPU-Zyklen, die auf einer Instance verwendet werden. Die CloudWatch Metrik CPU-Auslastung zeigt die CPU-Auslastung pro Instanz und nicht die CPU-Auslastung pro Kern. Die Baseline-CPU-Spezifikation einer Instance basiert auch auf der CPU-Auslastung pro Instance. Informationen zur Messung der CPU-Auslastung mit AWS-Managementkonsole oder dem AWS CLI finden Sie unterAbrufen von Statistiken für eine bestimmte Instance.

CPU-Guthaben

Eine Einheit von vCPU-Zeit.

Beispiele:

1 CPU-Guthaben = 1 vCPU * 100 % Auslastung * 1 Minute.

1 CPU-Guthaben = 1 vCPU * 50 % Auslastung * 2 Minuten.

1 CPU-Guthaben = 2 vCPU * 25 % Auslastung * 2 Minuten.

Basisauslastung

Die Basisauslastung ist die Ebene, auf der die CPU für ein Nettoguthaben von Null genutzt werden kann, wenn die Anzahl der verdienten CPU-Guthaben mit der Anzahl der verwendeten CPU-Guthaben übereinstimmt. Die Basisauslastung wird auch als Baseline bezeichnet. Die Basisauslastung wird als Prozentsatz der vCPU-Auslastung ausgedrückt, der wie folgt berechnet wird: Basisauslastung% = (Anzahl der Credits earned/number von vCPUs) /60 Minuten.

Informationen zur Basisauslastung der einzelnen Burstable Performance Instances finden Sie in der Guthabentabelle.

Erworbenes Guthaben

Guthaben, die von einer Instance kontinuierlich gesammelt werden, wenn sie ausgeführt wird.

Anzahl der pro Stunde verdienten Credits =% Basisauslastung x Anzahl der CPUs v* 60 Minuten

Beispiel:

Ein t3.nano mit 2 V CPUs und einer Basisauslastung von 5% verdient 6 Credits pro Stunde, berechnet wie folgt:

2 v CPUs * 5% Basiswert * 60 Minuten = 6 Credits pro Stunde

Ausgelaufene oder genutzte Guthaben

Guthaben, die von einer Instance kontinuierlich genutzt werden, wenn sie ausgeführt wird.

Pro Minute ausgegebene CPU-Guthaben = Anzahl von v CPUs * CPU-Auslastung x 1 Minute

Angesammelte Guthaben

Nicht ausgegebene CPU-Guthaben, wenn eine Instance weniger Guthaben benötigt, als für die Baseline-Auslastung erforderlich ist. Mit anderen Worten, aufgelaufene Guthaben = (verdiente Guthaben – Verwendete Guthaben) unterhalb der Basislinie.

Beispiel:

Wenn ein t3.nano mit einer CPU-Auslastung von 2 % läuft, die für eine Stunde unter der Baseline von 5 % liegt, werden die aufgelaufenen Guthaben wie folgt berechnet:

Aufgelaufene CPU-Guthaben = (Verdiente Credits pro Stunde — Verwendete Credits pro Stunde) = 6 — 2 v CPUs * 2% CPU-Auslastung * 60 Minuten = 6 — 2,4 = 3,6 aufgelaufene Credits pro Stunde

Guthabenansammlungslimit

Hängt von der Instance-Größe ab, ist aber im Allgemeinen gleich der Anzahl der maximalen Guthaben, die in 24 Stunden verdient wurden.

Beispiel:

Für t3.nano, das Kreditabgrenzungslimit = 24 * 6 = 144 Guthaben

Startguthaben

Gilt nur für T2-Instances, die für den Standardmodus konfiguriert sind. Startguthaben sind eine begrenzte Anzahl von CPU-Guthaben, die einer neuen T2-Instance zugewiesen werden, damit sie beim Start im Standardmodus über die Baseline hinausgehen kann.

Überschüssiges Guthaben

Guthaben, die von einer Instance ausgegeben werden, nachdem sie ihr angesammeltes Guthaben aufgebraucht hat. Das überschüssige Guthaben ist für Burstable-Instances ausgelegt,

um eine hohe Leistung über einen längeren Zeitraum aufrechtzuerhalten und werden nur im unbegrenzten Modus verwendet. Das überschüssige Guthaben wird verwendet, um zu bestimmen, wie viele Guthaben von der Instance für Burst im unbegrenzten Modus verwendet wurden.

Standardmodus

Der Guthaben-Konfigurationsmodus, der es einer Instance ermöglicht, über die Baseline zu springen, indem sie Guthaben ausgibt, die sie in ihrem Guthabenstand angesammelt hat.

Unbegrenzter Modus

Guthaben-Konfigurationsmodus, der es einer Instance ermöglicht, über die Baseline zu springen, indem sie bei Bedarf eine hohe CPU-Auslastung für einen beliebigen Zeitraum aufrechterhält. Der Instance-Stundenpreis deckt alle CPU-Nutzungsspitzen automatisch ab, wenn die durchschnittliche CPU-Nutzung der Instance in einem fortlaufendem 24-Stunden-Zeitraum oder über die Lebensdauer der Instance hinweg (es gilt der jeweils kürzere Zeitraum) bei oder unterhalb der Baseline liegt. Wenn die Instance für einen längeren Zeitraum mit einer höheren CPU-Nutzung ausgeführt wird, kann sie dies für eine pauschale Zusatzgebühr pro vCPU-Stunde tun.

In der folgenden Tabelle werden die wichtigsten Guthaben-Unterschiede zwischen den Burstable-Instance-Typen zusammengefasst.

Typ	Art der unterstützten CPU-Guthaben	Modi zur Konfiguration des Guthabens	Die Lebensdauer des aufgelaufenen CPU-Guthabens zwischen Instance- Starts und -Stopps
Neueste Generation			
T4g	Verdiente Guthaben, aufgelaufene Guthaben, ausgegebene Guthaben, überschüssige Guthaben (nur im unbegrenzten Modus)	Standard, Unbegrenzt (Standard)	7 Tage (Guthaben bleiben 7 Tage lang bestehen, nachdem eine Instance gestoppt wurde)

Typ	Art der unterstützten CPU-Guthaben	Modi zur Konfiguration des Guthabens	Die Lebensdauer des aufgelaufenen CPU-Guthabens zwischen Instance- Starts und -Stopps
T3a	Verdiente Guthaben, aufgelaufene Guthaben, ausgegebene Guthaben, überschüssige Guthaben (nur im unbegrenzten Modus)	Standard, Unbegrenzt (Standard)	7 Tage (Guthaben bleiben 7 Tage lang bestehen, nachdem eine Instance gestoppt wurde)
T3	Verdiente Guthaben, aufgelaufene Guthaben, ausgegebene Guthaben, überschüssige Guthaben (nur im unbegrenzten Modus)	Standard, Unbegrenzt (Standard)	7 Tage (Guthaben bleiben 7 Tage lang bestehen, nachdem eine Instance gestoppt wurde)
Vorherige Generation			
T2	Verdiente Guthaben, aufgelaufene Guthaben, ausgegebene Guthaben, Startguthaben (nur im Standardmodus), überschüssige Guthaben (nur im unbegrenzten Modus)	Standard (standard), Unbegrenzt	0 Tage (Guthaben gehen verloren, wenn eine Instance stoppt)

> **Note**
>
> Unbegrenzter Modus wird für T3-Instances, die auf einem Dedicated Host gestartet werden, nicht unterstützt.

Verdienen von CPU-Guthaben

Jede Burstable Performance Instance erhält kontinuierlich (mit einer Auflösung in Millisekunden) einen festgelegten Satz an CPU-Guthaben pro Stunde, der von der Instance-Größe abhängt. Der Berechnungsprozess dafür, ob Guthaben angesammelt oder verbraucht wird, geschieht ebenfalls in Millisekunden. Sie müssen sich also keine Sorgen machen, dass Sie zu viel CPU-Guthaben verbrauchen; durch eine kurzzeitige CPU-Steigerung wird nur ein Bruchteil des CPU-Guthabens verbraucht.

Wenn eine Burstable Performance Instance weniger CPU-Ressourcen verwendet, als für die Basisauslastung erforderlich ist (z. B. im Leerlauf), werden die nicht verbrauchten CPU-Guthaben dem CPU-Guthabenkonto gutgeschrieben. Benötigt eine Burstable Performance Instance eine höhere als die Basisauslastung, gibt sie die angesammelten Guthaben aus. Je mehr Guthaben sich für Ihre Burstable Performance Instance angesammelt hat, desto länger kann die Leistung über die Basisleistung hinaus gesteigert werden, wenn mehr CPU-Auslastung benötigt wird.

In der folgenden Tabelle sind die Instance-Typen mit Burstable-Performance, die Rate, mit der CPU-Guthaben pro Stunde verdient werden, die maximale Anzahl an verdienten CPU-Gutschriften, die eine Instance sammeln kann, die Anzahl von v CPUs pro Instance und die Basisauslastung als Prozentsatz eines vollen Kerns (mit einer einzelnen vCPU) aufgeführt.

Instance-Typ	Pro Stunde erworbenes CPU-Guthaben	Maximal verdiente Guthaben, die angesammelt werden können*	v *** CPUs	Basisauslastung pro vCPU
T2				
`t2.nano`	3	72	1	5 %
`t2.micro`	6	144	1	10 %
`t2.small`	12	288	1	20 %

Instance-Typ	Pro Stunde erworbenes CPU-Guthaben	Maximal verdiente Guthaben, die angesammelt werden können*	v *** CPUs	Basisauslastung pro vCPU
t2.medium	24	576	2	20 %**
t2.large	36	864	2	30 %**
t2.xlarge	54	1 296	4	22,5 %**
t2.2xlarge	81,6	1 958,4	8	17 %**
T3				
t3.nano	6	144	2	5 %**
t3.micro	12	288	2	10 %**
t3.small	24	576	2	20 %**
t3.medium	24	576	2	20 %**
t3.large	36	864	2	30 %**
t3.xlarge	96	2 304	4	40 %**
t3.2xlarge	192	4 608	8	40 %**
T3a				
t3a.nano	6	144	2	5 %**
t3a.micro	12	288	2	10 %**
t3a.small	24	576	2	20 %**
t3a.medium	24	576	2	20 %**
t3a.large	36	864	2	30 %**

Instance-Typ	Pro Stunde erworbenes CPU-Guthaben	Maximal verdiente Guthaben, die angesammelt werden können*	v *** CPUs	Basisauslastung pro vCPU
t3a.xlarge	96	2 304	4	40 %**
t3a.2xlarge	192	4 608	8	40 %**
T4g				
t4g.nano	6	144	2	5 %**
t4g.micro	12	288	2	10 %**
t4g.small	24	576	2	20 %**
t4g.medium	24	576	2	20 %**
t4g.large	36	864	2	30 %**
t4g.xlarge	96	2 304	4	40 %**
t4g.2xlarge	192	4 608	8	40 %**

* Die Anzahl der Guthaben, die angesammelt werden können, entspricht dem Guthaben, das in einem 24-Stunden-Zeitraum verdient werden kann.

** Die prozentuale Basisauslastung in der Tabelle angegeben pro vCPU In CloudWatch wird die CPU-Auslastung pro vCPU angezeigt. Beispielsweise wird die CPU-Auslastung für eine `t3.large` Instance, die auf der Basisebene betrieben wird, in den CloudWatch CPU-Metriken mit 30% angegeben. Weitere Informationen zum Berechnen der Basisauslastung finden Sie unter Basisauslastung.

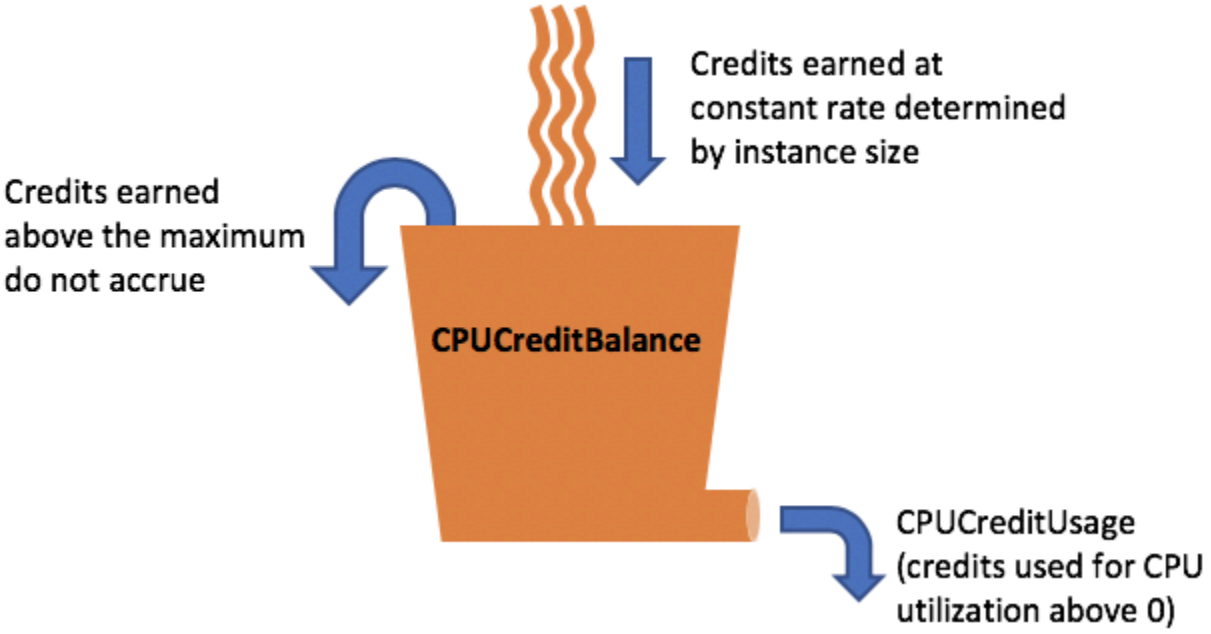
*** Jede vCPU ist ein Thread entweder eines Intel-Xeon-Kerns oder eines AMD-EPYC-Kerns, mit Ausnahme von T2- -Instances.

Erwerbsrate von CPU-Guthaben

Die Anzahl des pro Stunde erworbenen CPU-Guthabens wird anhand der Instance-Größe bestimmt. So erwirbt ein `t3.nano` z. B. sechs Guthaben pro Stunde, während ein `t3.small` 24 Guthaben pro Stunde erwirbt. Die oben stehende Tabelle listet die Guthaben-Erwerbsrate für alle Instances auf.

Limit für die Ansammlung von CPU-Guthaben

Während verdiente Guthaben für eine in Ausführung befindliche Instance nie ablaufen können, gibt es ein Limit für die Anzahl von Guthaben, die eine Instance ansammeln kann. Das Limit wird durch das CPU-Guthaben-Kontostand-Limit festgelegt. Nach Erreichen des Limits werden neu verdiente Guthaben verworfen, wie in folgendem Image angegeben. Der volle Bucket zeigt das CPU-Guthaben-Kontostand-Limit an, und der Überlauf zeigt neu verdiente Guthaben an, die das Limit überschreiten.



Das Limit für das CPU-Guthabenkonto ist von der jeweiligen Größe der jeweiligen -Instance abhängig. Beispielsweise kann eine `t3.micro`-Instance maximal 288 verdiente CPU-Guthaben auf dem CPU-Guthaben-Konto ansammeln. Die oben stehende Tabelle listet die Höchstzahl der verdienten Guthaben auf, die jede -Instance ansammeln kann.

T2-Standard-Instances verdienen zudem Startguthaben. Das Startguthaben wird dem Limit für das CPU-Guthaben-Konto nicht angerechnet. Wenn eine T2-Instance ihr Startguthaben nicht ausgegeben hat und für einen Zeitraum von 24 Stunden im Leerlauf verbleibt, während verdiente Guthaben angesammelt werden, erscheint sein CPU-Guthaben-Konto über dem Limit. Weitere Informationen finden Sie unter Startguthaben.

T4g-, T3a- und T3-Instances verdienen kein Startguthaben. Diese Instances werden standardmäßig als `unlimited` gestartet und können daher die Leistung sofort beim Start steigern, ohne dass Startguthaben erforderlich wäre. T3-Instances, die auf einem Dedicated Host standardmäßig als `standard` gestartet werden; `unlimited`-Modus wird für T3-Instances auf einem Dedicated Host nicht unterstützt.

Lebensdauer des angefallenen CPU-Guthabens

CPU-Guthaben für eine laufende Instance verfallen nicht.

Der CPU-Guthaben-Kontostand bleibt zwischen dem Anhalten und Starten einer Instance für T2 jedoch nicht erhalten. Wenn Sie eine T2-Instance anhalten, verliert die Instance alle angesammelten Guthaben.

Für T4g, T3a und T3 bleibt der CPU-Guthaben-Kontostand sieben Tage nach dem Anhalten einer Instance erhalten. Danach verfällt das Guthaben. Falls Sie die Instance innerhalb von sieben Tagen starten, geht kein Guthaben verloren.

Weitere Informationen finden Sie unter `CPUCreditBalance` in der CloudWatch -Metriktabelle.

Basisauslastung

Die Basisauslastung ist die Ebene, auf der die CPU für ein Nettoguthaben von Null genutzt werden kann, wenn die Anzahl der verdienten CPU-Guthaben mit der Anzahl der verwendeten CPU-Guthaben übereinstimmt. Die Basisauslastung wird auch als Baseline bezeichnet.

Die Basisauslastung wird als Prozentsatz der vCPU-Auslastung ausgedrückt, die wie folgt berechnet wird:

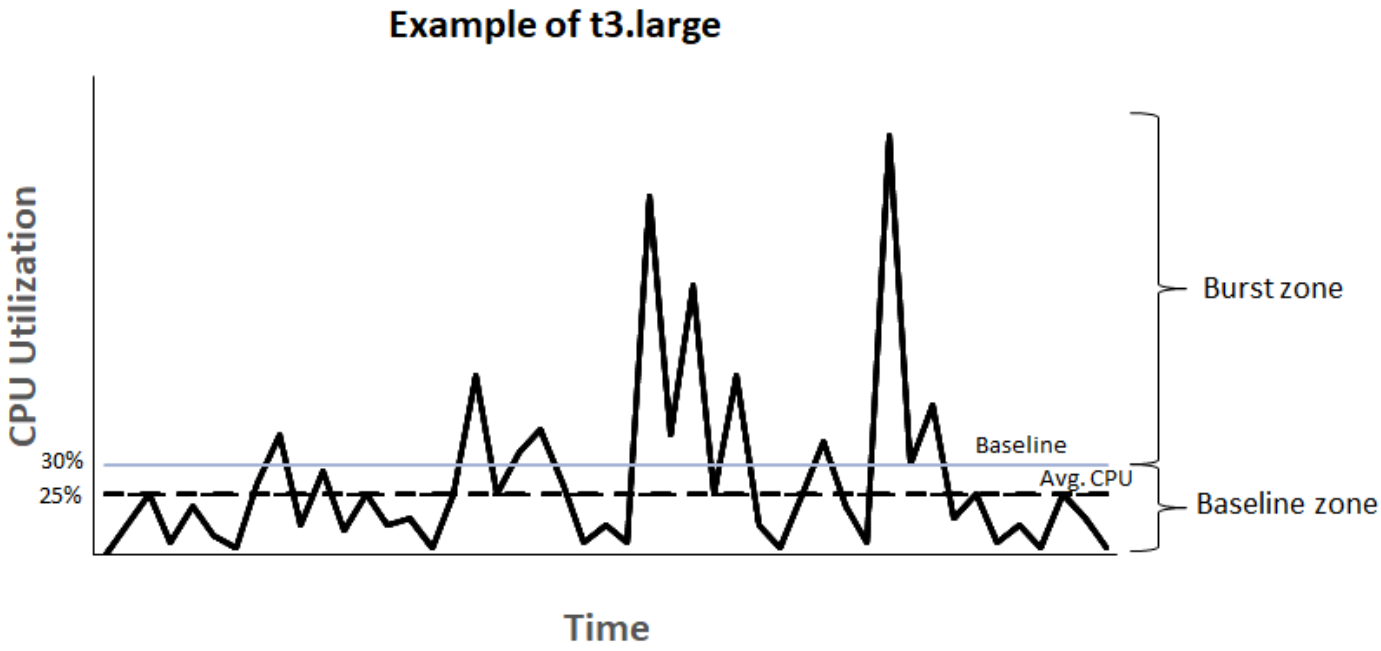
```
(number of credits earned/number of vCPUs)/60 minutes = % baseline
utilization
```

Beispielsweise verdient eine `t3.nano` Instance mit 2 V CPUs 6 Credits pro Stunde, was zu einer Basisauslastung von 5% führt, die wie folgt berechnet wird:

```
(6 credits earned/2 vCPUs)/60 minutes = 5% baseline utilization
```

Eine `t3.large` Instance mit 2 V CPUs verdient 36 Credits pro Stunde, was einer Basisauslastung von 30% () `(36/2)/60` entspricht.

Das folgende Diagramm zeigt ein Beispiel für eine `t3.large` mit einer durchschnittlichen CPU-Auslastung unterhalb der Baseline.



Unbegrenzter Modus für Burstable Performance Instances

Eine als `unlimited` konfigurierte Burstable Performance Instance kann eine hohe CPU-Auslastung je nach Bedarf in jedem erforderlichen Zeitraum aufrechterhalten. Der Instance-Stundenpreis deckt alle CPU-Nutzungsspitzen automatisch ab, wenn die durchschnittliche CPU-Nutzung der Instance in einem fortlaufendem 24-Stunden-Zeitraum oder über die Lebensdauer der Instance hinweg (es gilt der jeweils kürzere Zeitraum) bei oder unterhalb der Baseline liegt.

Für eine Mehrzahl von allgemeinen Workloads bieten als `unlimited` konfigurierte Instances ausreichend Leistung ohne zusätzliche Gebühren. Wenn die Instance für einen längeren Zeitraum mit einer höheren CPU-Nutzung ausgeführt wird, kann sie dies zu einer pauschalen Zusatzgebühr pro vCPU-Stunde tun.

Wenn Sie Ihre Instance AWS-Konto vor dem 15. Juli 2025 erstellt haben und eine `t2.micro`t3.micro Oder-Instance im Rahmen des Kostenloses AWS-KontingentAngebots und im `unlimited` Modus verwenden, können Gebühren anfallen, wenn Ihre durchschnittliche Auslastung über einen fortlaufenden Zeitraum von 24 Stunden die Basisnutzung der Instance übersteigt.

T4g-, T3a- und T3-Instances werden standardmäßig als `unlimited` gestartet (sofern Sie nicht die Standardeinstellung ändern). Wenn die durchschnittliche CPU-Auslastung über einen Zeitraum von 24 Stunden den Basiswert überschreitet, werden ebenso Gebühren für überschüssiges Guthaben anfallen. Wenn Sie Spot-Instances als `unlimited` starten und planen, sie sofort und für eine kurze

Dauer ohne Leerlaufzeit für die Anrechnung von CPU-Guthaben zu verwenden, werden Gebühren für überschüssiges Guthaben entstehen. Wir empfehlen Ihnen, Spot-Instances im Standardmodus zu starten, um höhere Kosten zu vermeiden. Weitere Informationen finden Sie unter Für überzähliges Guthaben können Gebühren anfallen und Instances mit Spitzenlastleistung starten.

> **Note**
>
> T3-Instances, die auf einem Dedicated Host standardmäßig als `standard` gestartet werden; `unlimited`-Modus wird für T3-Instances auf einem Dedicated Host nicht unterstützt.

Inhalt

- Konzepte zum unbegrenzten Modus für Instances mit Spitzenlastleistung
  - Funktionsweise der Unlimited Burstable Performance Instances
  - Verwendung des unbegrenzten Modus im Vergleich zu einer festen CPU
  - Für überzähliges Guthaben können Gebühren anfallen
  - Wie viel kostet unbegrenzte Spitzenlastleistung?
  - Kein Startguthaben für T2 Unlimited-Instances
  - Unbegrenzten Modus aktivieren
  - Was passiert mit dem Guthaben beim Wechsel zwischen unbegrenzt und Standard?
  - Überwachen der Guthabennutzung
- Unbegrenzter Modus für Instances mit Spitzenlastleistung
  - Beispiel 1: Beschreiben des Guthabenverbrauchs mit T3 Unlimited
  - Beispiel 2: Beschreiben des Guthabenverbrauchs mit T2 Unlimited

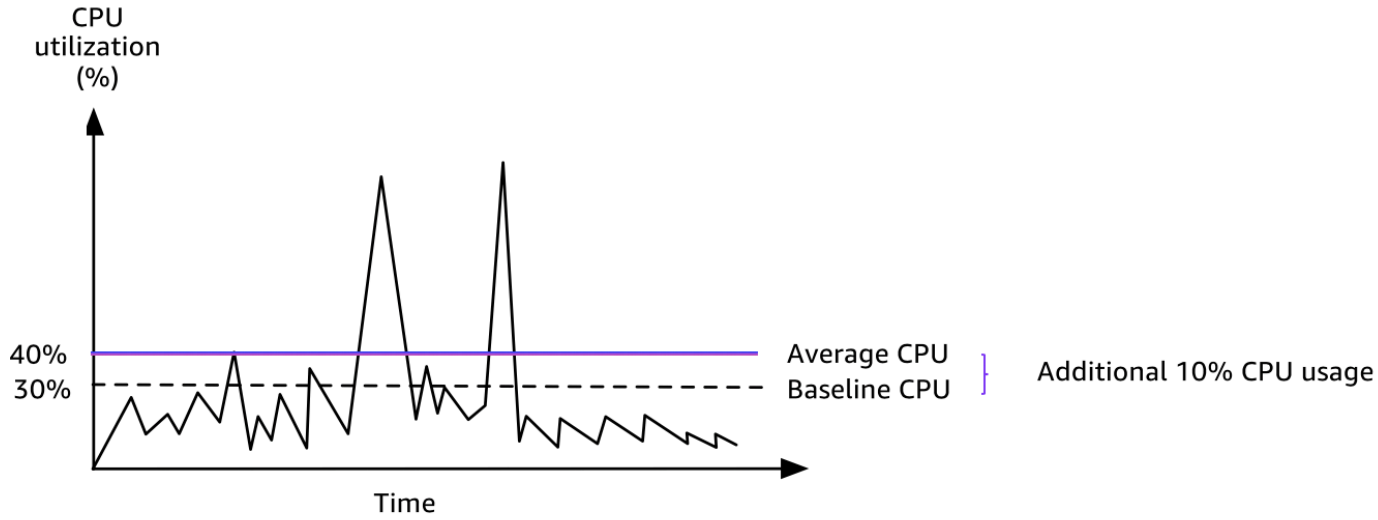
Konzepte zum unbegrenzten Modus für Instances mit Spitzenlastleistung

Der `unlimited`-Modus ist eine Guthabenkonfigurationsoption für Burstable Performance Instances. Er kann jederzeit für eine laufende oder angehaltene Instance aktiviert oder deaktiviert werden. Sie können diese Option auf Kontoebene pro AWS Region und pro Instance-Familie mit Burstable-Performance `unlimited` als Standardoption festlegen, sodass alle neuen Burstable-Performance-Instances im Konto mit der Standard-Kreditoption gestartet werden.

Funktionsweise der Unlimited Burstable Performance Instances

Wenn eine Burstable Performance Instance, die als `unlimited` konfiguriert ist, ihr CPU-Guthaben aufgebraucht hat, kann sie überzählige Guthaben verbrauchen, um die Leistung über die Baseline hinaus zu steigern. Wenn ihre CPU-Nutzung die Baseline unterschreitet, verwendet sie die verdienten CPU-Guthaben, um die zuvor verbrauchten überzähligen Guthaben wieder zurückzuzahlen. Durch die Möglichkeit, CPU-Guthaben zu sammeln, um überschüssige Credits zurückzuzahlen EC2 , kann Amazon die durchschnittliche CPU-Auslastung einer Instance über einen Zeitraum von 24 Stunden ermitteln. Wenn die durchschnittliche CPU-Auslastung über einen Zeitraum von 24 Stunden die Grundkapazität übersteigt, wird der Instance die zusätzliche Nutzung zu einer pauschalen Zusatzgebühr pro vCPU-Stunde in Rechnung gestellt.

Das folgende Diagramm zeigt die CPU-Nutzung einer `t3.large`. Die CPU-Basisnutzung für eine `t3.large` ist 30 %. Wenn die Instance über einen Zeitraum von 24 Stunden mit einer CPU-Basisnutzung von durchschnittlich 30 % oder weniger ausgeführt wird, fallen keine zusätzlichen Gebühren an, da die Kosten bereits vom Stundenpreis der Instance abgedeckt werden. Wenn die Instance über einen Zeitraum von 24 Stunden jedoch mit einer CPU-Basisnutzung von durchschnittlich 40 % ausgeführt wird (siehe Diagramm), wird der Instance die zusätzliche CPU-Auslastung von 10 % zu einer pauschalen Zusatzgebühr pro vCPU-Stunde in Rechnung gestellt.



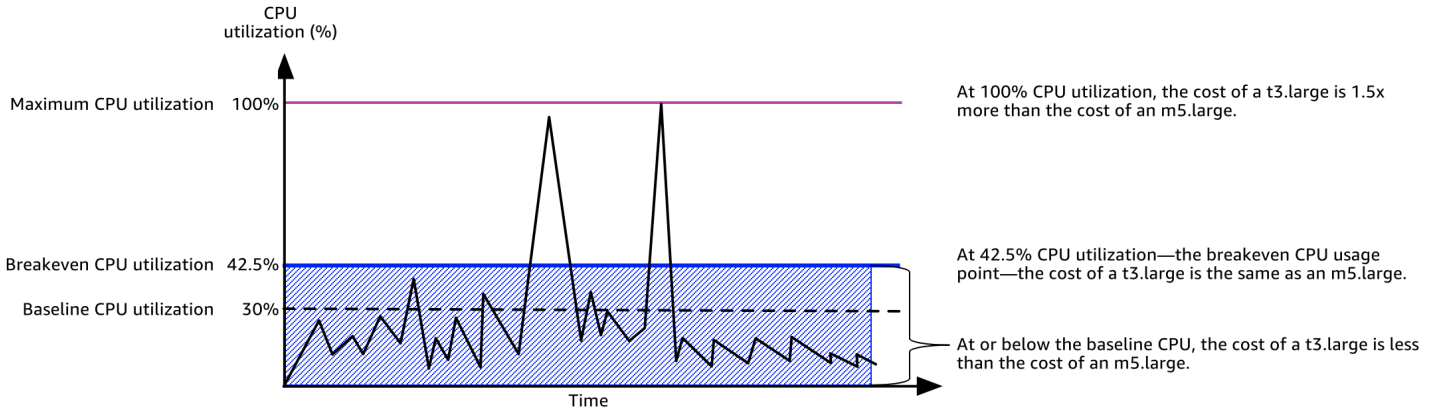
Weitere Informationen zur Basisauslastung pro vCPU für jeden Instance-Typ und dazu, wie viel Guthaben jeder Instance-Typ erwirbt, finden Sie in der Guthabentabelle.

Verwendung des unbegrenzten Modus im Vergleich zu einer festen CPU

Bei der Entscheidung, ob eine Burstable Performance Instances im `unlimited`-Modus, wie eine T3 oder eine Instance mit fester Leistung, wie eine M5, verwendet werden soll, müssen Sie den Break Even der CPU-Auslastung bestimmen. Der Break Even der CPU-Nutzung für eine Burstable Performance Instance ist der Punkt, an dem eine Burstable Performance Instance genauso günstig ist wie eine Instance mit fester Leistung. Anhand des Break Even der CPU-Nutzung können Sie Folgendes bestimmen:

- Wenn die durchschnittliche CPU-Nutzung in einem Zeitraum von 24 Stunden beim oder unterhalb des Break Even der CPU-Nutzung liegt, verwenden Sie eine Burstable Performance Instance im `unlimited`-Modus, sodass Sie vom niedrigeren Preis einer Burstable Performance Instance profitieren können, während Sie die gleiche Leistung wie bei einer Instance mit fester Leistung erhalten.
- Wenn die durchschnittliche CPU-Nutzung über einen Zeitraum von 24 Stunden oberhalb des Break Even der CPU-Nutzung liegt, kostet die Burstable Performance Instance mehr als die Instance mit fester Leistung gleicher Größe. Wenn eine T3-Instance kontinuierlich Spitzen bei 100 % CPU erreicht, zahlen etwa 1,5 Mal mehr als für eine M5-Instance der gleichen Größe.

Das folgende Diagramm zeigt den Break Even-CPU-Nutzungspunkt, an dem eine `t3.large` gleich viel kostet wie eine `m5.large`. Der Break Even-CPU-Nutzungspunkt für eine `t3.large` ist 42,5 %. Wenn die durchschnittliche CPU-Nutzung bei 42,5 % liegt, kostet das Ausführen von `t3.large` und `m5.large` das Gleiche, und es ist teurer, wenn die durchschnittliche CPU-Nutzung über 42,5 % liegt. Wenn der Workload weniger als die durchschnittliche CPU-Nutzung von 42,5 % erfordert, können Sie vom niedrigeren Preis der `t3.large` profitieren, während Sie die gleiche Leistung wie bei einer `m5.large` erhalten.



In der folgenden Tabelle wird gezeigt, wie Sie den Schwellenwert für den Break Even der CPU-Nutzung berechnen, sodass Sie bestimmen können, wann es weniger teuer ist, eine Burstable Performance Instance im `unlimited`-Modus oder eine Instance mit fester Leistung zu verwenden. Die Spalten in der Tabelle sind von A bis K gekennzeichnet.

Instance-Typ	v CPUs	T3 Preis*/ Stunde	M5 Preis*/ Stunde	Preisunterschied	T3-Basisauslastung pro vCPU (%)	Gebühr pro vCPU-Stunde für überzählige Guthaben	Gebühr pro vCPU-Minute	Zusätzliche verfügbare Steigerungsminuten pro vCPU	Zusätzliche CPU % verfügbar	Break Even CPU %
A	B	C	D	E = D - C	F	G	H = G / 60	I = E/H	J = (I / 60) / B	K = F + J
t3.large	2	0,0835 US$	0,096 US$	0,0125 US	30 %	0.05 USD	0,000833 US	15	12,5%	42,5 %

* Preis basiert auf us-east-1 und Linux OS.

Die Tabelle bietet die folgenden Informationen:

- Spalte A zeigt den Instance-Typ `t3.large`.
- Spalte B zeigt die Anzahl von v CPUs für `t3.large`.
- Spalte C zeigt den Preis einer `t3.large` pro Stunde.
- Spalte D zeigt den Preis einer `m5.large` pro Stunde.
- Spalte E zeigt den Preisunterschied zwischen der `t3.large` und der `m5.large`.
- Spalte F zeigt die Basisauslastung pro vCPU der `t3.large`, d. h. 30 %. Auf Baseline-Stufe deckt der Stundenpreis der Instance die Kosten der CPU-Nutzung ab.

- Spalte G zeigt die pauschale Zusatzgebühr pro vCPU-Stunde, die einer Instance in Rechnung gestellt wird, wenn sie ihre CPU-Nutzung auf 100 % steigert, nachdem sie ihr verdientes Guthaben aufgebraucht hat.
- Spalte H zeigt die pauschale Zusatzgebühr pro vCPU-Minute, die einer Instance in Rechnung gestellt wird, wenn sie ihre CPU-Nutzung auf 100 % steigert, nachdem sie ihr verdientes Guthaben aufgebraucht hat.
- Spalte I zeigt die Anzahl der zusätzlichen Minuten, die die `t3.large` pro Stunde bei 100 % CPU steigern kann, während der gleiche Preis pro Stunde wie bei einer `m5.large` bezahlt wird.
- Spalte J zeigt die zusätzliche CPU-Nutzung (in %) oberhalb der Baseline, die die Instance steigern kann, während der gleiche Preis pro Stunde wie bei einer `m5.large` bezahlt wird.
- Spalte K zeigt den Break Even der CPU-Nutzung (in %), den die `t3.large` steigern kann, ohne mehr zu bezahlen als bei der `m5.large`. Bei allem, was darüber hinausgeht, kostet die `t3.large` mehr als die `m5.large`.

Die folgende Tabelle zeigt den Break Even der CPU-Nutzung (in %) für T3-Instance-Typen im Vergleich zu M5-Instance-Typen ähnlicher Größe.

T3-Instance-Typ	Break Even der CPU-Nutzung (in %) für T3 im Vergleich zu M5
`t3.large`	42,5%
`t3.xlarge`	52,5 %
`t3.2xlarge`	52,5 %

Für überzähliges Guthaben können Gebühren anfallen

Wenn die durchschnittliche CPU-Nutzung einer Instance bei oder unterhalb der Baseline liegt, werden für die Instance keine zusätzlichen Gebühren erhoben. Da eine Instance in einem 24-Stunden-Zeitraum eine Höchstzahl von Guthaben verdient (eine `t3.micro`-Instance kann z. B. in einem 24-Stunden-Zeitraum eine Höchstzahl von 288 Guthaben verdienen), kann sie überzählige Guthaben bis zu dieser Höchstzahl verbrauchen, ohne dass diese sofort in Rechnung gestellt werden.

Wenn die CPU-Nutzung jedoch oberhalb der Baseline verbleibt, kann die Instance nicht genügend Guthaben verdienen, um die verbrauchten überzähligen Guthaben zurückzuzahlen. Die überzähligen Guthaben, die nicht zurückgezahlt werden, werden zu einer pauschalen Zusatzgebühr pro vCPU-Stunde in Rechnung gestellt. Informationen zum Tarif finden Sie unter Preise für unbegrenzten T2/T3/T4g-Modus.

Überzählige Guthaben, die zuvor ausgegeben wurden, werden in Rechnung gestellt, wenn einer der folgenden Fälle auftritt:

- Die ausgegebenen überzähligen Guthaben überschreiten die maximale Anzahl an Guthaben, die die Instance in einem 24-Stunden-Zeitraum verdienen kann. Über das Maximum hinaus ausgegebene überzählige Guthaben werden am Ende der Stunde abgerechnet.
- Die Instance wird angehalten oder beendet.
- Die Instance wird von `unlimited` in `standard` geändert.

Ausgegebene überschüssige Kredite werden anhand der CloudWatch Metrik erfasst`CPUSurplusCreditBalance`. Überschüssige Gutschriften, die in Rechnung gestellt werden, werden anhand der CloudWatch Kennzahl erfasst`CPUSurplusCreditsCharged`. Weitere Informationen finden Sie unter Zusätzliche CloudWatch Metriken für Instances mit hoher Leistung.

Wie viel kostet unbegrenzte Spitzenlastleistung?

Wenn Sie überschüssige Credits verwenden und diese nicht durch verdiente Credits zurückgezahlt werden (siehe Für überzähliges Guthaben können Gebühren anfallen), zahlen Sie für die überschüssigen Credits einen pauschalen Zusatztarif pro vCPU-Stunde. Der Tarif ist im Abschnitt T2/T3/T4g Unlimited Mode Pricing T2/T3 Unlimited Mode Pricing aufgeführt. EC2

Kein Startguthaben für T2 Unlimited-Instances

T2-Standard-Instances erhalten Startguthaben, T2 Unlimited-Instances erhalten jedoch keines. Bei einer T2 Unlimited-Instance kann die Leistung jederzeit ohne zusätzliche Gebühren über die Basisleistung hinaus gesteigert werden, solange ihre durchschnittliche CPU-Nutzung in einem fortlaufendem 24-Stunden-Zeitraum oder über die Lebensdauer der Instance hinweg (es gilt der jeweils kürzere Zeitraum) bei oder unterhalb der Baseline liegt. Daher benötigen T2 Unlimited-Instances keine Startguthaben, um sofort nach dem Start eine hohe Leistung zu erzielen.

Wenn eine T2-Instance von `standard` in `unlimited` geändert wird, werden alle angesammelten Startguthaben vom `CPUCreditBalance` entfernt, bevor der verbleibende `CPUCreditBalance` übertragen wird.

T4g, T3a- und T3-Instances erhalten nie Startguthaben, da sie standardmäßig im unbegrenzten Modus gestartet werden und daher beim Start sofort Spitzenlasten aufweisen können. Die Guthabenkonfiguration im unbegrenzten Modus ermöglicht es T4g-, T3a- und T3-Instances, so viel CPU wie nötig zu verwenden, um Spitzenlasten über der Basisauslastung so lange wie nötig zu halten.

Unbegrenzten Modus aktivieren

Sie können für eine laufende oder angehaltene Instance jederzeit von `unlimited` zu `standard` und von `standard` zu `unlimited` wechseln. Weitere Informationen erhalten Sie unter Die Guthaben-Spezifikation beim Start und Die Guthabenspezifikation einer Instance mit Spitzenlastleistung verwalten.

Sie können die Kreditoption auf Kontoebene pro AWS Region und pro Burstable-Performance-Instance-Familie `unlimited` als Standard-Kreditoption festlegen, sodass alle neuen Burstable-Performance-Instances im Konto mit der Standard-Kreditoption gestartet werden. Weitere Informationen finden Sie unter Die standardmäßige Guthaben-Spezifikation für ein Konto verwalten.

Sie können überprüfen, ob Ihre Burstable Performance-Instance als konfiguriert ist `unlimited` oder `standard` mithilfe der EC2 Amazon-Konsole oder der AWS CLI. Weitere Informationen finden Sie unter Instances mit Spitzenlastleistung konfigurieren.

Was passiert mit dem Guthaben beim Wechsel zwischen unbegrenzt und Standard?

`CPUCreditBalance`ist eine CloudWatch Metrik, die die Anzahl der von einer Instance gesammelten Credits erfasst. `CPUSurplusCreditBalance`ist eine CloudWatch Metrik, die die Anzahl der überschüssigen Credits erfasst, die von einer Instance ausgegeben wurden.

Wenn Sie eine als `unlimited` konfigurierte Instance in `standard` ändern, passiert Folgendes:

- Der `CPUCreditBalance`-Wert bleibt unverändert und wird übertragen.
- Der `CPUSurplusCreditBalance`-Wert wird sofort in Rechnung gestellt.

Wenn eine `standard`-Instance in `unlimited` geändert wird, passiert Folgendes:

- Der `CPUCreditBalance`-Wert, der das angesammelte verdiente Guthaben enthält, wird übertragen.
- Für T2 Standard-Instances werden alle Startguthaben vom `CPUCreditBalance`-Wert entfernt, und der verbleibende `CPUCreditBalance`-Wert mit angesammelten verdienten Guthaben wird übertragen.

Überwachen der Guthabennutzung

Um zu sehen, ob Ihre Instance mehr Credits ausgibt, als der Basiswert vorsieht, können Sie die Nutzung anhand von CloudWatch Metriken verfolgen und stündliche Alarme einrichten, um über die Nutzung des Guthabens informiert zu werden. Weitere Informationen finden Sie unter CPU-Guthaben auf Instances mit Spitzenlastleistung überwachen.

Unbegrenzter Modus für Instances mit Spitzenlastleistung

In den folgenden Beispielen wird die Guthabennutzung für Instances erläutert, die als `unlimited` konfiguriert sind.

Beispiele

- Beispiel 1: Beschreiben des Guthabenverbrauchs mit T3 Unlimited
- Beispiel 2: Beschreiben des Guthabenverbrauchs mit T2 Unlimited

Beispiel 1: Beschreiben des Guthabenverbrauchs mit T3 Unlimited

Dieses Beispiel veranschaulicht die CPU-Auslastung einer als `t3.nano` gestarteten `unlimited`-Instance und die Verwendung von verdienten und überzähligen Guthaben zur Aufrechterhaltung der CPU-Auslastung.

Eine `t3.nano`-Instance verdient 144 CPU-Guthaben in einem rollierenden 24-Stunden-Zeitraum, mit denen sie 144 Minuten an vCPU-Nutzung einlösen kann. Wenn ihr CPU-Guthabenguthaben aufgebraucht ist (dargestellt durch die CloudWatch Metrik`CPUCreditBalance`), kann sie überschüssige CPU-Guthaben — die sie noch nicht verdient hat — ausgeben, um sie so lange zu nutzen, wie sie benötigt. Da eine `t3.nano`-Instance in einem 24-Stunden-Zeitraum eine Höchstzahl von 144 Guthaben verdient, kann sie überzählige Guthaben bis zu dieser Höchstzahl verbrauchen, ohne dass diese sofort in Rechnung gestellt werden. Wenn sie mehr als 144 CPU-Guthaben verbraucht, wird ihr am Ende der Stunde die Differenz in Rechnung gestellt.

Das Beispiel soll anhand der folgenden Kurve veranschaulichen, wie eine Instance ihre Leistung sogar nach Verbrauch ihres `CPUCreditBalance` mithilfe überzähliger Guthaben steigern kann. Der folgende Workflow bezieht sich auf die nummerierten Endpunkte in der Kurve:

P1 – Bei 0 Stunden auf dem Graphen wird die Instance als `unlimited` gestartet und beginnt sofort, Guthaben zu verdienen. Die Instance bleibt ab dem Zeitpunkt, an dem sie gestartet wird, ungenutzt – die CPU-Auslastung beträgt 0 % – und es werden keine Guthabenpunkte ausgegeben. Alle nicht

verbrauchten Guthabenpunkt werden im Guthaben gesammelt. Die ersten 24 Stunden liegt die `CPUCreditUsage` bei 0 und der `CPUCreditBalance`-Wert erreicht den Höchstwert von 144.

P2 – In den nächsten 12 Stunden liegt die CPU-Nutzung bei 2,5 %, was unter der Baseline von 5 % liegt. Die Instance verdient mehr Guthaben, als sie verbraucht, `CPUCreditBalance`-Wert kann allerdings den Höchstwert von 144 Guthaben nicht übersteigen.

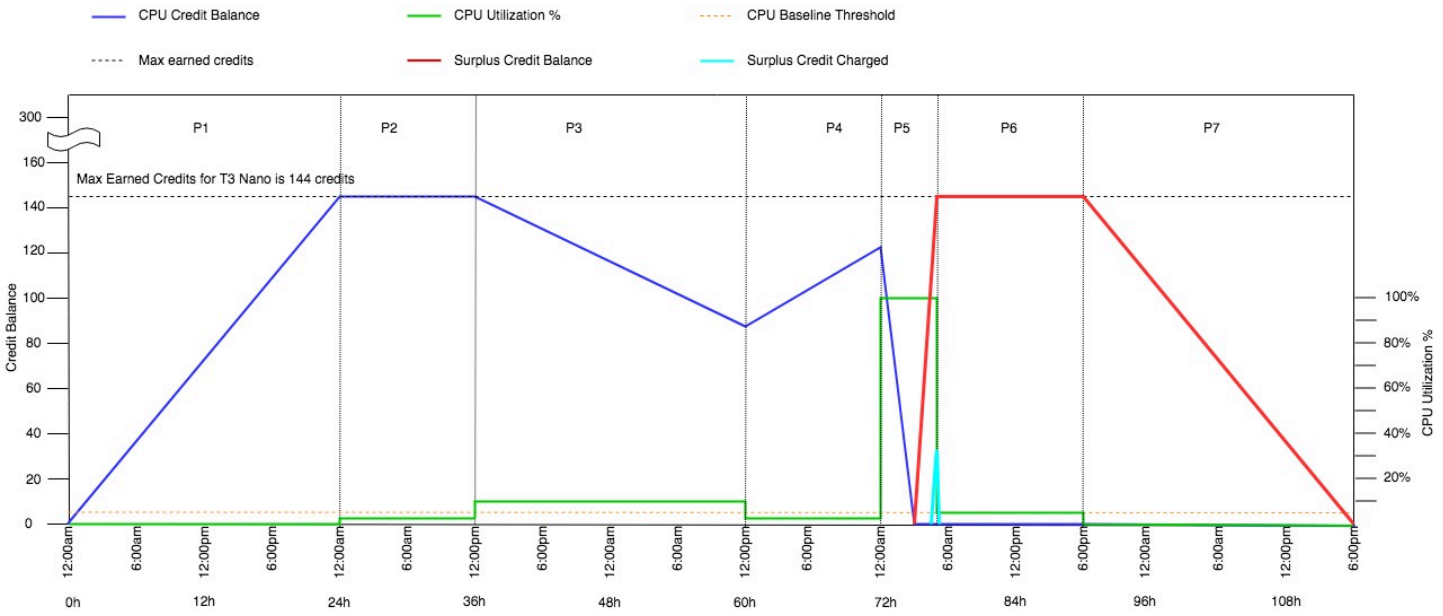
P3 – In den nächsten 24 Stunden liegt die CPU-Nutzung bei 7 % (über der Baseline), wodurch 57,6 Guthaben benötigt werden. Die Instance benötigt mehr Guthaben, als sie verdient, und der `CPUCreditBalance`-Wert wird auf 86,4 Guthaben reduziert.

P4 – In den nächsten 12 Stunden sinkt die CPU-Nutzung auf 2.5 % (unter der Baseline), wodurch 36 Guthaben benötigt werden. In dieser Zeit verdient die Instance 72 Guthaben. Die Instance verdient mehr Guthaben, als sie verbraucht, und der `CPUCreditBalance`-Wert steigt auf 122 Guthaben.

P5 – In den nächsten 5 Stunden steigert die Instance ihre CPU-Nutzung auf 100 % und verbraucht insgesamt 570 Guthaben, um die Laststeigerung aufrechtzuerhalten. Nach etwa einer Stunde hat die Instance ihr gesamtes `CPUCreditBalance`-Guthaben in Höhe von 122 aufgebraucht und benötigt überzähliges Guthaben, um die hohe CPU-Auslastung aufrechtzuerhalten. Dafür fallen 448 überzählige Guthaben in diesem Zeitraum an (570-122=448). Wenn der `CPUSurplusCreditBalance`-Wert 144 CPU-Guthaben erreicht (der Höchstwert, den eine `t3.nano`-Instance im Zeitraum von 24 Stunden verdienen kann), können keine überzähligen Guthaben, die danach verbraucht werden, durch verdiente Guthaben verrechnet werden. Für die danach verbrauchten überzähligen Guthaben in Summe von 304 Guthaben (448-144=304) fällt eine geringfügige zusätzliche Gebühr am Ende des Zeitraums in Höhe von 304 Guthaben an.

P6 – In den nächsten 13 Stunden liegt die CPU-Nutzung bei 5 % (Baseline). Die Instance verdient so viele Guthaben, wie sie ausgibt, ohne Überschuss zu Bezahlen des `CPUSurplusCreditBalance`. Der `CPUSurplusCreditBalance`-Wert verbleibt bei 144 Guthaben.

P7 – Für die letzten 24 Stunden in diesem Beispiel bleibt die Instance im Leerlauf und die CPU-Nutzung beträgt 0 %. Während dieser Zeit verdient die Instance 144 Guthaben, die zum Bezahlen des `CPUSurplusCreditBalance` verwendet werden.



Beispiel 2: Beschreiben des Guthabenverbrauchs mit T2 Unlimited

Dieses Beispiel veranschaulicht die CPU-Auslastung einer als `t2.nano` gestarteten `unlimited`-Instance und die Verwendung von verdienten und überzähligen Guthaben zur Aufrechterhaltung der CPU-Auslastung.

Eine `t2.nano`-Instance verdient 72 CPU-Guthaben in einem rollierenden 24-Stunden-Zeitraum, mit denen sie 72 Minuten an vCPU-Nutzung einlösen kann. Wenn das CPU-Guthaben aufgebraucht ist (dargestellt durch die CloudWatch Metrik`CPUCreditBalance`), kann es überschüssige CPU-Guthaben — die es noch nicht verdient hat — ausgeben, um es so lange wie nötig zu nutzen. Da eine `t2.nano`-Instance in einem 24-Stunden-Zeitraum eine Höchstzahl von 72 Guthaben verdient, kann sie überzählige Guthaben bis zu dieser Höchstzahl verbrauchen, ohne dass diese sofort in Rechnung gestellt werden. Wenn sie mehr als 72 CPU-Guthaben verbraucht, wird ihr am Ende der Stunde die Differenz in Rechnung gestellt.

Das Beispiel soll anhand der folgenden Kurve veranschaulichen, wie eine Instance ihre Leistung sogar nach Verbrauch ihres `CPUCreditBalance` mithilfe überzähliger Guthaben steigern kann. Es wird davon ausgegangen, dass die Instance am Anfang des Zeitstrahls im Graphen die Höchstzahl des Guthabens verdient hat, die sie in 24 Stunden verdienen kann. Der folgende Workflow bezieht sich auf die nummerierten Endpunkte in der Kurve:

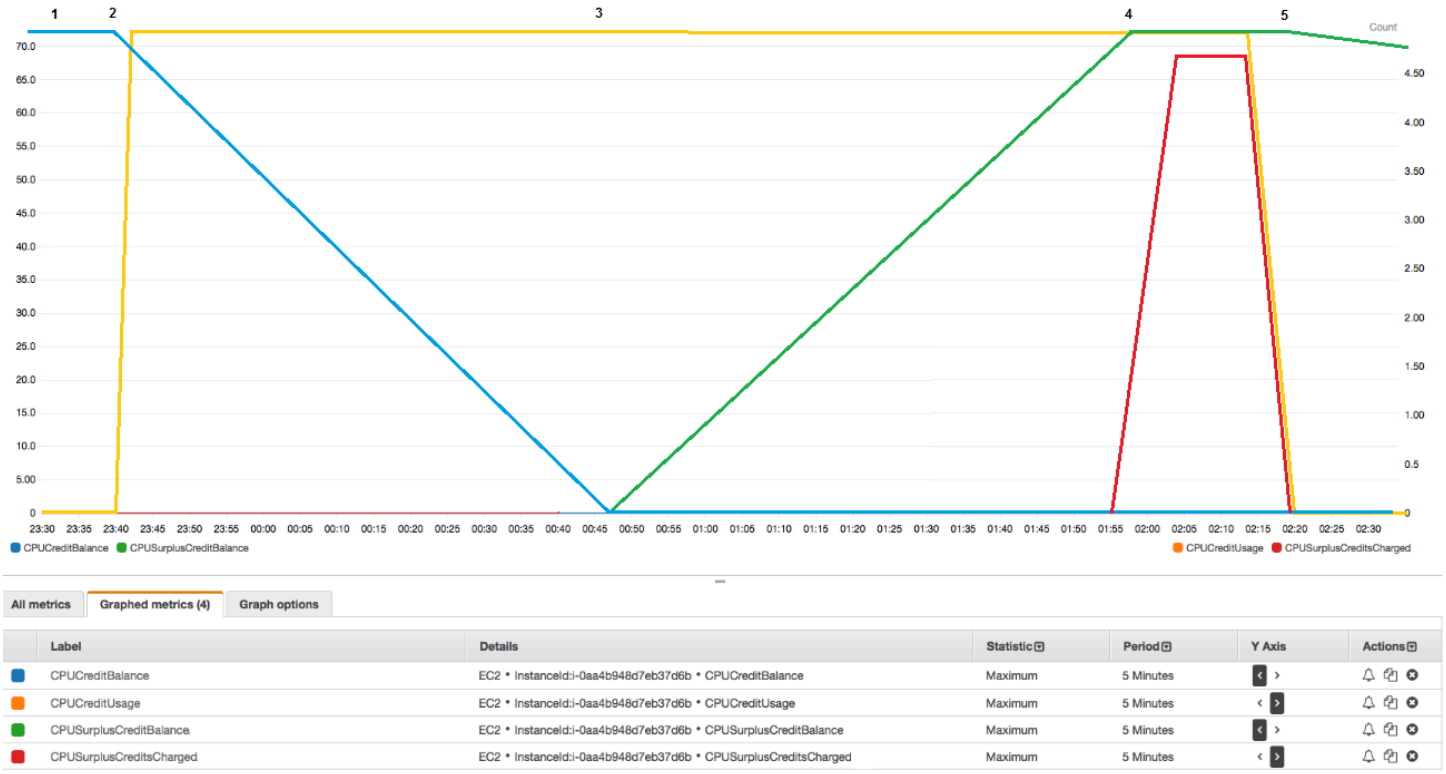
1 – In den ersten 10 Minuten beläuft sich `CPUCreditUsage` auf 0, und der `CPUCreditBalance`-Wert befindet sich weiterhin bei der Höchstzahl 72.

2 – Um 23.40 Uhr verbraucht die Instance mit zunehmender CPU-Nutzung CPU-Guthaben, und der `CPUCreditBalance`-Wert verringert sich.

3 – Gegen 00:47 Uhr hat die Instance ihr gesamtes `CPUCreditBalance` aufgebraucht und verbraucht nun überzählige Guthaben, um die hohe CPU-Auslastung aufrechtzuhalten.

4 – Überzählige Guthaben werden bis um 01.55 Uhr verwendet. Zu diesem Zeitpunkt erreicht der `CPUSurplusCreditBalance`-Wert 72 CPU-Guthaben. Dies entspricht der Höchstzahl, die eine `t2.nano`-Instance in einem 24-Stunden-Zeitraum verdienen kann. Alle danach verwendeten überzähligen Guthaben können innerhalb des 24-Stunden-Zeitraums nicht durch verdiente Guthaben ausgeglichen werden. Dies führt zu einer geringen zusätzlichen Gebühr am Ende der Stunde.

5 – Die Instance verwendet fortgesetzt überzählige Guthaben bis gegen 02.20 Uhr. Jetzt fällt die CPU-Nutzung unter die Baseline, und die Instance beginnt, 3 Guthaben pro Stunde (oder 0,25 Guthaben pro 5 Minuten) zu verdienen, die sie verwendet, um den `CPUSurplusCreditBalance` zurückzuzahlen. Nachdem der `CPUSurplusCreditBalance`-Wert auf 0 verringert wurde, beginnt die Instance, mit 0,25 Guthaben pro 5 Minuten, verdiente Guthaben in `CPUCreditBalance` anzusammeln.



Berechnung der Rechnung (Linux-Instance)

Überzählige Guthaben kosten 0,05 USD je vCPU-Stunde. Die Instance verbrauchte zwischen 01.55 Uhr und 02.20 Uhr ca. 25 überzählige Guthaben. Dies entspricht 0,42 vCPU-Stunden. Die zusätzlichen Kosten für diese Instance betragen 0,42 vCPU-Stunden x 0,05 USD/vCPU-Stunde = 0,021 USD, gerundet auf 0,02 USD. Hier ist die Abrechnung am Monatsende für diese T2 Unlimited-Instance:

Amazon Elastic Compute Cloud running Linux/UNIX		
$0.0058 per On Demand Linux t2.nano Instance Hour	720.000 Hrs	$4.18

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.05 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.02

Berechnung der Rechnung (Windows-Instance)

Überzählige Guthaben kosten 0,096 USD je vCPU-Stunde. Die Instance verbrauchte zwischen 01.55 Uhr und 02.20 Uhr ca. 25 überzählige Guthaben. Dies entspricht 0,42 vCPU-Stunden. Die zusätzlichen Kosten für diese Instance betragen 0,42 vCPU-Stunden x 0,096 USD/vCPU-Stunde = 0,04032 USD, gerundet auf 0,04 USD. Hier ist die Abrechnung am Monatsende für diese T2 Unlimited-Instance:

Amazon Elastic Compute Cloud running Windows		
$0.0081 per On Demand Windows t2.nano Instance Hour	720.000 Hrs	$5.83

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.096 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.04

Sie können Gebührenlimit-Warnungen einrichten, damit Sie jede Stunde über anfallende Gebühren benachrichtigt werden und ggf. Maßnahmen ergreifen können.

Standardmodus für Instances mit Spitzenlastleistung

Eine als `standard` konfigurierte Burstable Performance Instance ist für Workloads mit durchschnittlicher CPU-Auslastung geeignet, die dauerhaft unter der CPU-Basisauslastung der Instance liegt. Um die Basisleistung zu übersteigen, gibt die Instance Guthaben aus, die sie in ihrem CPU-Guthaben-Konto angesammelt hat. Wenn die Instance nicht mehr viele angesammelte Guthaben aufweist, wird die CPU-Auslastung schrittweise auf die Basisebene reduziert, sodass bei der Instance kein starker Leistungsrückgang auftritt, wenn ihr angesammelter CPU-Guthaben-

Kontostand aufgebraucht ist. Weitere Informationen finden Sie unter Schlüsselkonzepte und Definitionen für Instances mit Spitzenlastleistung.

Inhalt

- Standardmodus-Konzepte für Instances mit Spitzenlastleistung
  - Funktionsweise der Standard-Instances mit Spitzenlastleistung
  - Startguthaben
  - Startguthaben-Limits
  - Unterschiede zwischen Startguthaben und erworbenem Guthaben
- Beispiele für den Standardmodus für Instances mit Spitzenlastleistung
  - Beispiel 1: Beschreiben des Guthabenverbrauchs mit T3 Standard
  - Beispiel 2: Beschreiben des Guthabenverbrauchs mit T2 Standard
    - Zeitraum 1: 1–24 Stunden
    - Zeitraum 2: 25–36 Stunden
    - Zeitraum 3: 37–61 Stunden
    - Zeitraum 4: 62–72 Stunden
    - Zeitraum 5: 73–75 Stunden
    - Zeitraum 6: 76–90 Stunden
    - Zeitraum 7: 91–96 Stunden

Standardmodus-Konzepte für Instances mit Spitzenlastleistung

Der `standard`-Modus ist eine Konfigurationsoption für Instances mit Spitzenleistung. Er kann jederzeit für eine laufende oder angehaltene Instance aktiviert oder deaktiviert werden. Sie können die Kreditoption auf Kontoebene pro AWS Region und pro Instance-Familie mit hoher Leistung `standard` als Standardoption festlegen, sodass alle neuen Burstable-Performance-Instances im Konto mit der Standard-Kreditoption gestartet werden.

Funktionsweise der Standard-Instances mit Spitzenlastleistung

Wenn sich eine Burstable Performance Instance, die als `standard` konfiguriert ist, in einem Ausführungsstatus befindet, verdient sie kontinuierlich (mit einer Auflösung in Millisekunden) einen festgelegten Satz an verdientem Guthaben pro Stunde. Wenn eine T2-Standard-Instance beendet wird, verliert sie das gesamte angefallene Guthaben, und das Guthabenkonto wird auf Null zurückgesetzt. Wenn sie erneut gestartet wird, erhält sie einen neuen Satz an Startguthaben, und

beginnt mit dem Sammeln von verdientem Guthaben. Für T4g-, T3a- und T3-Standard-Instances bleibt der CPU-Guthaben-Kontostand sieben Tage nach dem Anhalten einer Instance erhalten. Danach verfällt das Guthaben. Falls Sie die Instance innerhalb von sieben Tagen starten, geht kein Guthaben verloren.

T2-Standard-Instances erhalten zwei Arten von CPU-Guthaben: erworbenes Guthaben und Startguthaben. Wenn sich eine T2 Standard-Instance in einem Ausführungsstatus befindet, verdient sie kontinuierlich (mit einer Auflösung in Millisekunden) einen festgelegten Satz an verdientem Guthaben pro Stunde. Beim Start hat sie noch kein Guthaben für eine gute Startuperfahrung verdient; daher erhält sie für einen gute Startuperfahrung Startguthaben, das sie zuerst ausgibt, während verdientes Guthaben gesammelt wird.

T4g-, T3a- und T3-Instances erhalten kein Startguthaben, da sie den unbegrenzten Modus unterstützen. Die Guthabenkonfiguration im unbegrenzten Modus ermöglicht es T4g-, T3a- und T3-Instances, so viel CPU wie nötig zu verwenden, um Spitzenlasten über der Basisauslastung so lange wie nötig zu halten.

Startguthaben

T2 Standard-Instances erhalten 30 Startguthaben pro vCPU beim Start oder Start, und T1 Standard-Instances erhalten 15 Startguthaben. Beispielsweise hat eine `t2.micro` Instance eine vCPU und erhält 30 Startguthaben, während eine `t2.xlarge` Instance vier V hat CPUs und 120 Startguthaben erhält. Das Startguthaben wurde für eine gute Startuperfahrung entwickelt, um die Steigerung der Leistung von Instances unmittelbar nach dem Start zu ermöglichen, bevor sie verdientes Guthaben angesammelt haben.

Das Startguthaben wird vor dem verdienten Guthaben verwendet. Nicht ausgegebenes Startguthaben wird auf dem CPU-Guthaben-Konto angesammelt, zählt aber nicht zum Limit für das CPU-Guthaben-Konto. Eine `t2.micro`-Instance hat beispielsweise ein Limit von 144 verdienten Guthaben für das CPU-Guthaben-Konto. Wenn sie gestartet und dann 24 Stunden lang nicht genutzt wird, erreicht ihr CPU-Guthaben-Kontostand den Wert 174 (30 Startguthaben + 144 verdiente Guthaben), womit das Limit überschritten ist. Nachdem die Instance jedoch die 30 Startguthaben verbraucht hat, darf der Guthaben-Kontostand 144 nicht überschreiten. Weitere Informationen zum Limit für das CPU-Guthaben-Konto für jede Instance-Größe finden Sie in der Guthabentabelle.

In der folgenden Tabelle sind die anfängliche CPU-Guthabenzuweisung aufgeführt, die beim Start oder Start erhalten wurde, sowie die Anzahl von V. CPUs

Instance-Typ	Startguthaben	v CPUs
t1.micro	15	1
t2.nano	30	1
t2.micro	30	1
t2.small	30	1
t2.medium	60	2
t2.large	60	2
t2.xlarge	120	4
t2.2xlarge	240	8

Startguthaben-Limits

Die Häufigkeit, mit der T2-Standard-Instances Startguthaben erhalten können, ist eingeschränkt. Das Standardlimit liegt bei 100 Startvorgängen aller T2-Standard-Instances zusammengenommen pro Konto, pro Region und pro rollierendem 24-Stunden-Zeitraum. Das Limit wird beispielsweise erreicht, wenn eine Instance innerhalb eines 24-Stunden-Zeitraums 100-mal angehalten und gestartet wird oder wenn 100 Instances innerhalb eines 24-Stunden-Zeitraums gestartet werden oder andere Kombinationen erfolgen, die 100 Starts entsprechen. Neue Konten weisen möglicherweise ein geringeres Limit auf, welches sich basierend auf Ihrer Nutzung im Laufe der Zeit erhöht.

> **Tip**
>
> Um sicherzustellen, dass Ihre Workloads immer die erforderliche Leistung erhalten, wechseln Sie zu Unbegrenzter Modus für Burstable Performance Instances oder erwägen die Verwendung einer größeren Instance-Größe.

Unterschiede zwischen Startguthaben und erworbenem Guthaben

Die folgende Tabelle führt die Unterschiede zwischen Startguthaben und erworbenem Guthaben auf.

	Startguthaben	Erworbenes Guthaben
Erwerbsrate von Guthaben	T2-Standard-Instances erhalten beim Start ein Startguthaben von 30 pro vCPU. Wenn eine T2-Instance von `unlimited` in `standard` geändert wird, erhält es beim Wechsel keine Startguthaben.	Jede T2-Instance erhält kontinuierlich (mit einer Auflösung in Millisekunden) einen festgelegten Satz an CPU-Guthaben pro Stunde, der von der Instance-Größe abhängt. Weitere Informationen zur Anzahl des CPU-Guthabens, das für jede Instance-Größe erworben wurde, finden Sie in der Guthabentabelle.
Erwerbslimit von Guthaben	Das Limit für den Erhalt von Startguthaben liegt bei 100 Startvorgängen aller T2-Standard-Instances zusammengenommen pro Konto, pro Region und pro rollierendem 24-Stunden-Zeitraum. Neue Konten weisen möglicherweise ein geringeres Limit auf, welches sich basierend auf Ihrer Nutzung im Laufe der Zeit erhöht.	Eine T2-Instance kann nicht mehr Guthaben ansammeln, als durch das Limit für das CPU-Guthaben-Konto zugelassen. Wenn das CPU-Guthaben-Konto sein Limit erreicht hat, werden alle Guthaben, die nach dem Erreichen des Limits verdient wurden, verworfen. Das Startguthaben wird dem Limit nicht angerechnet. Weitere Informationen zum Limit für das CPU-Guthaben-Konto für jede T2-Instance-Größe finden Sie in der Guthabentabelle.
Verwendung des Guthabens	Das Startguthaben wird vor dem verdienten Guthaben verwendet.	Verdientes Guthaben wird erst verwendet, nachdem das gesamte Startguthaben verbraucht wurde.
Ablauf des Guthabens	Wenn eine T2 Standard-Instance ausgeführt wird, verfällt das Startguthaben nicht. Wenn eine T2 Standard-Instance angehalten oder auf T2 Unlimited umgestellt wird, gehen alle Startguthaben verloren.	Wenn eine T2-Instance ausgeführt wird, verfällt das angesammelte verdiente Guthaben nicht. Wenn die T2-Instance beendet wird, geht das gesamte angesammelte verdiente Guthaben verloren.

Die Gesamtanzahl der angesammelten Startguthaben und der angesammelten verdienten Guthaben wird von der CloudWatch -Metrik `CPUCreditBalance` verfolgt. Weitere Informationen finden Sie unter `CPUCreditBalance` in der CloudWatch -Metriktabelle.

Beispiele für den Standardmodus für Instances mit Spitzenlastleistung

In den folgenden Beispielen wird die Guthabennutzung für Instances erläutert, die als `standard` konfiguriert sind.

Beispiele

- Beispiel 1: Beschreiben des Guthabenverbrauchs mit T3 Standard
- Beispiel 2: Beschreiben des Guthabenverbrauchs mit T2 Standard

Beispiel 1: Beschreiben des Guthabenverbrauchs mit T3 Standard

In diesem Beispiel sehen Sie, wie eine als `t3.nano` gestartete `standard`-Instance earned-Guthaben verdient, sammelt und ausgibt. Der Guthaben-Kontostand zeigt die angesammelten earned-Guthaben an.

Eine ausgeführte `t3.nano`-Instance verdient alle 24 Stunden 144 Guthaben. Das Limit für den Guthaben-Kontostand beträgt 144 verdiente Guthaben. Nachdem das Limit erreicht ist, werden alle neu verdienten Guthabenpunkte verworfen. Weitere Informationen zur Anzahl des Guthabens, das sich verdienen und ansammeln lässt, finden Sie in der Guthabentabelle.

Sie können eine T3-Standard-Instance starten und sofort verwenden. Oder Sie können eine T3 Standard-Instance starten und sie für einige Tage inaktiv lassen, bevor Sie Anwendungen darauf ausführen. Ob eine Instance genutzt wird oder ungenutzt bleibt, entscheidet darüber, ob Punkte ausgegeben oder angesammelt werden. Falls eine Instance nach ihrem Start 24 Stunden lang im Leerlauf verbleibt, erreicht der Guthaben-Kontostand sein Limit, die maximale Anzahl verdienter Guthaben, die angesammelt werden kann.

Dieses Beispiel beschreibt eine Instance, die nach dem Start 24 Stunden lang untätig bleibt, und führt Sie durch sieben Zeitabschnitte über einen Zeitraum von 96 Stunden, wobei die Rate, mit der Punkte für das Guthaben verdient, aufgelaufen, ausgegeben und verworfen werden, und der Wert des Guthabens am Ende jeder Zeitraum angezeigt werden.

Der folgende Workflow bezieht sich auf die nummerierten Endpunkte in der Kurve:

P1 – Bei 0 Stunden auf dem Graphen wird die Instance als `standard` gestartet und beginnt sofort, Guthaben zu verdienen. Die Instance bleibt ab dem Zeitpunkt, an dem sie gestartet wird, ungenutzt –

die CPU-Auslastung beträgt 0 % – und es werden keine Guthabenpunkte ausgegeben. Alle nicht verbrauchten Guthabenpunkt werden im Guthaben gesammelt. Die ersten 24 Stunden liegt die `CPUCreditUsage` bei 0 und der `CPUCreditBalance`-Wert erreicht den Höchstwert von 144.

P2 – In den nächsten 12 Stunden liegt die CPU-Nutzung bei 2,5 %, was unter der Baseline von 5 % liegt. Die Instance verdient mehr Guthaben, als sie verbraucht, `CPUCreditBalance`-Wert kann allerdings den Höchstwert von 144 Guthaben nicht übersteigen. Sämtliche verdienten Guthaben über das Limit hinaus verfallen.

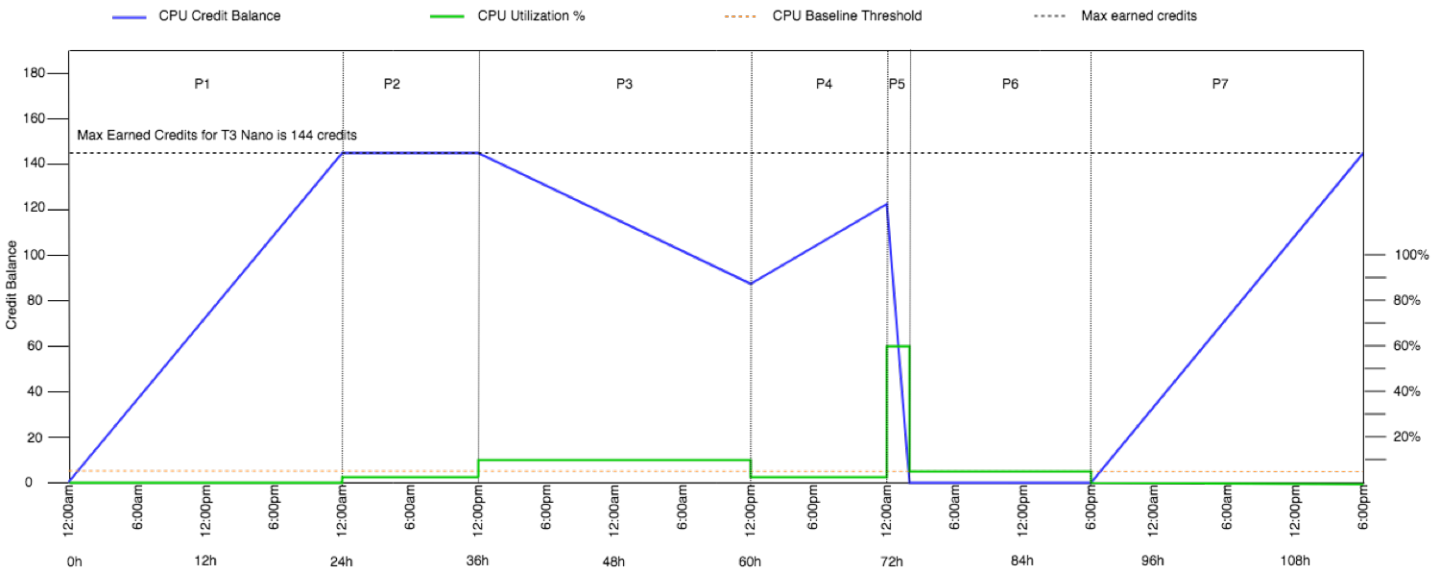
P3 – In den nächsten 24 Stunden liegt die CPU-Nutzung bei 7 % (über der Baseline), wodurch 57,6 Guthaben benötigt werden. Die Instance benötigt mehr Guthaben, als sie verdient, und der `CPUCreditBalance`-Wert wird auf 86,4 Guthaben reduziert.

P4 – In den nächsten 12 Stunden sinkt die CPU-Nutzung auf 2.5 % (unter der Baseline), wodurch 36 Guthaben benötigt werden. In dieser Zeit verdient die Instance 72 Guthaben. Die Instance verdient mehr Guthaben, als sie verbraucht, und der `CPUCreditBalance`-Wert steigt auf 122 Guthaben.

P5 – In den nächsten zwei Stunden steigert die Instance ihre CPU-Nutzung auf 60 % und verbraucht den gesamten `CPUCreditBalance`-Wert von 122 Guthaben. Am Ende dieses Zeitraums, wenn `CPUCreditBalance` gleich Null ist, wird ein Absinken der CPU-Auslastung auf die Basisauslastung von 5 % erzwungen. Auf Baseline-Stufe verdient die Instance so viel Guthaben, wie sie verbraucht.

P6 – In den nächsten 14 Stunden liegt die CPU-Nutzung bei 5 % (Baseline). Die Instance verdient so viele Guthaben, wie sie verbraucht. Der `CPUCreditBalance`-Wert verbleibt bei 0.

P7 – Für die letzten 24 Stunden in diesem Beispiel bleibt die Instance im Leerlauf und die CPU-Nutzung beträgt 0 %. Während dieser Zeit verdient die Instance 144 Guthaben, die im `CPUCreditBalance` angesammelt werden.



Beispiel 2: Beschreiben des Guthabenverbrauchs mit T2 Standard

In diesem Beispiel sehen Sie, wie eine als `t2.nano` gestartete `standard`-Instance launch- und earned-Guthaben verdient, sammelt und ausgibt. Sie sehen, wie das Guthaben nicht nur aufgelaufenes earned-Guthaben widerspiegelt, sondern auch aufgelaufenes launch-Guthaben.

Eine `t2.nano`-Instance erhält 30 Punkte Startguthaben, wenn sie gestartet wird, und verdient alle 24 Stunden 72 Punkte. Ihr Guthabenlimit beträgt 72 verdiente Punkte; Startguthaben wird nicht auf das Limit angerechnet. Nachdem das Limit erreicht ist, werden alle neu verdienten Guthabenpunkte verworfen. Weitere Informationen zur Anzahl des Guthabens, das sich verdienen und ansammeln lässt, finden Sie in der Guthabentabelle. Weitere Informationen zu Limits finden Sie unter Startguthaben-Limits.

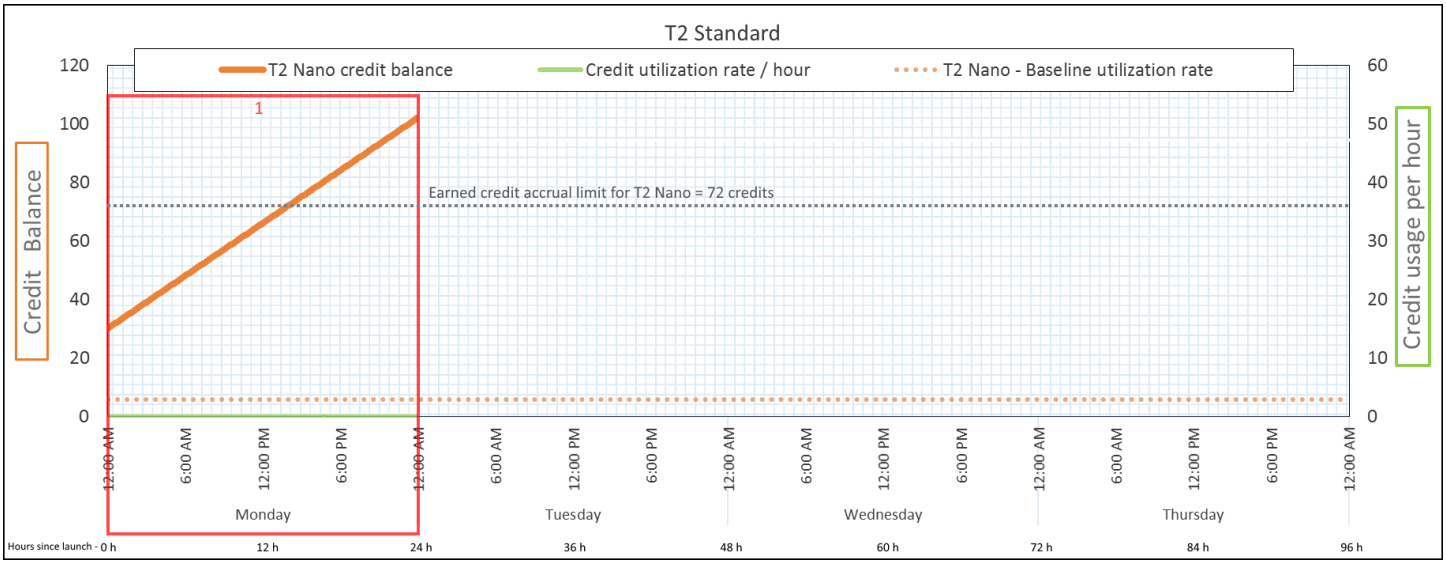
Sie können eine T2-Standard-Instance starten und sofort verwenden. Oder Sie können eine T2 Standard-Instance starten und sie für einige Tage inaktiv lassen, bevor Sie Anwendungen darauf ausführen. Ob eine Instance genutzt wird oder ungenutzt bleibt, entscheidet darüber, ob Punkte ausgegeben oder angesammelt werden. Wenn eine Instance nach dem Start 24 Stunden lang inaktiv bleibt, scheint das Guthaben sein Limit zu überschreiten, da das Guthaben sowohl die aufgelaufenen verdienten Punkte als auch das aufgelaufene Startguthaben widerspiegelt. Nach der Nutzung der CPU wird jedoch zuerst das Startguthaben ausgegeben. Danach spiegelt das Limit immer die maximale Anzahl des verdienten Startguthabens wider, die angesammelt werden können.

Dieses Beispiel beschreibt eine Instance, die nach dem Start 24 Stunden lang untätig bleibt, und führt Sie durch sieben Zeitabschnitte über einen Zeitraum von 96 Stunden, wobei die Rate, mit der

Punkte für das Guthaben verdient, aufgelaufen, ausgegeben und verworfen werden, und der Wert des Guthabens am Ende jeder Zeitraum angezeigt werden.

Zeitraum 1: 1–24 Stunden

Bei 0 Stunden auf dem Graphen wird die T2-Instance als `standard` gestartet und bekommt sofort 30 Punkte Startguthaben. Sie verdient Guthabenpunkte im laufenden Betrieb. Die Instance bleibt ab dem Zeitpunkt, an dem sie gestartet wird, ungenutzt – die CPU-Auslastung beträgt 0 % – und es werden keine Guthabenpunkte ausgegeben. Alle nicht verbrauchten Guthabenpunkt werden im Guthaben gesammelt. Etwa 14 Stunden nach dem Start beträgt das Guthaben 72 (30 Punkte Startguthaben + 42 Punkte verdientes Guthaben), was dem entspricht, was die Instance in 24 Stunden verdienen kann. 24 Stunden nach dem Start übersteigt das Guthaben 72 Punkte, da das nicht verbrauchte Startguthaben aufgelaufen ist. Es beträgt— nun 102 Punkte: 30 Punkte Startguthaben + 72 verdiente Punkte.



Ausgabe-Rate von Guthaben	0 Punkte pro 24 Stunden (0 % CPU-Auslastung)
Erwerbsrate von Guthaben	72 Punkte pro 24 Stunden
Verfall-Rate von Guthaben	0 Punkte pro 24 Stunden
Guthaben	102 Punkte (30 Punkte Startguthaben + 72 verdiente Punkte)

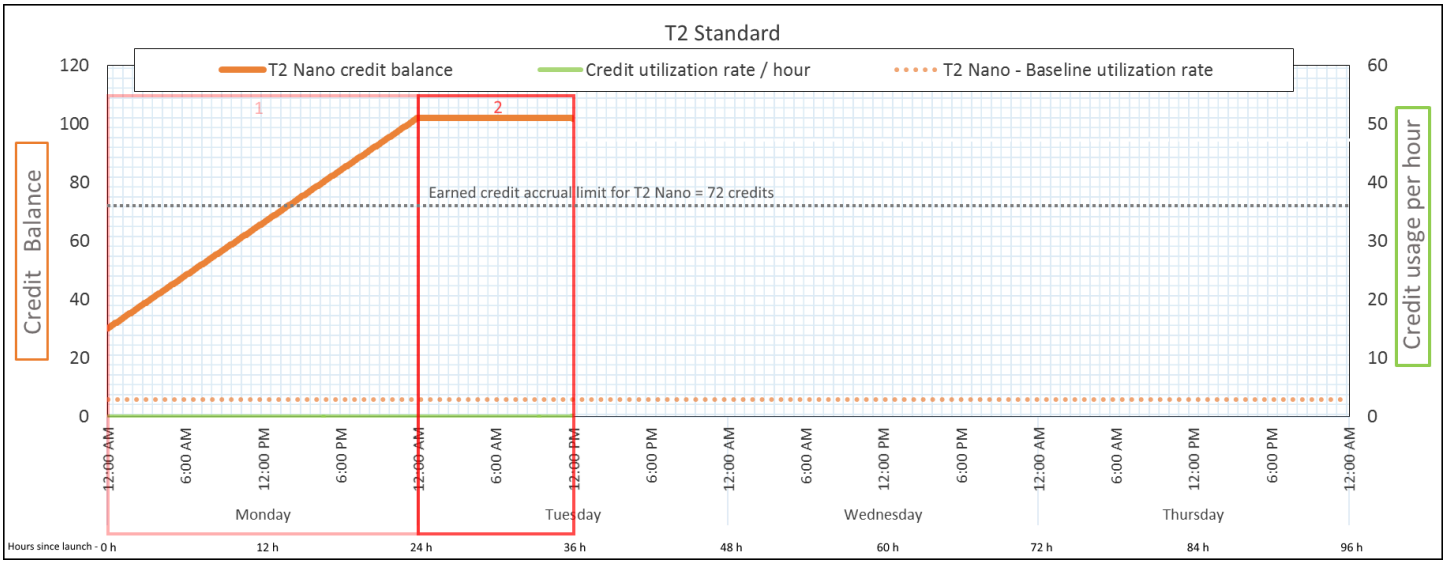
Schlussfolgerung

Wenn es nach dem Start keine CPU-Auslastung gibt, sammelt die Instance mehr Punkte, als sie in 24 Stunden verdienen kann (30 Punkte Startguthaben + 72 verdiente Punkte = 102 Punkte).

In einem realen Szenario verbraucht eine EC2 Instance beim Starten und Ausführen eine geringe Anzahl von Credits, wodurch verhindert wird, dass der Saldo in diesem Beispiel den maximalen theoretischen Wert erreicht.

Zeitraum 2: 25–36 Stunden

Für die nächsten 12 Stunden bleibt die Instance ungenutzt und verdient Punkte, aber das Guthaben erhöht sich nicht. Es verbleibt bei 102 Punkten (30 Punkte Startguthaben + 72 verdiente Punkte). Das Guthaben hat seine Grenze von 72 aufgelaufenen verdienten Punkten erreicht, sodass neu verdientes Guthaben verworfen wird.



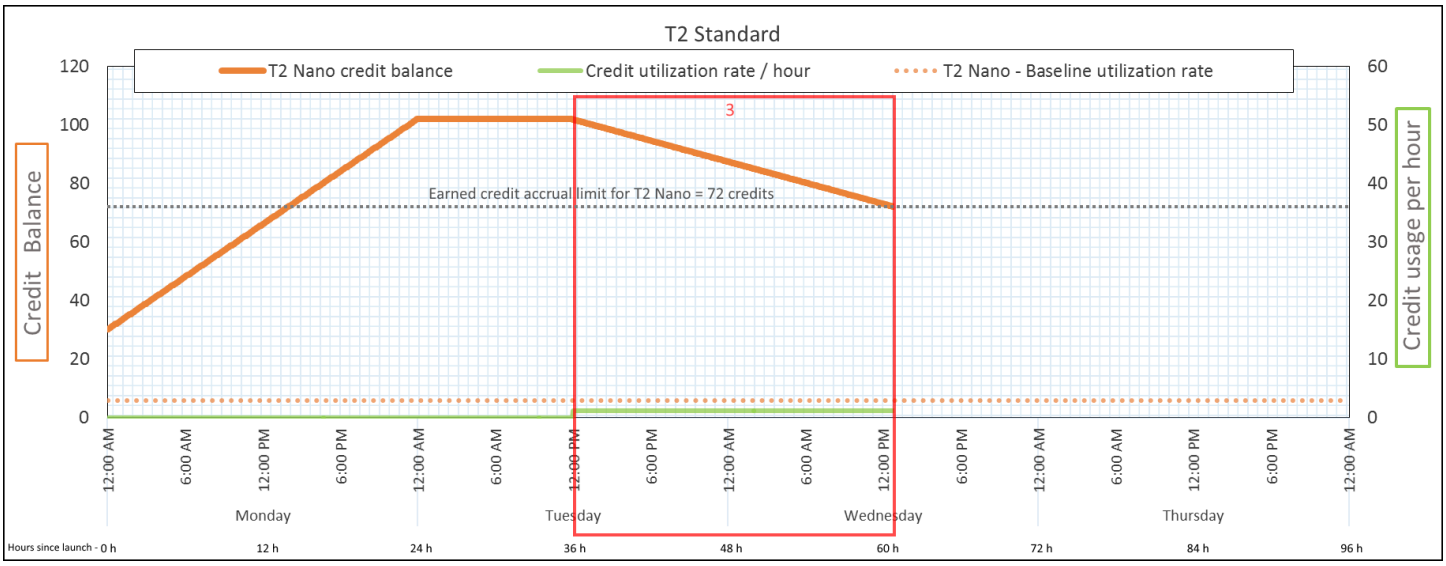
Ausgabe-Rate von Guthaben	0 Punkte pro 24 Stunden (0 % CPU-Auslastung)
Erwerbsrate von Guthaben	72 Credits pro 24 Stunden (3 Credits pro Stunde)
Verfall-Rate von Guthaben	72 Punkte pro 24 Stunden (100 % der Erwerbsrate von Guthaben)
Guthaben	102 Credits (30 Punkte Startguthaben + 72 verdiente Credits) — Saldo ist unverändert

Schlussfolgerung

Eine Instance verdient ständig Punkte, kann aber keine weiteren Punkte mehr sammeln, wenn das Guthaben sein Limit erreicht hat. Nach Erreichen des Limits werden neu verdiente Punkte verworfen. Das Startguthaben wird nicht auf das Guthabenlimit angerechnet. Wenn der Saldo aufgelaufenes Startguthaben enthält, scheint der Saldo über dem Limit zu liegen.

Zeitraum 3: 37–61 Stunden

Für die nächsten 25 Stunden verbraucht die Instance 2 % CPU, was 30 Punkte erfordert. Im gleichen Zeitraum verdient sie 75 Punkte, aber das Guthaben nimmt ab. Der Saldo verringert sich, weil das aufgelaufene Startguthaben zuerst verbraucht wird, während neu erworbenes Guthaben verworfen wird, weil das Guthaben bereits an der Grenze von 72 verdienten Punkten liegt.



Ausgabe-Rate von Guthaben	28,8 Credits pro 24 Stunden (1,2 Credits pro Stunde, 2 % CPU-Auslastung, 40 % der Kreditverdienstquote) — 30 Punkte über 25 Stunden
Erwerbsrate von Guthaben	72 Punkte pro 24 Stunden
Verfall-Rate von Guthaben	72 Punkte pro 24 Stunden (100 % der Erwerbsrate von Guthaben)

Guthaben	72 Punkte (30 Punkte Startguthaben wurden ausgegeben; 72 verdiente Punkte bleiben ungenutzt)

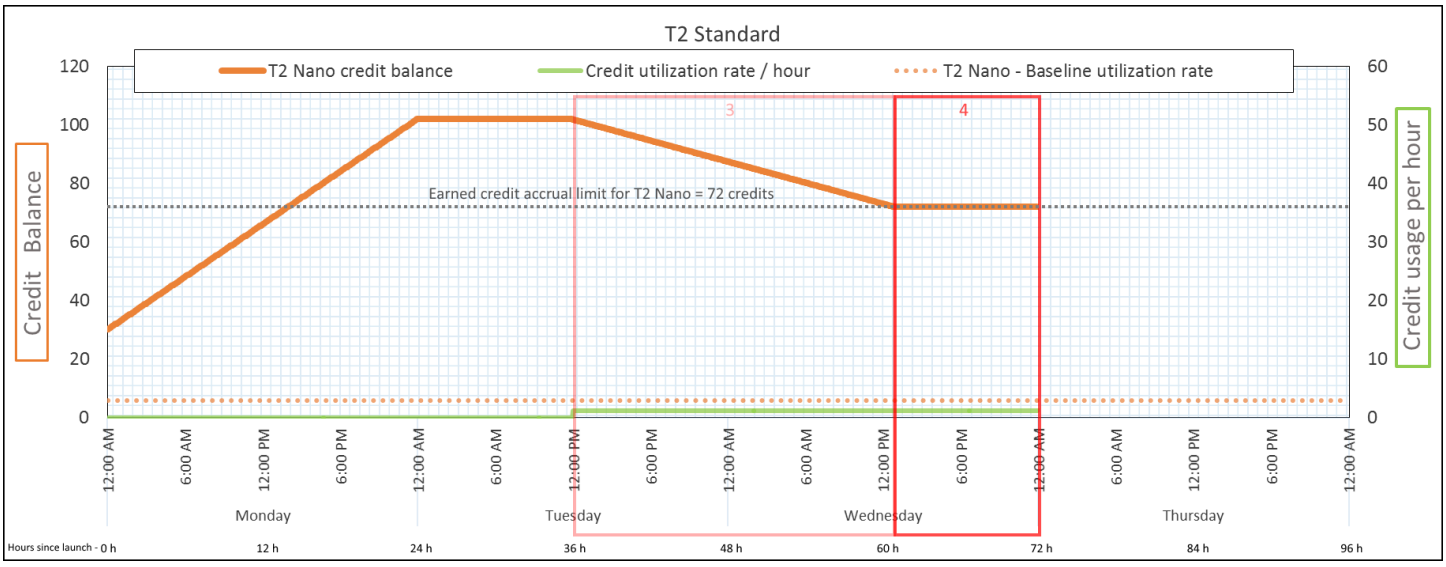
Schlussfolgerung

Eine Instance gibt zuerst das Startguthaben aus, bevor sie das verdiente Guthaben ausgibt. Das Startguthaben wird nicht auf das Guthabenlimit angerechnet. Nachdem das Startguthaben verbraucht ist, kann das Guthaben niemals höher sein als das, was in 24 Stunden verdient werden kann. Außerdem kann eine Instance, während sie läuft, kein weiteres Startguthaben erhalten.

Zeitraum 4: 62–72 Stunden

Für die nächsten 11 Stunden verbraucht die Instance 2 % CPU, was 13.2 Punkte erfordert. Dies ist die gleiche CPU-Auslastung wie im vorherigen Zeitraum, aber der Saldo sinkt nicht. Er bleibt bei 72 Punkten.

Der Saldo verringert sich nicht, da die Erwerbsrate von Guthaben höher ist als die Rate, mit der das Guthaben ausgegeben wird. In der Zeit, in der die Instance 13.2 Punkte ausgibt, verdient sie auch 33 Punkte. Das Saldo-Limit beträgt jedoch 72 Punkte, sodass alle verdienten Punkte, die das Limit überschreiten, verworfen werden. Der Saldo verbleibt bei 72 Punkten, die sich vom Stand von 102 Punkten in Zeitraum 2 unterscheiden, da es kein aufgelaufenes Startguthaben gibt.



Ausgabe-Rate von Guthaben	28,8 Credits pro 24 Stunden (1,2 Credits pro Stunde, 2 % CPU-Auslastung, 40 % der

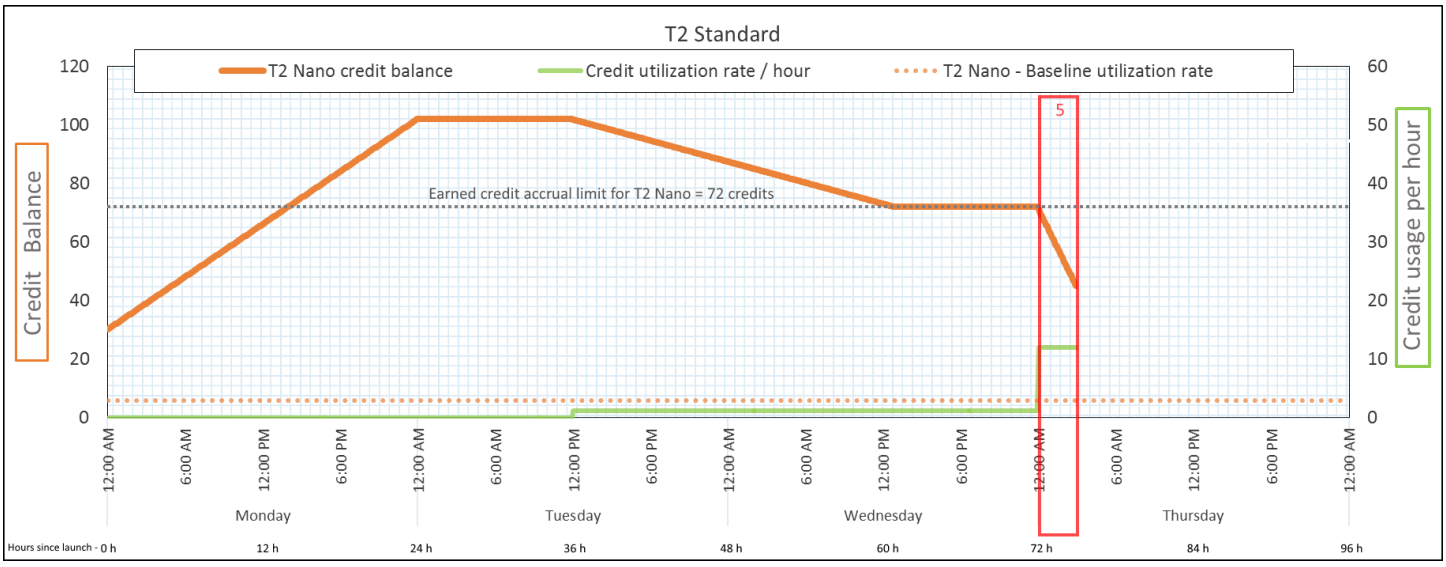
	Kreditverdienstquote) — 13,2 Punkte über 11 Stunden
Erwerbsrate von Guthaben	72 Punkte pro 24 Stunden
Verfall-Rate von Guthaben	43.2 Punkte pro 24 Stunden (60 % der Erwerbsrate von Guthaben)
Guthaben	72 Punkte (0 Punkte Startguthaben, 72 verdiente Punkte) — der Saldo ist am Limit

Schlussfolgerung

Nachdem das Startguthaben verbraucht ist, wird das Guthaben durch die Anzahl der Punkte bestimmt, die eine Instance innerhalb von 24 Stunden verdienen kann. Wenn die Instance mehr Punkte verdient, als sie ausgibt, werden neu verdiente Punkte über dem Limit verworfen.

Zeitraum 5: 73–75 Stunden

Für die nächsten drei Stunden verbraucht die Instance plötzlich 20 % CPU-Auslastung, was 36 Punkte erfordert. Die Instance verdient neun Punkte in den gleichen drei Stunden, was zu einer Verringerung des Nettosaldos um 27 Punkte führt. Am Ende von drei Stunden beträgt das Guthaben 45 aufgelaufene Punkte.



Ausgabe-Rate von Guthaben	288 Credits pro 24 Stunden (12 Credits pro Stunde, 20 % CPU-Auslastung, 400 % der

	Kreditverdienstquote) — 36 Punkte über 3 Stunden
Erwerbsrate von Guthaben	72 Punkte pro 24 Stunden (9 Punkte über 3 Stunden)
Verfall-Rate von Guthaben	0 Punkte pro 24 Stunden
Guthaben	45 Punkte (vorheriger Saldo [72] – verbrauchte Punkte [36] + verdiente Punkte [9]) — der Saldo sinkt mit einer Rate von 216 Punkten pro 24 Stunden (Ausgabenrate 288/24 + Erwerbsrate 72/24 = Saldoabnahmequote 216/24)

Schlussfolgerung

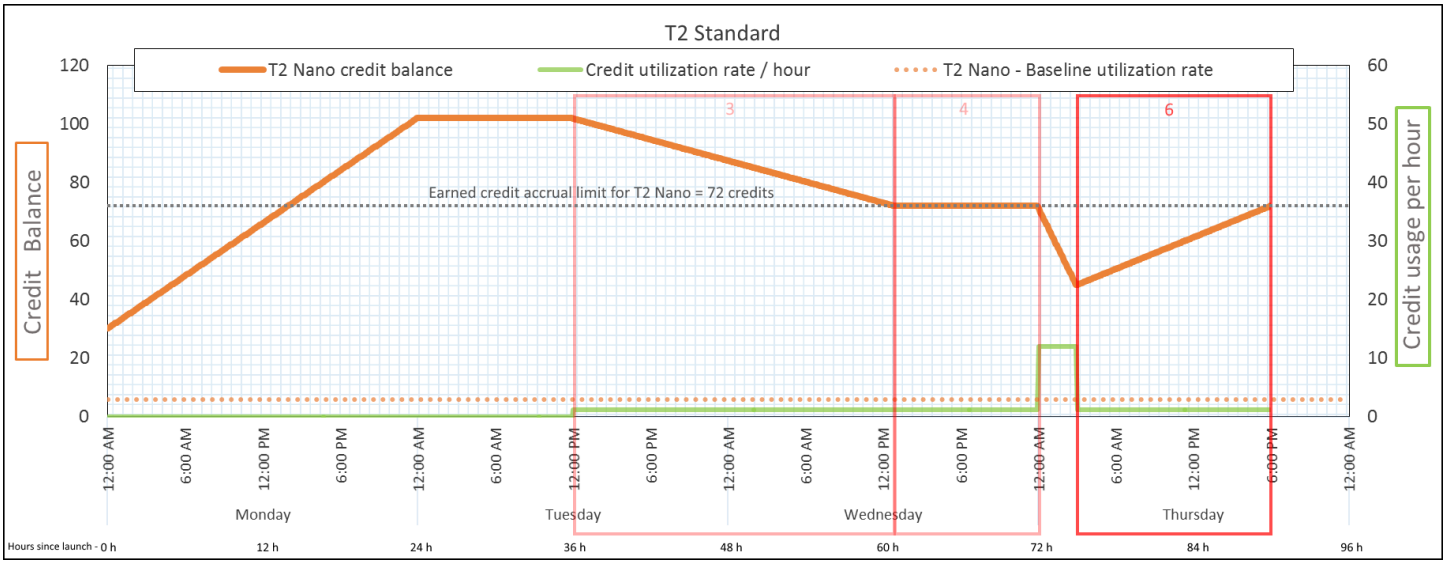
Wenn eine Instance mehr Punkte ausgibt, als sie verdient, verringert sich ihr Guthaben.

Zeitraum 6: 76–90 Stunden

Für die nächsten 15 Stunden verbraucht die Instance 2 % CPU, was 18 Punkte erfordert. Dies ist die gleiche CPU-Auslastung wie in den Zeiträumen 3 und 4. Allerdings steigt der Saldo in diesem Zeitraum an, während er im Zeitraum 3 zurückging und in Zeitraum 4 einen Höchstwert erreichte.

In Zeitraum 3 wurde das aufgelaufene Startguthaben verbraucht und alle verdienten Punkte, die das Guthaben-Limit überschritten haben, verworfen, was zu einem Rückgang des Guthabens führte. In Zeitraum 4 hat die Instance weniger Guthaben ausgegeben als sie verdient hat. Das verdiente Guthaben, das das Limit überschritt, wurde verworfen, so dass die Bilanz auf ihr Guthaben-Maximum von 72 stieg.

In diesem Zeitraum gibt es kein aufgelaufenes Startguthaben, und die Anzahl der aufgelaufenen verdienten Punkte im Saldo liegt unter dem Limit. Verdiente Punkte werden nicht verworfen. Außerdem verdient die Instance mehr Guthaben, als sie ausgibt, was zu einer Erhöhung des Guthabens führt.



Ausgabe-Rate von Guthaben	28,8 Credits pro 24 Stunden (1,2 Credits pro Stunde, 2 % CPU-Auslastung, 40 % der Kreditverdienstquote) — 18 Punkte über 15 Stunden
Erwerbsrate von Guthaben	72 Punkte pro 24 Stunden (45 Punkte über 15 Stunden)
Verfall-Rate von Guthaben	0 Punkte pro 24 Stunden
Guthaben	72 Punkte (Saldo steigt um 43,2 Punkte pro 24 Stunden — Änderungsrate = Ausgaberate 28,8/24 + Erwerbsrate 72/24)

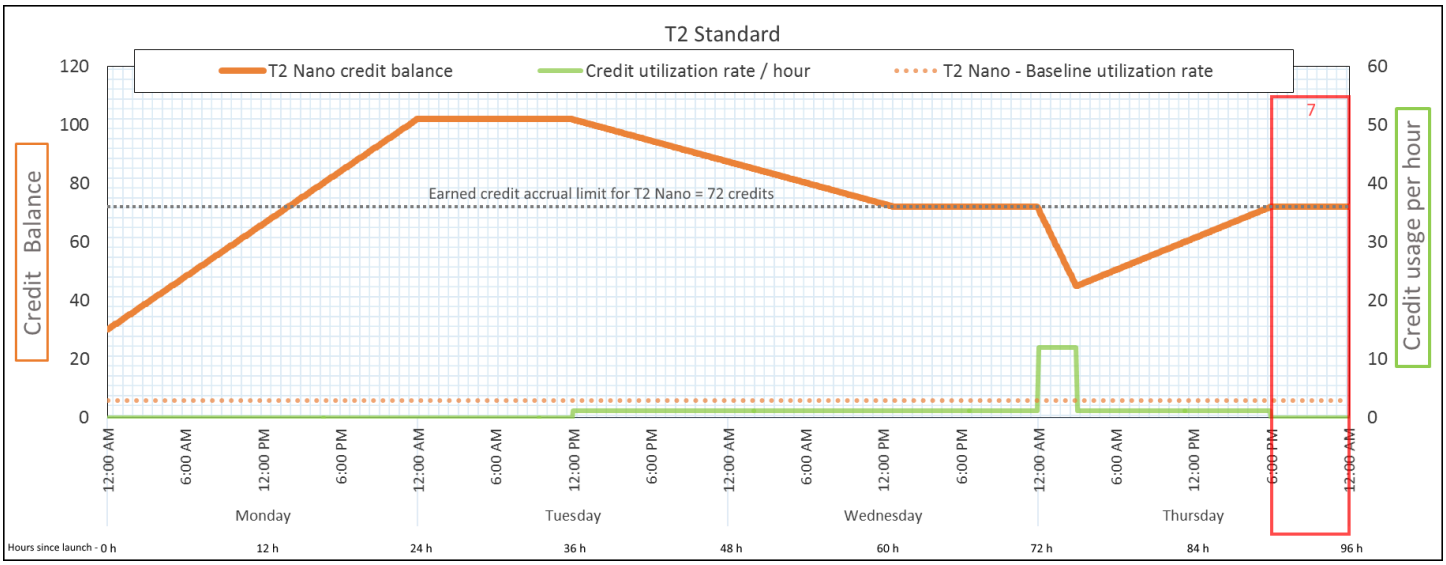
Schlussfolgerung

Wenn eine Instance weniger Punkte ausgibt, als sie verdient, erhöht sich ihr Guthaben.

Zeitraum 7: 91–96 Stunden

Für die nächsten sechs Stunden bleibt die Instance im Leerlauf, die CPU—Auslastung beträgt 0 % und es werden —keine Punkte ausgegeben. Dies ist die gleiche CPU-Auslastung wie im Zeitraum 2, aber der Saldo erreicht nicht 102 Punkte, sondern 72 Punkte, denn —dies ist das Guthabenlimit für die Instance.

Im Zeitraum 2 enthielt das Guthaben 30 aufgelaufene Punkte des Startguthabens. Das Startguthaben wurde in Zeitraum 3 ausgegeben. Eine laufende Instance kann kein weiteres Startguthaben erhalten. Nach Erreichen des Guthabenlimits werden alle verdienten Punkte, die das Limit überschreiten, verworfen.



Ausgabe-Rate von Guthaben	0 Punkte pro 24 Stunden (0 % CPU-Auslastung)
Erwerbsrate von Guthaben	72 Punkte pro 24 Stunden
Verfall-Rate von Guthaben	72 Punkte pro 24 Stunden (100 % der Erwerbsrate von Guthaben)
Guthaben	72 Punkte (0 Punkte Startguthaben, 72 verdiente Punkte)

Schlussfolgerung

Eine Instance verdient ständig Punkte, kann aber keine weiteren Punkte mehr sammeln, wenn das Guthabenlimit erreicht ist. Nach Erreichen des Limits werden neu verdiente Punkte verworfen. Das Guthabenlimit wird durch die Anzahl der Punkte bestimmt, die eine Instance in 24 Stunden verdienen kann. Weitere Informationen zu Guthabenlimits finden Sie in der Guthabentabelle.

Instances mit Spitzenlastleistung konfigurieren

Die Schritte zum Starten, Überwachen und Bearbeiten von Instances mit Spitzenlastleistung (T-Instances) ähneln sich. Der wichtigste Unterschied ist die standardmäßige Guthaben-Festlegung beim Start.

Jede T-Instance-Familie wird mit der folgenden standardmäßige Guthaben-Spezifikation geliefert:

- T4g-, T3a- und T3-Instances starten als `unlimited`
- T3-Instances auf einem Dedicated Host können nur als `standard` gestartet werden
- T2-Instances starten als `standard`

Sie können die standardmäßige Guthaben-Spezifikation für das Konto ändern.

Aufgaben

- Die Guthaben-Spezifikation beim Start
- Konfigurieren Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe, um die Kreditspezifikation als festzulegen unlimited
- Die Guthabenspezifikation einer Instance mit Spitzenlastleistung verwalten
- Die standardmäßige Guthaben-Spezifikation für ein Konto verwalten

Die Guthaben-Spezifikation beim Start

Sie können Ihre T-Instances mit einer Guthaben-Spezifikation von `unlimited` oder `standard` starten.

Die folgenden Verfahren beschreiben, wie Sie die EC2 Konsole oder die AWS CLI verwenden. Informationen zur Verwendung einer Amazon EC2 Auto Scaling Scaling-Gruppe finden Sie unterKonfigurieren Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe, um die Kreditspezifikation als festzulegen unlimited.

Console

So konfigurieren Sie die Guthaben-Spezifikation einer Instance beim Start

1. Befolgen Sie das Verfahren zum Starten einer Instance.
2. Wählen Sie unter Instance type (Instance-Typ) einen T-Instance-Typ aus.

3. Erweitern Sie Advanced Details (Erweiterte Details). Wählen Sie unter Guthaben-Spezifikation eine Guthaben-Spezifikation aus.
4. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus.

AWS CLI

So legen Sie die Guthaben-Spezifikation einer Instance beim Start fest

Verwenden den Befehl run-instances mit der Option `--credit-specification`.

```
--credit-specification CpuCredits=unlimited
```

PowerShell

So legen Sie die Guthaben-Spezifikation einer Instance beim Start fest

Verwenden Sie das New-EC2InstanceCmdlet mit dem `-CreditSpecification_CpuCredit` Parameter.

```
-CreditSpecification_CpuCredit unlimited
```

Konfigurieren Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe, um die Kreditspezifikation als festzulegen unlimited

Wenn T-Instances gestartet werden, benötigen sie CPU-Guthaben für eine gute Bootstrapping-Erfahrung. Wenn Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe verwenden, um Ihre Instances zu starten, empfehlen wir Ihnen, Ihre Instances als zu konfigurieren`unlimited`. Wenn Sie dies tun, verbrauchen die Instances überschüssiges Guthaben, wenn sie automatisch von der Amazon EC2 Auto Scaling Scaling-Gruppe gestartet oder neu gestartet werden. Mithilfe von überzähligen Guthaben lassen sich Leistungseinschränkungen verhindern.

Erstellen einer Startvorlage

Sie müssen eine Startvorlage zum Starten von Instances wie `unlimited` in einer Amazon EC2 Auto Scaling Scaling-Gruppe verwenden. Eine Startkonfiguration unterstützt das Starten von Instances als `unlimited` nicht.

Console

So erstellen Sie eine Startvorlage, die die Guthaben-Spezifikation festlegt

1. Folgen Sie dem Verfahren Erstellen einer Startvorlage mithilfe erweiterter Einstellungen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.
2. Wählen Sie unter Inhalt der Startvorlage für Instance-Typ eine Instance-Größe aus.
3. Um Instances wie `unlimited` in einer Amazon EC2 Auto Scaling Scaling-Gruppe zu starten, wählen Sie unter Erweiterte Details für Kreditspezifikation die Option Unbegrenzt aus.
4. Wenn Sie die Parameter der Startvorlage definiert haben, wählen Sie Create launch template.

AWS CLI

So erstellen Sie eine Startvorlage, die die Guthaben-Spezifikation festlegt

Verwenden Sie den Befehl create-launch-template.

```
aws ec2 create-launch-template \
    --launch-template-name my-launch-template \
    --version-description FirstVersion \
    --launch-template-data CreditSpecification={CpuCredits=unlimited}
```

PowerShell

So erstellen Sie eine Startvorlage, die die Guthaben-Spezifikation festlegt

Verwenden Sie das cmdlet New-EC2LaunchTemplate. Definieren Sie die Guthaben-Spezifikation für die Daten der Startvorlage wie folgt.

```
$creditSpec = New-Object Amazon.EC2.Model.CreditSpecificationRequest
$creditSpec.CpuCredits = "unlimited"
$launchTemplateData = New-Object Amazon.EC2.Model.RequestLaunchTemplateData
$launchTemplateData.CreditSpecification = $creditSpec
```

Ordnen Sie einer Startvorlage eine Amazon EC2 Auto Scaling Scaling-Gruppe zu

Um die Startvorlage einer Amazon EC2 Auto Scaling Scaling-Gruppe zuzuordnen, erstellen Sie die Amazon EC2 Auto Scaling Scaling-Gruppe mithilfe der Startvorlage oder fügen Sie die Startvorlage einer vorhandenen Amazon EC2 Auto Scaling Scaling-Gruppe hinzu.

Console

So erstellen Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe mithilfe einer Startvorlage

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Navigationsleiste oben auf dem Bildschirm dieselbe Region aus, die Sie bei der Erstellung der Startvorlage angegeben haben.
3. Wählen Sie im Navigationsbereich Amazon EC2 Auto Scaling Scaling-Gruppen, Amazon EC2 Auto Scaling Scaling-Gruppe erstellen aus.
4. Wählen Sie Launch Template (Startvorlage), Ihre Startvorlage und anschließend Next Step (Nächster Schritt) aus.
5. Füllen Sie die Felder für die Amazon EC2 Auto Scaling Scaling-Gruppe aus. Wenn Sie mit der Überprüfung Ihrer Konfigurationseinstellung auf der Seite Review (Überprüfung) fertig sind, wählen Sie Create Auto Scaling group (Auto Scaling-Gruppe erstellen). Weitere Informationen finden Sie unter Erstellen einer Amazon EC2 Auto Scaling Scaling-Gruppe mithilfe einer Startvorlage im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

So fügen Sie einer vorhandenen Amazon EC2 Auto Scaling Scaling-Gruppe eine Startvorlage hinzu

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Navigationsleiste oben auf dem Bildschirm dieselbe Region aus, die Sie bei der Erstellung der Startvorlage angegeben haben.
3. Wählen Sie im Navigationsbereich Amazon EC2 Auto Scaling Groups aus.
4. Wählen Sie aus der Amazon EC2 Auto Scaling Scaling-Gruppenliste eine Amazon EC2 Auto Scaling Scaling-Gruppe aus und klicken Sie auf Aktionen, Bearbeiten.
5. Wählen Sie auf der Registerkarte Details für Launch Template (Startvorlage) eine Startvorlage und dann Save (Speichern).

AWS CLI

So erstellen Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe mithilfe einer Startvorlage

Verwenden Sie den create-auto-scaling-group-Befehl und geben Sie den `--launch-template`-Parameter an.

So fügen Sie einer vorhandenen Amazon EC2 Auto Scaling Scaling-Gruppe eine Startvorlage hinzu

Verwenden Sie den update-auto-scaling-group-Befehl und geben Sie den `--launch-template`-Parameter an.

PowerShell

So erstellen Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe mithilfe einer Startvorlage

Verwenden Sie das ASAuto ScalingGroup Cmdlet New- und geben Sie den Parameter `-LaunchTemplate_LaunchTemplateId` or `-LaunchTemplate_LaunchTemplateName` an.

So fügen Sie einer vorhandenen Amazon EC2 Auto Scaling Scaling-Gruppe eine Startvorlage hinzu

Verwenden Sie das ASAuto ScalingGroup Cmdlet Update- und geben Sie den Parameter `-LaunchTemplate_LaunchTemplateId` or `-LaunchTemplate_LaunchTemplateName` an.

Die Guthabenspezifikation einer Instance mit Spitzenlastleistung verwalten

Sie können die Guthaben-Spezifikation für die Nutzung einer laufenden oder angehaltenen Instance jederzeit zwischen `unlimited` und `standard` wechseln.

Beachten Sie, dass eine Instance im `unlimited`-Modus überschüssiges Guthaben einsetzen kann, wofür eine zusätzliche Gebühr anfallen kann. Weitere Informationen finden Sie unter Für überzähliges Guthaben können Gebühren anfallen.

Console

So verwalten Sie die Guthaben-Spezifikation einer Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. (Optional) Wählen Sie eine Instance aus. Suchen Sie auf der Registerkarte Details nach Guthaben-Spezifikation. Der Wert ist entweder `unlimited` oder `standard`.
4. (Optional) Um die Guthaben-Spezifikation für mehrere Instances auf einmal zu ändern, wählen Sie alle aus.

5. Wählen Sie Aktionen, Instance-Einstellungen, Change credit specification (Guthabenspezifikation ändern). Diese Option ist nur aktiviert, wenn Sie eine T-Instance ausgewählt haben.
6. Für den Ungebrenzten Modus aktivieren oder deaktivieren Sie das Kontrollkästchen neben jeder Instance-ID.

AWS CLI

So rufen Sie die Guthaben-Spezifikation einer Instance ab

Verwenden Sie den Befehl describe-instance-credit-specifications. Wenn Sie keine Instance-ID angeben, werden alle Instances mit der Guthaben-Spezifikation `unlimited` zurückgegeben. Die Ausgabe würde auch Instances enthalten, die zuvor mit der Guthaben-Spezifikation `unlimited` konfiguriert wurden. Wenn Sie beispielsweise die Größe einer T3-Instance auf eine M4-Instance ändern, während sie als `unlimited` konfiguriert ist, EC2 gibt Amazon die M4-Instance zurück.

```
aws ec2 describe-instance-credit-specifications \
    --instance-id i-1234567890abcdef0 \
    --query InstanceCreditSpecifications[].CpuCredits \
    --output text
```

Es folgt eine Beispielausgabe.

```
unlimited
```

So legen Sie die Guthaben-Spezifikation einer Instance fest

Verwenden Sie den Befehl modify-instance-credit-specification.

```
aws ec2 modify-instance-credit-specification \
    --region us-east-1 \
    --instance-credit-specification
 "InstanceId=i-1234567890abcdef0,CpuCredits=unlimited"
```

PowerShell

So rufen Sie die Guthaben-Spezifikation einer Instance ab

Verwenden Sie das cmdlet Get-EC2CreditSpecification.

```
(Get-EC2CreditSpecification `
    -InstanceId i-1234567890abcdef0).CpuCredits
```

Es folgt eine Beispielausgabe.

```
unlimited
```

So legen Sie die Guthaben-Spezifikation einer Instance fest

Verwenden Sie das cmdlet Edit-EC2InstanceCreditSpecification.

```
Edit-EC2InstanceCreditSpecification `
    -Region us-east-1 `
    -InstanceCreditSpecification @({InstanceId="i-1234567890abcdef0"
 CpuCredits="unlimited"})
```

Die standardmäßige Guthaben-Spezifikation für ein Konto verwalten

Jede T-Instance kommt mit einer standardmäßigen Guthaben-Spezifikation. Sie können die Standard-Kreditspezifikation für jede T-Instance-Familie auf Kontoebene pro Region ändern. AWS Die gültigen Werte für die standardmäßige Guthaben-Spezifikation sind `unlimited` und `standard`.

Wenn Sie den Launch-Instance-Assistenten in der EC2 Konsole verwenden, um Instances zu starten, hat der Wert, den Sie für die Kreditspezifikation auswählen, Vorrang vor der Standard-Kreditspezifikation auf Kontoebene. Wenn Sie den AWS CLI zum Starten von Instances verwenden, werden alle neuen T-Instances im Konto mit der Standard-Kreditspezifikation gestartet. Die Guthaben-Spezifikation für vorhandene laufende oder gestoppte Instances ist nicht davon betroffen.

Überlegungen

Die standardmäßige Guthaben-Spezifikation für eine Instance-Familie kann nur einmal in einem fortlaufenden 5-Minuten-Zeitraum und bis zu viermal in einem fortlaufenden 24-Stunden-Zeitraum geändert werden.

Console

So verwalten Sie die standardmäßige Guthaben-Spezifikation

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im linken Navigationsbereich Dashboard aus. EC2
4. Wählen Sie unter Kontoattribute die Option Standard-Guthaben-Spezifikation aus.
5. Wählen Sie Manage (Verwalten).
6. Wählen Sie für jede Instance-Familie Unlimited oder Standard und dann Update.

AWS CLI

So rufen Sie die standardmäßige Guthaben-Spezifikation ab

Verwenden Sie den Befehl get-default-credit-specification.

```
aws ec2 get-default-credit-specification \
    --region us-east-1 \
    --instance-family t2 \
    --query InstanceFamilyCreditSpecifications[].CpuCredits \
    --output text
```

Es folgt eine Beispielausgabe.

```
standard
```

So legen Sie die standardmäßige Guthaben-Spezifikation fest

Verwenden Sie den Befehl modify-default-credit-specification. Im folgenden Beispiel wird der Wert auf `unlimited` festgelegt.

```
aws ec2 modify-default-credit-specification \
    --region us-east-1 \
    --instance-family t2 \
    --cpu-credits unlimited
```

PowerShell

So rufen Sie die standardmäßige Guthaben-Spezifikation ab

Verwenden Sie das cmdlet Get-EC2DefaultCreditSpecification.

```
(Get-EC2DefaultCreditSpecification `
```

```
    -Region us-east-1 `
    -InstanceFamily t2).CpuCredits
```

Es folgt eine Beispielausgabe.

```
standard
```

So legen Sie die standardmäßige Guthaben-Spezifikation fest

Verwenden Sie das cmdlet Edit-EC2DefaultCreditSpecification. Im folgenden Beispiel wird der Wert auf `unlimited` festgelegt.

```
Edit-EC2DefaultCreditSpecification `
    -Region us-east-1 `
    -InstanceFamily t2 `
    -CpuCredit unlimited
```

CPU-Guthaben auf Instances mit Spitzenlastleistung überwachen

EC2 sendet Metriken an Amazon CloudWatch. Sie können die CPU-Guthabenmetriken in den EC2 Amazon-Instanz-Metriken der CloudWatch Konsole einsehen oder indem Sie die AWS CLI Metriken für jede Instance auflisten. Weitere Informationen finden Sie unter CloudWatch Metriken, die für Ihre Instances verfügbar sind.

Inhalt

- Zusätzliche CloudWatch Metriken für Instances mit hoher Leistung
- Berechnung der CPU-Guthabennutzung

Zusätzliche CloudWatch Metriken für Instances mit hoher Leistung

Burstable Performance-Instances verfügen über diese zusätzlichen CloudWatch Metriken, die alle fünf Minuten aktualisiert werden:

- `CPUCreditUsage` – Die Anzahl des während des Messzeitraums verbrauchten CPU-Guthabens.
- `CPUCreditBalance` – Die Anzahl von CPU-Guthaben, die eine Instance angesammelt hat. Dieser Saldo wird während der Steigerung der CPU-Leistung aufgebraucht, da die CPU-Guthaben schneller verbraucht als erworben werden.

- `CPUSurplusCreditBalance` – Die Anzahl der überzähligen CPU-Guthaben, die zur Aufrechterhaltung der CPU-Auslastung verwendet werden, wenn der `CPUCreditBalance`-Wert gleich Null ist.
- `CPUSurplusCreditsCharged` – Die Anzahl des überzähligen CPU-Guthabens, das die Höchstzahl des CPU-Guthabens überschritten hat, das in einem 24-Stunden-Zeitraum erworben werden kann, und für das daher eine zusätzliche Gebühr erhoben wird.

Die beiden letzten Metriken treffen nur auf Instances zu, die als `unlimited` konfiguriert wurden.

In der folgenden Tabelle werden die CloudWatch Metriken für Burstable-Performance-Instances beschrieben. Weitere Informationen finden Sie unter CloudWatch Metriken, die für Ihre Instances verfügbar sind.

Metrik	Beschreibung
`CPUCreditUsage`	Die Anzahl der von der Instance für die CPU-Nutzung verbrauchten CPU-Guthaben. Ein CPU-Guthaben entspricht einer vCPU, die eine Minute lang bei 100% Auslastung läuft, oder einer äquivalenten Kombination aus vCPUs, Auslastung und Zeit (z. B. eine vCPU, die zwei Minuten lang mit 50% Auslastung läuft oder zwei v, die zwei Minuten lang mit 25% Auslastung CPUs laufen). Die Metriken für CPU-Guthaben sind nur mit einer fünfminütigen Frequenz verfügbar. Wenn Sie ein größeres Intervall als 5 Minuten angeben, verwenden Sie die Statistik `Sum` anstelle der Statistik `Average`. Einheiten: Guthaben (vCPU-Minuten)
`CPUCreditBalance`	Die Anzahl verdienter CPU-Guthaben, die eine Instance angesammelt hat, seit sie gestartet wurde. Für T2 Standard beinhaltet `CPUCreditBalance` auch die Anzahl der angesammelten Startguthaben. Guthaben werden auf dem Guthaben-Konto angesammelt, nachdem sie verdient wurden, und davon entfernt, wenn sie verbraucht werden. Der Guthaben-Kontostand hat ein

Metrik	Beschreibung
	maximales Limit, das anhand der Instance-Größe bestimmt wird. Nachdem das Limit erreicht ist, verfallen alle neu verdienten Guthabenpunkte. Für T2 Standard zählen Startguthaben nicht zum Limit. Die Guthaben in `CPUCreditBalance` sind verfügbar, um die Leistung der Instance über die Baseline ihrer CPU-Nutzung hinaus zu steigern. Wenn eine Instance ausgeführt wird, verfallen Guthaben im `CPUCreditBalance` nicht. Wenn eine T4g-, T3a- oder T3-Instance angehalten wird, bleibt der `CPUCreditBalance` -Wert sieben Tage lang erhalten. Danach verfallen alle angesamme lten Guthaben. Wenn eine T2-Instance beendet wird, bleibt der `CPUCreditBalance` -Wert nicht erhalten, und alle angesammelten Guthaben gehen verloren. Die Metriken für CPU-Guthaben sind nur mit einer fünfminütigen Frequenz verfügbar. Einheiten: Guthaben (vCPU-Minuten)
`CPUSurplusCreditBa lance`	Die Anzahl überzähliger Guthaben, die von einer `unlimited` -Instance verbraucht wurden, wenn ihr `CPUCreditBalance` -Wert null ist. Der `CPUSurplusCreditBalance` -Wert wird durch erworbene CPU-Guthaben abgezahlt. Wenn die Anzahl überzähliger Guthaben die Höchstzahl der Guthaben überschre itet, die die Instance in einem 24-Stunden-Zeitraum verdienen kann, fallen für die verbrauchten überzähligen Guthaben zusätzliche Gebühren an. Einheiten: Guthaben (vCPU-Minuten)

Metrik	Beschreibung
`CPUSurplusCreditsCharged`	Die Anzahl verbrauchter überzähliger Guthaben, die nicht durch verdiente CPU-Guthaben zurückgezahlt wurden, und für die deshalb eine zusätzliche Gebühr anfällt. Verbrauchte überzählige Guthaben werden in Rechnung gestellt, wenn einer der folgenden Fälle auftritt: • Die ausgegebenen überzähligen Guthaben überschreiten die maximale Anzahl an Guthaben, die die Instance in einem 24-Stunden-Zeitraum verdienen kann. Über das Maximum hinaus ausgegebene überzählige Guthaben werden am Ende der Stunde abgerechnet. • Die Instance wird angehalten oder beendet. • Die Instance wird von `unlimited` in `standard` geändert. Einheiten: Guthaben (vCPU-Minuten)

Berechnung der CPU-Guthabennutzung

Die CPU-Guthabenauslastung von Instances wird anhand der in der vorherigen Tabelle beschriebenen CloudWatch Instance-Metriken berechnet.

Amazon EC2 sendet die Messwerte CloudWatch alle fünf Minuten. Ein Verweis auf einen vorherigen Wert einer Metrik an einem beliebigen Zeitpunkt setzt den vorherigen Wert der Metrik voraus, der vor fünf Minuten gesendet wurde.

Berechnen der CPU-Guthaben-Nutzung für Standard-Instances

- Der CPU-Guthaben-Kontostand erhöht sich, wenn die CPU-Nutzung unterhalb der Baseline liegt und weniger Guthaben verbraucht werden, als im vorherigen Fünf-Minuten-Zeitraum verdient wurden.
- Der CPU-Guthaben-Kontostand verringert sich, wenn die CPU-Nutzung oberhalb der Baseline liegt und mehr Guthaben verbraucht werden, als im vorherigen Fünf-Minuten-Zeitraum verdient wurden.

Mathematisch wird dies durch die folgende Gleichung erfasst:

Example

```
CPUCreditBalance = prior CPUCreditBalance + [Credits earned per hour * (5/60) -
 CPUCreditUsage]
```

Die Größe der Instance bestimmt die Anzahl der Guthaben, die die Instance pro Stunde verdienen kann, sowie der Anzahl der verdienten Guthaben, die sie auf dem Guthaben-Konto ansammeln kann. Weitere Informationen zur Anzahl der pro Stunde verdienten Guthaben, sowie zum Guthaben-Konto-Limit für die verschiedenen Instance-Größen finden Sie in der Guthabentabelle.

Beispiel

Dieses Beispiel verwendet eine `t3.nano`-Instance. Um den `CPUCreditBalance`-Wert der Instance zu berechnen, verwenden Sie folgendermaßen die obige Gleichung:

- `CPUCreditBalance` – Der aktuelle zu berechnende Guthaben-Kontostand.
- `prior CPUCreditBalance` – Der Guthaben-Kontostand vor fünf Minuten. In diesem Beispiel hat die Instance zwei Guthaben angesammelt.
- `Credits earned per hour` – Eine `t3.nano`-Instance erwirbt sechs Guthaben pro Stunde.
- `5/60`— Stellt das Fünf-Minuten-Intervall zwischen der Veröffentlichung der CloudWatch Kennzahlen dar. Multiplizieren Sie die pro Stunde erworbenen Guthaben mit 5/60 (fünf Minuten), um die Anzahl der Guthaben zu erhalten, die die Instance in den letzten fünf Minuten erworben hat. Eine `t3.nano`-Instance erwirbt alle fünf Minuten 0,5 Guthaben.
- `CPUCreditUsage` – Wie viele Guthaben die Instance in den letzten fünf Minuten verbraucht hat. In diesem Beispiel verbrauchte die Instance in den letzten fünf Minuten ein Guthaben.

Anhand dieser Werte können Sie den `CPUCreditBalance`-Wert berechnen:

Example

```
CPUCreditBalance = 2 + [0.5 - 1] = 1.5
```

Berechnen der CPU-Guthaben-Nutzung für Unlimited-Instances

Wenn eine Burstable Performance Instance ihre Leistung über die Baseline hinaus steigern muss, verbraucht sie immer zuerst die verdienten Guthaben, bevor sie die überzähligen Guthaben verbraucht. Wenn ihr angesammeltes CPU-Guthaben aufgebraucht ist, kann sie so lange wie nötig zur CPU-Leistungssteigerung überzählige Guthaben verbrauchen. Wenn die CPU-Nutzung die

Baseline unterschreitet, werden immer zuerst überzählige Guthaben abgezahlt, bevor die Instance erworbene Guthaben ansammelt.

Wir verwenden den Begriff `Adjusted balance` in den folgenden Gleichungen zur Bezeichnung der Aktivität, die in diesem Fünf-Minuten-Intervall stattfindet. Wir verwenden diesen Wert, um die Werte für die `CPUSurplusCreditBalance` CloudWatch Metriken `CPUCreditBalance` und zu ermitteln.

Example

```
Adjusted balance = [prior CPUCreditBalance - prior CPUSurplusCreditBalance] + [Credits
 earned per hour * (5/60) - CPUCreditUsage]
```

Ein Wert von `0` für `Adjusted balance` bedeutet, dass die Instance alle ihre verdienten Guthaben für die Leistungssteigerung verbraucht hat und keine überzähligen Guthaben verwendet wurden. Dies hat zur Folge, dass sowohl `CPUCreditBalance` als auch `CPUSurplusCreditBalance` auf `0` eingestellt werden.

Ein Wert von `Adjusted balance` bedeutet, dass die Instance erworbene Guthaben angesammelt hat und dass vorherige überzählige Guthaben, sofern vorhanden, abgezahlt wurden. Dies hat zur Folge, dass der `Adjusted balance`-Wert `CPUCreditBalance` zugewiesen und `CPUSurplusCreditBalance` auf `0` eingestellt wird. Die Instance-Größe bestimmt die maximale Anzahl an Guthaben, die die Instance ansammeln kann.

Example

```
CPUCreditBalance = min [max earned credit balance, Adjusted balance]
CPUSurplusCreditBalance = 0
```

Ein negativer Wert für `Adjusted balance` bedeutet, dass die Instance alle verdienten, angesammelte Guthaben verbraucht und zudem überzählige Guthaben für die Leistungssteigerung ausgegeben hat. Dies hat zur Folge, dass der `Adjusted balance`-Wert `CPUSurplusCreditBalance` zugewiesen und `CPUCreditBalance` auf `0` eingestellt wird. Auch hier bestimmt die Instance-Größe die maximale Anzahl an Guthaben, die die Instance ansammeln kann.

Example

```
CPUSurplusCreditBalance = min [max earned credit balance, -Adjusted balance]
CPUCreditBalance = 0
```

Wenn die ausgegebenen überzähligen Guthaben die Höchstzahl der Guthaben überschreiten, die die Instance ansammeln kann, wird der überzählige Guthaben-Kontostand wie in der obigen Gleichung veranschaulicht auf die Höchstzahl eingestellt. Für die restlichen überzähligen Guthaben werden wie von der `CPUSurplusCreditsCharged`-Metrik repräsentiert Gebühren berechnet.

Example

```
CPUSurplusCreditsCharged = max [-Adjusted balance - max earned credit balance, 0]
```

Wenn die Instance beendet wird, werden schließlich für alle im `CPUSurplusCreditBalance` nachverfolgten überzähligen Guthaben Gebühren berechnet. Wenn die Instance von `unlimited` in `standard` geändert wird, werden für den gesamten verbleibenden `CPUSurplusCreditBalance` ebenfalls Gebühren berechnet.

Leistungsbeschleunigung mit GPU-Instances

GPU-basierte Instances bieten Zugriff auf NVIDIA GPUs mit Tausenden von Rechenkernen. Mit diesen Instances können Sie wissenschaftliche, technische und Rendering-Anwendungen beschleunigen, indem Sie das CUDA- oder OpenCL-Framework (Open Computing Language) für die parallele Datenverarbeitung verwenden. Sie können sie außerdem für Grafikanwendungen verwenden, u. a. das Streamen von Spielen und 3-D-Anwendungen sowie andere Grafik-Workloads.

Bevor Sie eine GPU-basierte Instance aktivieren oder optimieren können, müssen Sie die entsprechenden Treiber wie folgt installieren:

- Informationen zum Installieren von NVIDIA-Treibern auf einer Instance mit einer angeschlossenen NVIDIA-GPU, z. B. einer P3- oderG4DN-Instance, finden Sie unter NVIDIA-Treiber.
- Informationen zum Installieren von AMD-Treibern auf einer Instance mit einer angeschlossenen AMD-GPU, z. B. einer G4ad-Instance, finden Sie unter AMD-Treiber.

Inhalt

- Aktivieren Sie virtuelle NVIDIA GRID-Anwendungen auf Ihren Amazon EC2 GPU-basierten Instances
- Optimieren Sie die GPU-Einstellungen auf EC2 Amazon-Instances
- Dual-4K-Displays in G4ad-Linux-Instances einrichten
- Erste Schritte mit GPU-beschleunigten Instances

Aktivieren Sie virtuelle NVIDIA GRID-Anwendungen auf Ihren Amazon EC2 GPU-basierten Instances

Um die virtuellen GRID-Anwendungen auf GPU-basierten Instances mit NVIDIA zu aktivieren GPUs (NVIDIA GRID Virtual Workstation ist standardmäßig aktiviert), müssen Sie den Produkttyp für den Treiber definieren. Der Prozess, den Sie verwenden, ist vom Betriebssystem Ihrer Instance abhängig.

Linux-Instances

So aktivieren Sie GRID Virtual Applications auf Ihren Linux-Instances

1. Erstellen Sie die Datei `/etc/nvidia/gridd.conf` aus der bereitgestellten Vorlagendatei.

   ```
   [ec2-user ~]$ sudo cp /etc/nvidia/gridd.conf.template /etc/nvidia/gridd.conf
   ```

2. Öffnen Sie die Datei `/etc/nvidia/gridd.conf` in Ihrem bevorzugten Texteditor.
3. Suchen Sie die Zeile `FeatureType` und setzen Sie den Wert auf `0`. Fügen Sie dann eine Zeile mit `IgnoreSP=TRUE` hinzu.

   ```
   FeatureType=0 IgnoreSP=TRUE
   ```

4. Speichern Sie die Datei und schließen Sie sie.
5. Starten Sie die Instance neu, damit die neue Konfiguration übernommen und angezeigt wird.

   ```
   [ec2-user ~]$ sudo reboot
   ```

Windows-Instances

So aktivieren Sie GRID Virtual Applications auf Ihren Windows-Instances

1. Führen Sie regedit.exe aus, um den Registrierungs-Editor zu öffnen.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global \GridLicensing`.
3. Öffnen Sie im rechten Bereich das Kontextmenü (Rechtsklick) und wählen Sie Neu und DWORD aus.
4. Geben Sie als Namen ein FeatureTypeund geben Sie ein. `Enter`
5. Öffnen Sie das Kontextmenü (Rechtsklick) FeatureTypeund wählen Sie Ändern.

6. Geben Sie für Wertdaten den Wert `0` for NVIDIA GRID Virtual Applications ein und wählen Sie OK.
7. Öffnen Sie im rechten Bereich das Kontextmenü (Rechtsklick) und wählen Sie Neu und DWORD aus.
8. Geben sie unter Name den Wert IgnoreSP und danach `Enter` ein.
9. Öffnen Sie das Kontextmenü (Rechtsklick) für IgnoreSP und wählen Sie Ändern aus.
10. Geben Sie für Wertdaten 1 ein und wählen Sie OK.
11. Schließen Sie den Registrierungs-Editor.

Optimieren Sie die GPU-Einstellungen auf EC2 Amazon-Instances

Sie können verschiedene Optimierungen an den GPU-Einstellungen vornehmen, um die bestmögliche Leistung in Ihren NVIDIA-GPU-Instances zu erzielen. Bei einigen dieser Instance-Typen verwendet der NVIDIA-Treiber ein Autoboost-Feature, das die GPU-Taktfrequenzen variiert. Wenn Sie die Autoboost-Funktion deaktivieren und die GPU-Taktfrequenzen auf den maximalen Wert einstellen, können Sie in Ihren GPU-Instances permanent die maximale Leistung abrufen.

GPU-Einstellungen in Linux optimieren

1. Konfigurieren Sie die GPU für persistente Leistung. Die Ausführung dieses Befehls kann mehrere Minuten in Anspruch nehmen.

   ```
   [ec2-user ~]$ sudo nvidia-persistenced
   ```

2. [Nur G3- und P2-Instances] Deaktivieren Sie die Autoboost-Funktion für alle GPUs Instances.

   ```
   [ec2-user ~]$ sudo nvidia-smi --auto-boost-default=0
   ```

3. Setzen Sie alle GPU-Taktfrequenzen auf den Maximalwert. Verwenden Sie die in den folgenden befehlen angegebenen Speicher- und Grafik-Taktraten.

   Einige Versionen des NVIDIA-Treibers unterstützen keine Einstellung der Taktrate der Anwendung und werfen den `"Setting applications clocks is not supported for GPU..."`-Fehler auf, den Sie ignorieren können.

   - G3-Instances:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 2505,1177
     ```

- G4dn-Instances:

```
[ec2-user ~]$ sudo nvidia-smi -ac 5001,1590
```

- G5-Instances:

```
[ec2-user ~]$ sudo nvidia-smi -ac 6250,1710
```

- G6-, G6f-, Gr6- und Gr6f-Instances:

```
[ec2-user ~]$ sudo nvidia-smi -ac 6251,2040
```

- G6e-Instances:

```
[ec2-user ~]$ sudo nvidia-smi -ac 9001,2520
```

- P2-Instances:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2505,875
```

- P3- und P3dn-Instances:

```
[ec2-user ~]$ sudo nvidia-smi -ac 877,1530
```

- P4d-Instances:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1215,1410
```

- P4de-Instances:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1593,1410
```

- P5-Instances:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2619,1980
```

- P5e- und P5en-Instances:

```
[ec2-user ~]$ sudo nvidia-smi -ac 3201,1980
```

- P6-B200-Instances:

```
[ec2-user ~]$ sudo nvidia-smi -ac 3996,1965
```

- P6-B300-Instanzen:

```
[ec2-user ~]$ sudo nvidia-smi -ac 3996,2032
```

Optimieren der GPU-Einstellungen in Windows

1. Öffnen Sie ein PowerShell Fenster und navigieren Sie zum NVIDIA-Installationsordner.

```
PS C:\> cd "C:\Windows\System32\DriverStore\FileRepository\nvgridsw_aws.inf_*\"
```

2. [Nur G3- und P2-Instances] Deaktivieren Sie die Autoboost-Funktion für alle GPUs Instances.

```
PS C:\> .\nvidia-smi --auto-boost-default=0
```

3. Setzen Sie alle GPU-Taktfrequenzen auf den Maximalwert. Verwenden Sie die in den folgenden befehlen angegebenen Speicher- und Grafik-Taktraten.

   Einige Versionen des NVIDIA-Treibers unterstützen keine Einstellung der Taktrate der Anwendung und werfen den `"Setting applications clocks is not supported for GPU..."`-Fehler auf, den Sie ignorieren können.

   - G3-Instances:

```
PS C:\> .\nvidia-smi -ac "2505,1177"
```

   - G4dn-Instances:

```
PS C:\> .\nvidia-smi -ac "5001,1590"
```

   - G5-Instances:

```
PS C:\> .\nvidia-smi -ac "6250,1710"
```

   - G6-, G6f-, Gr6- und Gr6f-Instances:

```
PS C:\> .\nvidia-smi -ac "6251,2040"
```

- G6e-Instances:

```
PS C:\> .\nvidia-smi -ac "9001,2520"
```

- P2-Instances:

```
PS C:\> .\nvidia-smi -ac "2505,875"
```

- P3- und P3dn-Instances:

```
PS C:\> .\nvidia-smi -ac "877,1530"
```

Dual-4K-Displays in G4ad-Linux-Instances einrichten

Nachdem Sie eine G4ad-Instance gestartet haben, können Sie zwei 4K-Displays einrichten.

So installieren Sie die AMD-Treiber und konfigurieren Dual-Bildschirme

1. Stellen Sie eine Verbindung zu Ihrer Linux-Instance her, um die PCI-Bus-Adresse der GPU zu erhalten, die Sie für Dual 4K (2x4k) anzielen möchten:

   ```
   lspci -vv | grep -i amd
   ```

   Sie erhalten eine Ausgabe, die dem Folgenden ähnelt:

   ```
   00:1e.0 Display controller: Advanced Micro Devices, Inc. [*AMD*/ATI] Device 7362 (rev
    c3)
   Subsystem: Advanced Micro Devices, Inc. [AMD/ATI] Device 0a34
   ```

2. Beachten Sie, dass die PCI-Bus-Adresse in der obigen Ausgabe 00:1e.0 lautet. Erstellen Sie eine Datei mit dem Namen `/etc/modprobe.d/amdgpu.conf` und fügen Sie Folgendes hinzu:

   ```
   options amdgpu virtual_display=0000:00:1e.0,2
   ```

3. Informationen zum Installieren der AMD-Treiber in Linux finden Sie unter AMD-Treiber für Ihre EC2-Instance. Wenn Sie den AMD-GPU-Treiber bereits installiert haben, müssen Sie die amdgpu-Kernelmodule über dkms neu erstellen.
4. Verwenden Sie die folgende xorg.conf-Datei, um die duale (2x4K) Bildschirmtopologie zu definieren, und speichern Sie die Datei in `/etc/X11/xorg.conf`:

```
~$ cat /etc/X11/xorg.conf
Section "ServerLayout"
    Identifier     "Layout0"
    Screen          0 "Screen0"
    Screen        1 "Screen1"
    InputDevice     "Keyboard0" "CoreKeyboard"
    InputDevice     "Mouse0" "CorePointer"
    Option          "Xinerama" "1"
EndSection
Section "Files"
    ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
    ModulePath "/opt/amdgpu/lib/xorg/modules"
    ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
    ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
    ModulePath "/usr/lib64/xorg/modules"
    ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Mouse0"
    Driver         "mouse"
    Option         "Protocol" "auto"
    Option         "Device" "/dev/psaux"
    Option         "Emulate3Buttons" "no"
    Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Keyboard0"
    Driver         "kbd"
EndSection

Section "Monitor"
    Identifier     "Virtual"
    VendorName     "Unknown"
    ModelName      "Unknown"
    Option         "Primary" "true"
EndSection

Section "Monitor"
    Identifier     "Virtual-1"
    VendorName     "Unknown"
    ModelName      "Unknown"
```

```
    Option         "RightOf" "Virtual"
EndSection

Section "Device"
    Identifier     "Device0"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Device"
    Identifier     "Device1"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Extensions"
    Option         "DPMS" "Disable"
EndSection

Section "Screen"
    Identifier     "Screen0"
    Device         "Device0"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection

Section "Screen"
    Identifier     "Screen1"
    Device         "Device1"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
```

```
    EndSubSection
EndSection
```

5. Richten Sie DCV ein, indem Sie die Anweisungen zum Einrichten eines interaktiven Desktops befolgen.
6. Nachdem die DCV-Einrichtung abgeschlossen ist, starten Sie neu.
7. Vergewissern Sie sich, dass der Treiber funktioniert:

```
dmesg | grep amdgpu
```

   Die Antwort sollte wie folgt aussehen:

```
Initialized amdgpu
```

8. Sie sollten in der Ausgabe für `DISPLAY=:0 xrandr -q` sehen, dass Sie 2 virtuelle Displays angeschlossen haben:

```
~$ DISPLAY=:0 xrandr -q
Screen 0: minimum 320 x 200, current 3840 x 1080, maximum 16384 x 16384
Virtual connected primary 1920x1080+0+0 (normal left inverted right x axis y axis)
 0mm x 0mm
 4096x3112  60.00
 3656x2664  59.99
 4096x2160  60.00
 3840x2160  60.00
 1920x1200  59.95
 1920x1080  60.00
 1600x1200  59.95
 1680x1050  60.00
 1400x1050  60.00
 1280x1024  59.95
 1440x900 59.99
 1280x960 59.99
 1280x854 59.95
 1280x800 59.96
 1280x720 59.97
 1152x768 59.95
 1024x768 60.00 59.95
 800x600  60.32 59.96 56.25
 848x480  60.00 59.94
 720x480  59.94
```

```
 640x480  59.94 59.94
Virtual-1 connected 1920x1080+1920+0 (normal left inverted right x axis y axis) 0mm x
 0mm
 4096x3112  60.00
 3656x2664  59.99
 4096x2160  60.00
 3840x2160  60.00
 1920x1200  59.95
 1920x1080  60.00
 1600x1200  59.95
 1680x1050  60.00
 1400x1050  60.00
 1280x1024  59.95
 1440x900 59.99
 1280x960 59.99
 1280x854 59.95
 1280x800 59.96
 1280x720 59.97
 1152x768 59.95
 1024x768 60.00 59.95
 800x600  60.32 59.96 56.25
 848x480  60.00 59.94
 720x480  59.94
640x480  59.94 59.94
```

9. Wenn Sie eine Verbindung zu DCV herstellen, ändern Sie die Auflösung auf 2x4K, um sicherzustellen, dass die Unterstützung für zwei Monitore von DCV registriert wird.

Interaktiven Desktop für Linux einrichten

Nachdem Sie bestätigt haben, dass in Ihrer Linux-Instance der AMD-GPU-Treiber installiert ist und amdgpu verwendet wird, können Sie einen interaktiven Desktop-Manager installieren. Wir empfehlen die MATE-Desktop-Umgebung für die beste Kompatibilität und Leistung.

Voraussetzung

Öffnen Sie einen Texteditor und speichern Sie Folgendes als eine Datei mit dem Namen `xorg.conf`. Sie benötigen diese Datei auf Ihrer Instance.

```
Section "ServerLayout"
Identifier     "Layout0"
Screen          0 "Screen0"
InputDevice     "Keyboard0" "CoreKeyboard"
InputDevice     "Mouse0" "CorePointer"
EndSection
Section "Files"
ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
ModulePath "/opt/amdgpu/lib/xorg/modules"
ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
ModulePath "/usr/lib64/xorg/modules"
ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Mouse0"
Driver         "mouse"
Option         "Protocol" "auto"
Option         "Device" "/dev/psaux"
Option         "Emulate3Buttons" "no"
Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Keyboard0"
Driver         "kbd"
EndSection
Section "Monitor"
Identifier     "Monitor0"
VendorName     "Unknown"
ModelName      "Unknown"
EndSection
Section "Device"
Identifier     "Device0"
Driver         "amdgpu"
VendorName     "AMD"
BoardName      "Radeon MxGPU V520"
BusID          "PCI:0:30:0"
EndSection
Section "Extensions"
Option         "DPMS" "Disable"
EndSection
```

```
Section "Screen"
Identifier     "Screen0"
Device         "Device0"
Monitor        "Monitor0"
DefaultDepth   24
Option         "AllowEmptyInitialConfiguration" "True"
SubSection "Display"
    Virtual    3840 2160
    Depth      32
EndSubSection
EndSection
```

Einrichten eines interaktiven Desktops auf Amazon Linux 2

1. Installieren Sie das EPEL-Repository.

   ```
   [ec2-user ~]$ sudo amazon-linux-extras install epel -y
   ```

2. Installieren Sie den MATE-Desktop.

   ```
   [ec2-user ~]$ sudo amazon-linux-extras install mate-desktop1.x -y
   [ec2-user ~]$ sudo yum groupinstall "MATE Desktop" -y
   [ec2-user ~]$ sudo systemctl disable firewalld
   ```

3. Kopieren Sie die `xorg.conf`-Datei nach `/etc/X11/xorg.conf`.
4. Starten Sie die Instance neu.

   ```
   [ec2-user ~]$ sudo reboot
   ```

5. (Optional) Installieren Sie den Amazon-DCV-Server, um Amazon-DCV als leistungsstarkes Anzeigeprotokoll zu verwenden, und verbinden Sie sich dann mit einer Amazon-DCV-Sitzung) mit Ihrem bevorzugten Client.

Einrichten eines interaktiven Desktops auf Ubuntu

1. Installieren Sie den MATE-Desktop.

   ```
   $ sudo apt install xorg-dev ubuntu-mate-desktop -y
   $ sudo apt purge ifupdown -y
   ```

2. Kopieren Sie die `xorg.conf`-Datei nach `/etc/X11/xorg.conf`.

3. Starten Sie die Instance neu.

```
$ sudo reboot
```

4. Installieren Sie den AMF-Encoder für die entsprechende Version von Ubuntu.

```
$ sudo apt install ./amdgpu-pro-20.20-*/amf-amdgpu-pro_20.20-*_amd64.deb
```

5. (Optional) Installieren Sie den Amazon-DCV-Server, um Amazon-DCV als leistungsstarkes Anzeigeprotokoll zu verwenden, und verbinden Sie sich dann mit einer Amazon-DCV-Sitzung) mit Ihrem bevorzugten Client.
6. Geben Sie nach der DCV-Installation dem DCV-Benutzer Videoberechtigungen ein:

```
$ sudo usermod -aG video dcv
```

Einrichten eines interaktiven Desktops auf CentOS

1. Installieren Sie das EPEL-Repository.

```
$ sudo yum update -y
$ sudo yum install epel-release -y
```

2. Installieren Sie den MATE-Desktop.

```
$ sudo yum groupinstall "MATE Desktop" -y
$ sudo systemctl disable firewalld
```

3. Kopieren Sie die `xorg.conf`-Datei nach `/etc/X11/xorg.conf`.
4. Starten Sie die Instance neu.

```
$ sudo reboot
```

5. (Optional) Installieren Sie den Amazon-DCV-Server, um Amazon-DCV als leistungsstarkes Anzeigeprotokoll zu verwenden, und verbinden Sie sich dann mit einer Amazon-DCV-Sitzung) mit Ihrem bevorzugten Client.

Erste Schritte mit GPU-beschleunigten Instances

Die neueste Generation von GPU-beschleunigten Instance-Typen, wie sie in der folgenden Liste aufgeführt sind, bieten die leistungsstärksten Funktionen für Deep-Learning- und High Performance Computing (HPC)-Anwendungen. Wählen Sie den Link zum Instancetyp aus, um mehr über seine Funktionen zu erfahren.

- P6-Familie
- P6-Familie
- P5-Familie

Eine vollständige Liste der Instance-Typspezifikationen für beschleunigte Instance-Typen finden Sie unter Accelerated Computing in der Amazon EC2 Instance Types-Referenz.

Softwarekonfiguration

Der einfachste Weg, mit den GPU-beschleunigten Instance-Typen der neuesten Generation zu beginnen, besteht darin, eine Instance über ein AWS Deep Learning-AMI zu starten, das mit der gesamten erforderlichen Software vorkonfiguriert ist. Aktuelle Informationen AWS Deep Learning AMIs zur Verwendung mit GPU-beschleunigten Instance-Typen finden Sie unter P6 Supported DLAMI im AWS Deep Learning AMIs Developer Guide.

Wenn Sie ein benutzerdefiniertes AMI erstellen müssen, um Instances zu starten, die Deep-Learning- oder HPC-Anwendungen hosten, sollten Sie zusätzlich zu Ihrem Basis-Image die folgenden Mindest-Software-Versionen installieren:

Instance-Typ	NVIDIA-Treiber	CUDA	NVIDIA GDRCopy	EFA-Installer	NCCL	EFA K8s [1]
P5	530	12,1	2.3	1.24.1	2.18.3	0.4.4
P5.4xlarge	530	12,1	2.3	1.43.1 [2]	2.18.3	0.4.4
P5e	550	12,1	2.3	1.24.1	2.18.3	0.5.5
P5en	550	12,1	2.3	1.24.1	2.18.3	0.5.6
P6-B200	570	12,8	2.5	1,41,0	2.26.2-1	0.5,10

Instance-Typ	NVIDIA-Treiber	CUDA	NVIDIA GDRCopy	EFA-Installer	NCCL	EFA K8s [1]
P6e-0 GB2	570	12,8	2.5	1,41,0	2.26.2-1	0.5,10
P6-B300	580	13,0	2.5	1,44,0	2,28,3	0.5,10

[1] Die Spalte EFA K8s enthält die empfohlene Mindestversion für `aws-efa-k8s-device-plugin`.

[2] Es gibt ein Kompatibilitätsproblem, das `P5.4xlarge` Instanzen betrifft, in denen der Elastic Fabric Adapter (EFA) und die NVIDIA Collective Communications Library (NCCL) für die GPU-to-GPU Kommunikation verwendet werden. Um das Problem zu beheben, setzen Sie die Umgebungsvariable `FI_HMEM_DISABLE_P2P` auf 1 und stellen Sie sicher, dass Sie EFA Version 1.43.1 oder neuer installieren.

> **Note**
>
> Wenn Sie Version 1.41.0 des EFA-Installationsprogramms verwenden, ist `aws-ofi-nccl plugin` enthalten. Verwenden Sie für frühere Versionen des EFA-Installationsprogramms `aws-ofi-nccl plugin` Version `1.7.2-aws` oder höher.

Außerdem empfiehlt es sich, die Instance so zu konfigurieren, dass keine tieferen Ruhezustände verwendet werden. Weitere Informationen finden Sie unter Hohe Performance und geringe Latenz durch die Beschränkung von tieferen C-Zuständen im Benutzerhandbuch für Amazon Linux 2. Die neuesten AWS Deep Learning Base-GPUs AMIs sind so vorkonfiguriert, dass sie keine tieferen C-States verwenden.

Informationen zu Netzwerk und Elastic Fabric Adapter (EFA)-Konfiguration finden Sie unter Maximieren Sie die Netzwerkbandbreite auf EC2 Amazon-Instances mit mehreren Netzwerkkarten.

Amazon EC2 Mac-Instanzen

EC2 Mac-Instances eignen sich ideal zum Entwickeln, Erstellen, Testen und Signieren von Anwendungen für Apple-Plattformen wie iPhone, iPad, Mac, Vision Pro, Apple Watch, Apple TV und Safari. Sie können über SSH oder Apple Remote Desktop (ARD) eine Verbindung mit Ihrer Mac-Instance herstellen.

> **Note**
>
> Die Fakturierungseinheit ist der Dedicated Host. Für die Instances, die auf diesem Host laufen, entstehen keine zusätzlichen Gebühren.

Amazon EC2 Mac-Instances unterstützen nativ das macOS-Betriebssystem.

- EC2 x86-Mac-Instances (`mac1.metal`) basieren auf Mac Mini-Hardware von 2018, die von 3,2 GHz Intel Core i7-Prozessoren der achten Generation (Coffee Lake), 6 physischen und 12 logischen Kernen und 32 GiB Arbeitsspeicher angetrieben wird.
- EC2 M1 Mac-Instances (`mac2.metal`) basieren auf Mac Mini-Hardware von 2020, die von einem Apple Silicon M1-Prozessor, 8 CPU-Kernen, 8 GPU-Kernen, 16 GiB Arbeitsspeicher und der Apple Neural Engine mit 16 Kernen angetrieben wird.
- EC2 M1 Ultra Mac-Instances (`mac2-m1ultra.metal`) basieren auf Mac Studio-Hardware von 2022, die von einem Apple Silicon M1 Ultra-Prozessor, 20 CPU-Kernen, 64 GPU-Kernen, 128 GiB Arbeitsspeicher und der Apple Neural Engine mit 32 Kernen angetrieben wird.
- EC2 M2 Mac-Instances (`mac2-m2.metal`) basieren auf Mac-Mini-Hardware von 2023, die von einem Apple Silicon M2-Prozessor, 8 CPU-Kernen, 10 GPU-Kernen, 24 GiB Arbeitsspeicher und der Apple Neural Engine mit 16 Kernen angetrieben wird.
- EC2 M2 Pro Mac-Instances (`mac2-m2pro.metal`) basieren auf Mac-Mini-Hardware von 2023, die von einem Apple Silicon M2 Pro-Prozessor, 12 CPU-Kernen, 19 GPU-Kernen, 32 GiB Arbeitsspeicher und der Apple Neural Engine mit 16 Kernen angetrieben wird.
- EC2 M4 Mac-Instances (`mac-m4.metal`) basieren auf Mac-Mini-Hardware von 2024, die von einem Apple Silicon M4-Prozessor, 10 CPU-Kernen, 10 GPU-Kernen, 24 GiB Arbeitsspeicher und der Apple Neural Engine mit 16 Kernen angetrieben wird.
- EC2 M4 Pro Mac Mac-Instances (`mac-m4pro.metal`) basieren auf Mac-Mini-Hardware von 2024, die von einem Apple Silicon M4 Pro-Prozessor, 14 CPU-Kernen, 20 GPU-Kernen, 48 GiB Arbeitsspeicher und der Apple Neural Engine mit 16 Kernen angetrieben wird.

Amazon EC2 Mac Dedicated Hosts unterstützen die auto Wiederherstellung von Dedicated Hosts und die Host-Wartung auf Basis eines Neustarts.

Inhalt

- Überlegungen

- Instance-Bereitschaft
- EC2 macOS AMIs
- EC2 macOS Init
- Amazon EC2 System Monitor für macOS
- Zugehörige Ressourcen
- Starten Sie eine Mac-Instance mit dem AWS-Managementkonsole oder AWS CLI
- Herstellen einer Verbindung zu Ihrer Mac-Instance mithilfe von SSH oder einer GUI
- Aktualisieren Sie das Betriebssystem und die Software auf Amazon EC2 Mac-Instances
- Erhöhen Sie die Größe eines EBS-Volumes auf Ihrer Mac-Instance
- Beenden oder beenden Sie Ihre Amazon EC2 Mac-Instance
- Systemintegritätsschutz für Amazon EC2 Mac-Instances konfigurieren
- Finden Sie unterstützte macOS-Versionen für Ihren Amazon EC2 Mac Dedicated Host
- So abonnieren Sie macOS-AMI-Benachrichtigungen
- Rufen Sie das macOS-AMI IDs mithilfe der AWS Systems Manager Parameter Store API ab
- AMIs Versionshinweise zu Amazon EC2 macOS

Überlegungen

Die folgenden Überlegungen gelten für Mac-Instances:

- Mac-Instances sind auf Dedicated Hosts nur als Bare-Metal-Instances mit einer Mindestzuweisungsdauer von 24 Stunden verfügbar, bevor Sie den Dedicated Host freigeben können. Sie können eine Mac-Instance pro Dedicated Host starten. Sie können den Dedicated Host für die AWS Konten oder Organisationseinheiten innerhalb Ihrer AWS Organisation oder für die gesamte AWS Organisation gemeinsam nutzen.
- Mac-Instanzen sind in verschiedenen Varianten verfügbar AWS-Regionen. Eine Liste der Verfügbarkeit von Mac-Instances in den AWS-Regionen einzelnen Regionen finden Sie unter EC2 Amazon-Instance-Typen nach Regionen.
- Mac-Instances sind nur als On-Demand-Instances verfügbar. Sie sind nicht als Spot-Instances oder Reserved Instances verfügbar. Sie können Geld für Mac-Instances sparen, indem Sie einen Savings Plan erwerben.

- Die Kompatibilität verschiedener Mac-Instanztypen mit bestimmten macOS Amazon Machine Images (AMIs) ist unterschiedlich. Weitere Informationen finden Sie unter AMIs Versionshinweise zu Amazon EC2 macOS.
- EBS-Hotplug wird unterstützt.
- AWS verwaltet oder unterstützt die interne SSD auf der Apple-Hardware nicht. Wir empfehlen dringend, stattdessen Amazon EBS-Volumes zu verwenden. EBSVolumes bieten auf Mac-Instances dieselben Elastizitäts-, Verfügbarkeits- und Haltbarkeitsvorteile wie auf jeder anderen EC2 Instance.
- Wir empfehlen die Verwendung eines Amazon EBS-Volumes mit 10.000 IOPS und 400 MiB/s Durchsatz mit Mac-Instances, um eine optimale Leistung zu erzielen. Weitere Informationen finden Sie unter Amazon-EBS-Volume-Typen im Amazon-EBS-Benutzerhandbuch.
- Mac-Instances unterstützen Amazon EC2 Auto Scaling.
- Auf x86-Mac-Instances sind automatische Softwareupdates deaktiviert. Wir empfehlen, dass Sie Updates anwenden und auf Ihrer Instance testen, bevor Sie die Instance in Produktion nehmen. Weitere Informationen finden Sie unter Aktualisieren Sie das Betriebssystem und die Software auf Amazon EC2 Mac-Instances.
- Wenn Sie eine Mac-Instance anhalten oder beenden, wird ein Scrubbing-Workflow auf Dedicated Host ausgeführt. Weitere Informationen finden Sie unter Beenden oder beenden Sie Ihre Amazon EC2 Mac-Instance.
- **Important**

  Apple-Intelligence-Features sind nicht verfügbar, wenn Mac-Hardware von einem externen Volume gestartet wird. Da EC2 Mac-Instances standardmäßig von externen EBS-Volumes gestartet werden, unterstützen sie keine Apple Intelligence-Funktionen.
- **Warning**

  Nicht verwenden FileVault. Wenn Sie diese Option aktivieren FileVault, kann der Host nicht gestartet werden, da die Partitionen gesperrt sind. Wenn Datenverschlüsselung erforderlich ist, verwenden Sie Amazon-EBS-Verschlüsselung, um Startprobleme und Leistungseinbußen zu vermeiden. Bei der Amazon EBS-Verschlüsselung finden Verschlüsselungsvorgänge auf den Hostservern statt, wodurch die Sicherheit sowohl data-at-rest der Instances als auch data-in-transit zwischen den Instances und ihrem angeschlossenen EBS-Speicher gewährleistet wird. Weitere Informationen finden Sie unter Amazon-EBS-Verschlüsselung im Amazon-EBS-Benutzerhandbuch.

Instance-Bereitschaft

Nachdem Sie eine Mac-Instance gestartet haben, müssen Sie warten, bis die Instance bereit ist, bevor Sie eine Verbindung zu ihr herstellen können. Für ein AWS verkauftes AMI mit einer x86-Mac-Instance oder einer Apple-Silicon-Mac-Instance kann die Startzeit zwischen etwa 6 Minuten und 20 Minuten liegen. Die Startzeit kann sich je nach den ausgewählten Größen von Amazon-EBS-Volumes, der Einbindung zusätzlicher Skripts in Benutzerdaten oder zusätzlich geladener Software in einem benutzerdefinierten macOS-AMI verlängern.

Sie können ein kleines Shell-Skript wie das unten stehende verwenden, um die describe-instance-status API abzufragen, um zu erfahren, wann die Instance bereit ist, eine Verbindung herzustellen. Ersetzen Sie im folgenden Befehl die Beispiel-Instance-ID mit Ihrer eigenen.

```
for i in $(seq 1 200); do aws ec2 describe-instance-status --instance-
ids=i-1234567890abcdef0 \
    --query='InstanceStatuses[0].InstanceStatus.Status'; sleep 5; done;
```

EC2 macOS AMIs

Amazon EC2 macOS wurde entwickelt, um eine stabile, sichere und leistungsstarke Umgebung für Entwickler-Workloads bereitzustellen, die auf Amazon EC2 Mac-Instances ausgeführt werden. EC2 macOS AMIs enthält Pakete, die eine einfache Integration ermöglichen AWS, z. B. Startkonfigurationstools und beliebte AWS Bibliotheken und Tools.

Weitere Informationen zu EC2 macOS AMIs finden Sie unter AMIs Versionshinweise zu Amazon EC2 macOS.

AWS stellt regelmäßig aktualisierte EC2 macOS AMIs bereit, die Updates für Pakete enthalten, die Eigentum von AWS und der neuesten vollständig getesteten macOS-Version sind. Darüber hinaus AWS werden die Updates AMIs mit den neuesten Nebenversionsaktualisierungen oder Hauptversionsupdates bereitgestellt, sobald sie vollständig getestet und überprüft werden können. Wenn Sie keine Daten oder Anpassungen an Ihren Mac-Instances beibehalten müssen, können Sie die neuesten Updates erhalten, indem Sie eine neue Instance mit dem aktuellen AMI starten und dann die vorherige Instance beenden. Andernfalls können Sie auswählen, welche Updates auf Ihre Mac-Instances angewendet werden sollen.

Informationen zum Abonnieren von macOS-AMI-Benachrichtigungen finden Sie unter So abonnieren Sie macOS-AMI-Benachrichtigungen.

EC2 macOS Init

EC2-macOS-Init wird verwendet, um EC2-Mac-Instances beim Start zu initialisieren. Es verwendet Prioritätsgruppen, um logische Aufgabengruppen gleichzeitig auszuführen.

Die launchd-plist-Datei ist `/Library/LaunchDaemons/com.amazon.ec2.macos-init.plist`. Die Dateien für EC2 macOS Init befinden sich in`/usr/local/aws/ec2-macos-init`.

Weitere Informationen finden Sie unter https://github.com/aws/ec2-macos-init.

Amazon EC2 System Monitor für macOS

Amazon EC2 System Monitor für macOS stellt Amazon Metriken zur CPU-Auslastung zur Verfügung CloudWatch. Es sendet diese Messwerte innerhalb von 1 Minute an CloudWatch mehr als ein benutzerdefiniertes serielles Gerät. Sie können diesen Agenten wie folgt aktivieren oder deaktivieren. Er ist standardmäßig aktiviert.

```
sudo setup-ec2monitoring [enable | disable]
```

> **Note**
>
> Amazon EC2 System Monitor für macOS wird derzeit auf Apple Silicon Mac-Instances nicht unterstützt.

Zugehörige Ressourcen

Informationen zu den Preisen erhalten Sie unter Preise.

Weitere Informationen zu Mac-Instances finden Sie unter Amazon EC2 Mac-Instances.

Weitere Informationen zu den Hardware-Spezifikationen und der Netzwerkleistung von Mac-Instances finden Sie unter Allzweck-Instances.

Starten Sie eine Mac-Instance mit dem AWS-Managementkonsole oder AWS CLI

EC2 Mac-Instanzen benötigen einen Dedicated Host. Sie müssen Ihrem Konto zuerst einen Host zuweisen und dann die Instance über den Host starten.

Sie können eine Mac-Instanz mit dem AWS-Managementkonsole oder dem starten AWS CLI.

Starten einer Mac-Instance mit der Konsole

Starten einer Mac-Instance auf einem Dedicated Host

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Weisen Sie den Dedicated Host wie folgt zu:
    a. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
    b. Wählen Sie Dedicated Host zuweisen und gehen Sie wie folgt vor:
        i. Wählen Sie für Instance-Familie eine Mac-Instance-Familie aus. Wenn die Instance-Familie nicht in der Liste erscheint, wird sie in der aktuell ausgewählten Region nicht unterstützt.
        ii. Wählen Sie für Instance-Typ den Instance-Typ anhand der ausgewählten Instance-Familie aus.
        iii. Wählen Sie in Availability Zone die Availability Zone für Dedicated Host aus.
        iv. Für Quantity (Menge) behalten Sie 1.
        v. Wählen Sie Allocate aus.
3. Starten Sie die Instance über den Host wie folgt:
    a. Wählen Sie die von Ihnen erstellte Dedicated Host aus, und klicken Sie dann auf Folgendes:
        i. Wählen Sie Actions (Aktionen), Launch instances onto host (Instances auf Host starten).
        ii. Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) ein macOS-AMI.
        iii. Wählen Sie unter Instance-Typ den Mac-Instance-Typ aus.
        iv. Stellen Sie unter Erweiterte Details sicher, dass Tenancy, Tenancy gehostet von und Tenancy-Host-ID basierend auf dem von Ihnen erstellten Dedicated Host vorkonfiguriert sind. Aktualisieren Sie die Tenancy affinity (Tenancy-Affinität), wenn nötig.
        v. Schließen Sie den Assistenten ab und geben Sie nach Bedarf EBS-Volumes, Sicherheitsgruppen und Schlüsselpaare an.
        vi. Wählen Sie in der Übersicht Launch instance (Instance starten) aus.

b. Auf einer Bestätigungsseite wird Ihnen mitgeteilt, dass die Instance gestartet wird. Wählen Sie View all Instances (Alle Instances anzeigen) aus, um die Bestätigungsseite zu schließen und zur Konsole zurückzukehren. Der anfängliche Status einer Instance ist `pending`. Die Instance ist bereit, wenn sich ihr Status in `running` ändert und Statusprüfungen besteht.

Starten Sie eine Mac-Instance mit dem AWS CLI

Zuweisen eines Dedicated Hosts

Verwenden Sie Befehl allocate-hosts, um einen Dedicated Host für Ihre Mac-Instance zuzuweisen, und ersetzen Sie den `instance-type` durch einen gültigen Mac-Instance-Typ und die `region` und `availability-zone` Ihrer Umgebung entsprechend.

```
aws ec2 allocate-hosts --region us-east-1 --instance-type mac1.metal --availability-
zone us-east-1b --auto-placement "on" --quantity 1
```

Starten der Instance über den Host

Verwenden Sie den Befehl run-instances, um eine Mac-Instance zu starten, und ersetzen Sie wieder den `instance-type` durch einen gültigen Mac-Instance-Typ und die `region` und `availability-zone` durch die zuvor verwendeten.

```
aws ec2 run-instances --region us-east-1 --instance-type mac1.metal --placement
 Tenancy=host --image-id ami_id --key-name my-key-pair
```

Der anfängliche Status einer Instance ist `pending`. Die Instance ist bereit, wenn sich ihr Status in `running` ändert und Statusprüfungen besteht. Verwenden Sie den folgenden describe-instance-statusBefehl, um Statusinformationen für Ihre Instanz anzuzeigen.

```
aws ec2 describe-instance-status --instance-ids i-017f8354e2dc69c4f
```

Im Folgenden finden Sie eine Beispielausgabe für eine Instance, die ausgeführt wird und Statusprüfungen bestanden hat.

```
{
    "InstanceStatuses": [
        {
            "AvailabilityZone": "us-east-1b",
            "InstanceId": "i-017f8354e2dc69c4f",
```

```
            "InstanceState": {
                "Code": 16,
                "Name": "running"
            },
            "InstanceStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
                ],
                "Status": "ok"
            },
            "SystemStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
                ],
                "Status": "ok"
            }
        }
    ]
}
```

Herstellen einer Verbindung zu Ihrer Mac-Instance mithilfe von SSH oder einer GUI

Sie können per SSH oder per grafischer Benutzeroberfläche (GUI) eine Verbindung mit Ihrer Mac-Instance herstellen.

Mehrere Benutzer können gleichzeitig auf das Betriebssystem zugreifen. In der Regel gibt es eine 1:1-user:GUI-Sitzung aufgrund des integrierten Bildschirmfreigabe-Services auf Port 5900. Die Verwendung von SSH in macOS unterstützt mehrere Sitzungen bis zum Limit „Max. Sitzungen“ in der `sshd_config`-Datei.

Herstellung einer Verbindung zu Ihrer Instance mit SSH

Amazon EC2 Mac-Instances erlauben standardmäßig kein Remote-Root-SSH. Das ec2-user-Konto ist für die Fernanmeldung mit SSH konfiguriert. Das ec2-user-Konto hat auch sudo-Privilegien. Nachdem Sie eine Verbindung zu Ihrer Instance hergestellt haben, können Sie weitere Benutzer hinzufügen.

Um die Verbindung mit Ihrer Instance mithilfe von SSH zu unterstützen, starten Sie die Instance mit einem Schlüsselpaar und einer Sicherheitsgruppe, die SSH-Zugriff ermöglicht, und stellen Sie sicher, dass die Instance über eine Internetverbindung verfügt. Sie geben die `.pem`-Datei für das Schlüsselpaar an, wenn Sie eine Verbindung mit der Instance herstellen.

Verwenden Sie die folgende Vorgehensweise, um per SSH-Client eine Verbindung mit Ihrer Mac-Instance herzustellen. Weitere Informationen zu Problemen, die beim Aufbau einer Verbindung zu Instances auftreten können, finden Sie unter Fehlersuche bei Verbindungsproblemen mit Ihrer Amazon-EC2-Linux-Instance.

So stellen Sie per SSH eine Verbindung mit Ihrer Instance her

1. Stellen Sie sicher, dass auf Ihrem lokalen Computer ein SSH-Client installiert ist, indem Sie ssh über die Befehlszeile eingeben. Wenn Ihr Computer den Befehl nicht erkennt, suchen Sie nach einem SSH-Client für Ihr Betriebssystem und installieren Sie ihn.
2. Holen Sie sich den öffentlichen DNS-Namen Ihrer Instance. In der EC2 Amazon-Konsole finden Sie den öffentlichen DNS-Namen sowohl auf den Registerkarten Details als auch auf der Registerkarte Netzwerk. Mithilfe von können Sie den öffentlichen DNS-Namen mithilfe des Befehls describe-instances finden. AWS CLI
3. Suchen Sie die `.pem`-Datei für das Schlüsselpaar, das Sie beim Starten der Instance angegeben haben.
4. Stellen Sie mithilfe des folgenden Befehls ssh unter Angabe des öffentlichen DNS-Namens der Instance und der `.pem`-Datei eine Verbindung zu Ihrer Instance her.

```
ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

Die Passwort-Authentifizierung ist deaktiviert, um Brute-Force-Angriffe zu verhindern. Bevor Sie Änderungen an der SSH-Konfiguration vornehmen, öffnen Sie die `/usr/local/aws/ec2-macos-init/init.toml` und stellen Sie `secureSSHDConfig` auf `false` ein.

Eine Verbindung mit der grafischen Benutzerschnittstelle (GUI) Ihrer Instance herstellen

Verwenden Sie die folgende Vorgehensweise, um per VNC, Apple Remote Desktop (ARD) oder die Apple Screen Sharing-Anwendung (im Lieferumfang von macOS enthalten) eine Verbindung mit der GUI Ihrer Instance herzustellen.

> **Note**
>
> macOS 10.14 und höher erlaubt die Steuerung nur, wenn die Bildschirmfreigabe in den Systemeinstellungen aktiviert ist.

Herstellen einer Verbindung zu Ihrer Instance per ARD- oder VNC-Client

1. Stellen Sie sicher, dass auf Ihrem lokalen Computer ein ARD-Client oder ein VNC-Client installiert ist, der ARD installiert hat. Unter macOS können Sie die integrierte Screen-Sharing-Anwendung nutzen. Andernfalls suchen Sie nach ARD für Ihr Betriebssystem und installieren Sie es.
2. Verbinden Sie sich mit Ihrer Instance über SSH von Ihrem lokalen Computer aus.
3. Richten Sie mit dem passwd-Befehl wie folgt ein Passwort für das ec2-Benutzerkonto ein.

   ```
   [ec2-user ~]$ sudo passwd ec2-user
   ```

4. Installieren und starten Sie macOS Screen Sharing mit dem folgenden Befehl.

   ```
   [ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
   sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
   ```

5. Trennen Sie die Verbindung zur Instance, indem Sie exit eingeben und die Eingabetaste drücken.
6. Stellen Sie von Ihrem Computer aus mit dem folgenden ssh-Befehl eine Verbindung zu Ihrer Instance her. Verwenden Sie zusätzlich zu den im vorherigen Abschnitt gezeigten Optionen die -L-Option, um die Port-Weiterleitung zu aktivieren und den gesamten Datenverkehr auf dem lokalen Port 5900 an den ARD-Server auf der Instance weiterzuleiten.

   ```
   ssh -L 5900:localhost:5900 -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
   ```

7. Verwenden Sie auf Ihrem lokalen Computer den ARD- oder VNC-Client, der ARD unterstützt, um eine Verbindung zu `localhost:5900` herzustellen. Verwenden Sie beispielsweise die Screen-Sharing-Anwendung unter macOS wie folgt:

   a. Öffnen Sie den Finder und wählen Sie Go.

   b. Wählen Sie Mit Server verbinden aus.

c. Geben Sie `vnc://localhost:5900` in das Feld Serveradresse ein.

d. Melden Sie sich wie aufgefordert an und verwenden Sie **`ec2-user`** als Benutzernamen und das Passwort, das Sie für das EC2-Benutzerkonto erstellt haben.

Ändern der macOS-Bildschirmauflösung auf Mac-Instances

Nachdem Sie mit ARD oder einem VNC-Client, der ARD unterstützt, eine Verbindung zu Ihrer EC2 Mac-Instanz hergestellt haben, können Sie die Bildschirmauflösung Ihrer macOS-Umgebung mit allen öffentlich verfügbaren macOS-Tools oder -Dienstprogrammen wie Displayplacer ändern.

So ändern Sie die Bildschirmauflösung mit displayplacer

1. Installieren Sie displayplacer.

```
[ec2-user ~]$ brew tap jakehilborn/jakehilborn && brew install displayplacer
```

2. Zeigen Sie die aktuellen Bildschirminformationen und mögliche Bildschirmauflösungen an.

```
[ec2-user ~]$ displayplacer list
```

3. Wenden Sie die gewünschte Bildschirmauflösung an.

```
[ec2-user ~]$ displayplacer "id:<screenID> res:<width>x<height> origin:(0,0)
 degree:0"
```

   Zum Beispiel:

```
RES="2560x1600"
displayplacer "id:69784AF1-CD7D-B79B-E5D4-60D937407F68 res:${RES} scaling:off
 origin:(0,0) degree:0"
```

Aktualisieren Sie das Betriebssystem und die Software auf Amazon EC2 Mac-Instances

Im folgenden Thema wird erklärt, wie das Betriebssystem und die Software auf Apple-Halbleiter-Mac-Instances (Mac2, Mac2-m1ultra, Mac2-m2, Mac2-m2pro, Mac-m4 und Mac-m4pro) und x86-Mac-Instances (Mac1) aktualisiert werden.

Warning

Die Installation von Beta- oder Vorschauversionen von macOS ist nur auf Apple-Halbleiter-Mac-Instances möglich. Amazon qualifiziert EC2 weder Beta- noch Vorschauversionen von macOS und stellt nicht sicher, dass Instances auch nach einem Update auf eine macOS-Vorserienversion funktionsfähig bleiben.
Der Versuch, Beta- oder Vorschauversionen von macOS auf Amazon EC2 x86-Mac-Instances zu installieren, führt zu einer Verschlechterung Ihres Amazon EC2 Mac Dedicated Hosts, wenn Sie Ihre Instances beenden oder beenden, und verhindert, dass Sie eine neue Instance auf diesem Host starten oder starten können.

Note

Wenn Sie ein direktes macOS-Update durchführen, bevor AWS ein offizielles AMI veröffentlicht, gilt das Update nur für den ausgewählten Host. Wenn Sie andere Hosts haben oder neue Hosts starten, müssen Sie denselben Aktualisierungsvorgang auch auf diesen Hosts durchführen. Für jede macOS-Version ist eine minimale Firmware-Version auf der zugrunde liegenden Apple-Mac-Hardware erforderlich. Das direkte Update aktualisiert nur die Firmware auf dem ausgewählten Host und wird nicht auf andere bestehende oder neue Hosts übertragen. Informationen darüber, welche macOS-Versionen mit Ihrem Amazon EC2 Mac Dedicated Host kompatibel sind, finden Sie unter Unterstützte macOS-Versionen für Ihren Amazon EC2 Mac Dedicated Host finden.

Software in Apple-Silicon-Instances aktualisieren

Voraussetzungen

Aufgrund eines Updates in der Netzwerktreiberkonfiguration ist die ENA-Treiberversion 1.0.2 nicht mit macOS 13.3 oder höher kompatibel. Wenn Sie eine Beta-, Vorschau- oder Produktionsversion von macOS 13.3 oder höher installieren möchten und nicht den neuesten ENA-Treiber installiert haben, gehen Sie folgendermaßen vor, um eine neue Version des Treibers zu installieren.

Installieren einer neuen Version des ENA-Treibers

1. Stellen Sie in einem Terminal-Fenster über SSH eine Verbindung mit Ihrer Apple-Silicon-Mac-Instance her.

2. Verwenden Sie den folgenden Befehl, um Homebrew zu aktualisieren und die ENA-Anwendung in die `Applications`-Datei herunterzuladen.

```
[ec2-user ~]$ brew update
```

```
[ec2-user ~]$ brew install amazon-ena-ethernet-dext
```

3. Trennen Sie die Verbindung zur Instance, indem Sie exit eingeben und die Eingabetaste drücken.
4. Verwenden Sie den VNC-Client, um die ENA-Anwendung zu aktivieren.

   a. Richten Sie den VNC-Client mit Eine Verbindung mit der grafischen Benutzerschnittstelle (GUI) Ihrer Instance herstellen ein.

   b. Sobald Sie mithilfe der Bildschirmfreigabe-Anwendung eine Verbindung zu Ihrer Instance hergestellt haben, wechseln Sie zum Ordner Anwendungen und öffnen Sie die ENA-Anwendung.

   c. Wählen Sie Activate.

   d. Führen Sie den folgenden Befehl im Terminalfenster aus, um sicherzustellen, dass der Treiber korrekt aktiviert wurde. Die Ausgabe des Befehls zeigt, dass sich der alte Treiber im Status „Wird beendet“ und der neue Treiber im Status „Aktiviert“ befindet.

```
systemextensionsctl list;
```

   e. Nach dem Neustart der Instance ist nur der neue Treiber vorhanden.

Das Software-Update durchführen

In Apple-Silicon-Mac-Instances müssen Sie mehrere Schritte ausführen, um ein direktes Betriebssystem-Update durchzuführen. Dies beinhaltet die Delegierung des Besitzes des Amazon-EBS-Root-Volumes an den Administratorbenutzer des EBS-Root-Volumes. Sie können wählen, ob Sie dies entweder automatisch mithilfe einer EC2 Amazon-API oder manuell tun möchten, indem Sie die Befehle auf Ihrer Instance ausführen.

Automated volume ownership delegation (Recommended)

Überlegungen

- Es kann zwischen 30 und 90 Minuten dauern, bis die Aufgabe zur Delegierung des Volume-Besitzes abgeschlossen ist. Während dieser Zeit ist die Instance nicht erreichbar.
- Die folgenden macOS-Versionen werden unterstützt:
  - Mac2 | Mac2-m1ultra – macOS Ventura (Version 13.0 oder höher)
  - Mac2-m2 | Mac2-m2pro – macOS Ventura (Version 13,2 oder höher)
  - Mac-m4 | Mac-m4pro – macOS Sequoia (Version 15.6 oder höher)
- Instances dürfen nur ein bootfähiges Volume haben, und jedes angehängte Volume kann nur einen zusätzlichen Admin-Benutzer haben.

Schritt 1: Legen Sie ein Passwort fest und aktivieren Sie das sichere Token für den Administratorbenutzer des EBS-Root-Volume.

Sie müssen ein Passwort festlegen und das sichere Token für den Administratorbenutzer des Amazon-EBS-Root-Volume (`ec2-user`) aktivieren.

> **Note**
>
> Das Passwort und das sichere Token werden festgelegt, wenn Sie zum ersten Mal über die GUI eine Verbindung zu einer Apple-Halbleiter-Mac-Instance herstellen. Wenn Sie zuvor über die GUI eine Verbindung mit der Instance hergestellt haben, müssen Sie diese Schritte nicht ausführen.

1. Stellen Sie über SSH eine Connect zur Instance her.
2. Legen Sie das Passwort für den `ec2-user`-Benutzer fest.

   ```
   $ sudo /usr/bin/dscl . -passwd /Users/ec2-user
   ```

3. Aktivieren Sie das sichere Token für den `ec2-user`-Benutzer. Geben Sie für `-oldPassword` dasselbe Passwort aus dem vorherigen Schritt an. Geben Sie für `-newPassword` ein anderes Passwort ein. Der folgende Befehl geht davon aus, dass Sie Ihre alten und neuen Passwörter in `.txt`-Dateien gespeichert haben.

```
$ sysadminctl -oldPassword `cat old_password.txt` -newPassword `cat
 new_password.txt`
```

4. Stellen Sie sicher, dass das sichere Token aktiviert ist.

```
$ sysadminctl -secureTokenStatus ec2-user
```

Schritt 2: Delegieren Sie den Besitze des Amazon-EBS-Root-Volumes an den Administratorbenutzer des EBS-Root-Volumes.

Um den Besitz zu delegieren, müssen Sie eine Aufgabe zur Delegierung des Volume-Besitzes erstellen.

1. Verwenden Sie den Befehl create-delegate-mac-volume-ownership-task, um die Aufgabe zu erstellen. Geben Sie für `--instance-id` die ID der Instance an. Geben Sie für `--mac-credentials` die folgenden Anmeldeinformationen an:

   - Administratorbenutzer der internen Festplatte
     - Benutzername – Nur der standardmäßige Administratorbenutzer (`aws-managed-user`) wird unterstützt und standardmäßig verwendet. Sie können keinen anderen Administratorbenutzer angeben.
     - Passwort – Wenn Sie das Standardpasswort für `aws-managed-user` nicht geändert haben, geben Sie das Standardpasswort ein, das leer ist. Andernfalls geben Sie Ihr Passwort ein.
   - Administrator-Benutzer des Amazon-EBS-Root-Volumes
     - Benutzername – Wenn Sie den standardmäßigen Administratorbenutzer nicht geändert haben, geben Sie `ec2-user` an. Geben Sie andernfalls den Benutzernamen für Ihren Administratorbenutzer an.
     - Passwort – Geben Sie das Passwort ein, das Sie in Schritt 1 oben für den Administratorbenutzer des Root-Volumes festgelegt haben.

```
aws ec2 create-delegate-mac-volume-ownership-task \
--instance-id i-1234567890abcdef0 \
--mac-credentials file://mac-credentials.json
```

Im folgenden ist der Inhalt der in den vorherigen Beispielen referenzierten `mac-credentials.json`-Datei dargestellt.

```
{
  "internalDiskPassword":"internal-disk-admin_password",
  "rootVolumeUsername":"root-volume-admin_username",
  "rootVolumepassword":"root-volume-admin_password"
}
```

2. Warten Sie, bis die Aufgabe zur Delegierung des Volume-Besitzes abgeschlossen ist und die Instance wieder fehlerfrei ist. Verwenden Sie den Befehl describe-mac-modification-tasks. Geben Sie für `--mac-modification-task-id` die ID der Aufgabe zur Delegierung des Volume-Besitzes aus dem vorherigen Schritt an.

```
aws ec2 describe-mac-modification-tasks \
--mac-modification-task-id task-id
```

3. Wenn die Aufgabe zur Delegierung des Volume-Besitzes abgeschlossen ist, fahren Sie mit Schritt 3 fort.

Schritt 3: Software aktualisieren

Nachdem Sie den Besitz des Amazon-EBS-Root-Volumes delegiert haben, führen Sie die unter Software auf x86-Mac-Instances aktualisieren (unten) beschriebenen Schritte aus, um die Software zu aktualisieren.

Manual volume ownership delegation

Während Sie dieses Verfahren durcharbeiten, erstellen Sie zwei Passwörter. Ein Passwort ist für den Administratorbenutzer des Amazon-EBS-Root-Volume (`ec2-user`) und das andere Passwort ist für den Administratorbenutzer der internen Festplatte (`aws-managed-user`). Merken Sie sich diese Passwörter, da Sie sie im weiteren Verlauf des Verfahrens verwenden werden.

> **Note**
>
> Mit diesem Verfahren auf macOS Big Sur können Sie nur kleinere Aktualisierungen durchführen, z. B. die Aktualisierung von macOS Big Sur 11.7.3 zu macOS Big Sur 11.7.4. Für macOS Monterey oder höher können Sie größere Softwareupdates durchführen.

Für den Zugriff auf die interne Festplatte

1. Stellen Sie von Ihrem lokalen Computer aus im Terminal mit dem folgenden Befehl über SSH eine Verbindung zu Ihrer Apple-Silicon-Mac-Instance her. Weitere Informationen finden Sie unter Herstellung einer Verbindung zu Ihrer Instance mit SSH.

   ```
   ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
   ```

2. Installieren und starten Sie macOS Screen Sharing mit dem folgenden Befehl.

   ```
   [ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
   sudo launchctl load -w /System/Library/LaunchDaemons/
   com.apple.screensharing.plist
   ```

3. Legen Sie ein Passwort für `ec2-user` mit dem folgenden Befehl fest. Merken Sie sich das Passwort, da Sie es später verwenden werden.

   ```
   [ec2-user ~]$ sudo /usr/bin/dscl . -passwd /Users/ec2-user
   ```

4. Trennen Sie die Verbindung zur Instance, indem Sie exit eingeben und die Rücktaste drücken.
5. Verbinden Sie sich von Ihrem lokalen Computer aus im Terminal erneut mit Ihrer Instance mit einem SSH-Tunnel zum VNC-Port, indem Sie den folgenden Befehl eingeben.

   ```
   ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 ec2-user@instance-public-
   dns-name
   ```

   > **Note**
   >
   > Beenden Sie diese SSH-Sitzung erst, wenn die folgenden VNC-Verbindungs- und GUI-Schritte abgeschlossen sind. Wenn die Instance neu gestartet wird, wird die Verbindung automatisch geschlossen.

6. Verbinden Sie sich von Ihrem lokalen Computer aus mit `localhost:5900`, indem Sie die folgenden Schritte ausführen:

   a. Öffnen Sie den Finder und wählen Sie Go.

   b. Wählen Sie Mit Server verbinden aus.

   c. Geben Sie `vnc://localhost:5900` in das Feld Serveradresse ein.

7. Stellen Sie im macOS-Fenster eine Verbindung zur Remote-Sitzung der Apple-Silicon-Mac-Instance als `ec2-user` mit dem Passwort her, das Sie in Schritt 3 erstellt haben.
8. Greifen Sie mit einer der folgenden Optionen auf das interne Laufwerk mit dem Namen InternalDiskzu.

   a. Für macOS Ventura oder höher: Öffnen Sie die Systemeinstellungen, wählen Sie im linken Bereich Allgemein und dann unten rechts im Bereich Startup-Diskette aus.

   b. Für macOS Monterey oder darunter: Öffnen Sie die Systempräferenzen, wählen Sie Startup-Diskette und entsperren Sie den Bereich dann, indem Sie das Schlosssymbol unten links im Fenster auswählen.

   > **Tipp zur Problembehebung**
   >
   > Wenn Sie die interne Festplatte mounten müssen, führen Sie den folgenden Befehl im Terminal aus.
   >
   > ```
   > APFSVolumeName="InternalDisk" ; SSDContainer=$(diskutil list | grep
   >  "Physical Store disk0" -B 3 | grep "/dev/disk" | awk {'print $1'} ) ;
   >  diskutil apfs addVolume $SSDContainer APFS $APFSVolumeName
   > ```

9. Wählen Sie das interne Laufwerk mit dem Namen InternalDiskaus und klicken Sie auf Neu starten. Wählen Sie erneut Neu starten, wenn Sie dazu aufgefordert werden.

   > **Important**
   >
   > Wenn die interne Festplatte statt Macintosh HD heißt InternalDisk, muss Ihre Instanz gestoppt und neu gestartet werden, damit der dedizierte Host aktualisiert werden kann. Weitere Informationen finden Sie unter Beenden oder beenden Sie Ihre Amazon EC2 Mac-Instance.

Gehen Sie wie folgt vor, um den Besitz an den administrativen Benutzer zu delegieren. Wenn Sie sich mit SSH wieder mit Ihrer Instance verbinden, starten Sie von der internen Festplatte unter Verwendung des speziellen administrativen Benutzers (`aws-managed-user`). Das ursprüngliche Passwort für `aws-managed-user` ist leer, daher müssen Sie es bei Ihrer ersten Verbindung überschreiben. Dann müssen Sie die Schritte wiederholen, um macOS Screen Sharing zu installieren und zu starten, da sich das Startvolume geändert hat.

Die Inhaberschaft auf einem Amazon-EBS-Volume an den Administrator zu delegieren

1. Stellen Sie von Ihrem lokalen Computer aus im Terminal mit dem folgenden Befehl eine Verbindung zu Ihrer Apple-Silicon-Mac-Instance her.

```
ssh -i /path/key-pair-name.pem aws-managed-user@instance-public-dns-name
```

2. Verwenden Sie einen der folgenden Befehle, um das Problem zu beheben, wenn Sie die Warnung `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!` erhalten.

   a. Löschen Sie die bekannten Hosts mit dem folgenden Befehl. Wiederholen Sie dann den vorherigen Schritt.

```
rm ~/.ssh/known_hosts
```

   b. Fügen Sie dem SSH-Befehl im vorherigen Schritt Folgendes aus.

```
-o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no
```

3. Legen Sie das Passwort für `aws-managed-user` mit dem folgenden Befehl fest. Das ursprüngliche `aws-managed-user` Passwort ist leer, daher müssen Sie es bei Ihrer ersten Verbindung überschreiben.

   a.
```
[aws-managed-user ~]$ sudo /usr/bin/dscl . -passwd /Users/aws-managed-user password
```

   b. Wenn Sie die Eingabeaufforderung `Permission denied. Please enter user's old password:` erhalten, drücken Sie die Eingabetaste.

> **Tipp zur Problembehebung**
>
> Wenn Sie den Fehler `passwd: DS error: eDSAuthFailed` erhalten, verwenden Sie den folgenden Befehl.
>
> ```
> [aws-managed-user ~]$ sudo passwd aws-managed-user
> ```

4. Installieren und starten Sie macOS Screen Sharing mit dem folgenden Befehl.

```
[aws-managed-user ~]$ sudo launchctl enable system/com.apple.screensharing
```

```
sudo launchctl load -w /System/Library/LaunchDaemons/
com.apple.screensharing.plist
```

5. Trennen Sie die Verbindung zur Instance, indem Sie exit eingeben und die Rücktaste drücken.
6. Verbinden Sie sich von Ihrem lokalen Computer aus im Terminal erneut mit Ihrer Instance mit einem SSH-Tunnel zum VNC-Port, indem Sie den folgenden Befehl eingeben.

```
ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 aws-managed-user@instance-
public-dns-name
```

7. Verbinden Sie sich von Ihrem lokalen Computer aus mit `localhost:5900`, indem Sie die folgenden Schritte ausführen:

   a. Öffnen Sie den Finder und wählen Sie Go.

   b. Wählen Sie Mit Server verbinden aus.

   c. Geben Sie `vnc://localhost:5900` in das Feld Serveradresse ein.

8. Stellen Sie im macOS-Fenster eine Verbindung zur Remote-Sitzung der Apple-Silicon-Mac-Instance als `aws-managed-user` mit dem Passwort her, das Sie in Schritt 3 erstellt haben.

> **Note**
>
> Wenn Sie aufgefordert werden, sich mit Ihrer Apple ID anzumelden, wählen Sie Später einrichten.

9. Greifen Sie mit einer der folgenden Optionen auf das Amazon EBS Volume zu.

   a. Für macOS Ventura oder höher: Öffnen Sie die Systemeinstellungen, wählen Sie im linken Bereich Allgemein und dann unten rechts im Bereich Startup-Diskette aus.

   b. Für macOS Monterey oder darunter: Öffnen Sie die Systempräferenzen, wählen Sie Startup-Diskette und entsperren Sie den Bereich dann mit dem Schlosssymbol unten links im Fenster.

> **Note**
>
> Wenn Sie bis zum Neustart zur Eingabe eines Administrator-Passworts aufgefordert werden, verwenden Sie das Passwort, das Sie oben für `aws-managed-user` festgelegt haben. Dieses Passwort kann sich von dem unterscheiden, das Sie für

`ec2-user` oder für das Standard-Administratorkonto in Ihrer Instance festgelegt haben. Die folgenden Anweisungen geben an, wann das Administratorkennwort Ihrer Instance verwendet werden soll.

10. Wählen Sie das Amazon EBS-Volume aus (das Volume, das InternalDiskim Fenster Startdiskette nicht benannt ist) und wählen Sie Restart.

> **Note**
>
> Wenn Sie mehrere startfähige Amazon-EBS-Volumes an Ihre Apple-Silicon-Mac-Instance angefügt haben, achten Sie darauf, für jedes Volume einen eindeutigen Namen zu verwenden.

11. Bestätigen Sie den Neustart und wählen Sie dann Benutzer autorisieren, wenn Sie dazu aufgefordert werden.
12. Vergewissern Sie sich, dass im Bereich Benutzer auf diesem Volume autorisieren der Administratorbenutzer (standardmäßig `ec2-user`) ausgewählt ist, und wählen Sie dann Autorisieren aus.
13. Geben Sie das `ec2-user`-Passwort ein, das Sie in Schritt 3 des vorherigen Verfahrens erstellt haben, und wählen Sie dann Weiter aus.
14. Geben Sie das Passwort für den speziellen Administratorbenutzer (`aws-managed-user`) ein, wenn Sie dazu aufgefordert werden.
15. Stellen Sie von Ihrem lokalen Computer aus im Terminal mithilfe von SSH und dem Benutzernamen `ec2-user` erneut eine Verbindung zu Ihrer Instance her

> **Tipp zur Problembehebung**
>
> Wenn Sie die Warnung `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!` erhalten, führen Sie den folgenden Befehl aus und stellen Sie mithilfe von SSH erneut eine Verbindung zu Ihrer Instance her.
>
> ```
> rm ~/.ssh/known_hosts
> ```

16. Verwenden Sie die Befehle unter Software auf x86-Mac-Instances aktualisieren, um das Softwareupdate durchzuführen.

Software auf x86-Mac-Instances aktualisieren

Auf x86-Mac-Instances können Sie Betriebssystem-Updates von Apple mit dem `softwareupdate`-Befehl installieren.

So installieren Sie Betriebssystem-Updates von Apple auf x86-Mac-Instances

1. Listen Sie die Pakete mit verfügbaren Updates mit dem folgenden Befehl auf.

   ```
   [ec2-user ~]$ softwareupdate --list
   ```

2. Installieren Sie alle Updates oder nur bestimmte Updates. Verwenden Sie den folgenden Befehl, um bestimmte Updates zu installieren.

   ```
   [ec2-user ~]$ sudo softwareupdate --install label
   ```

   Verwenden Sie den folgenden Befehl, um stattdessen alle Updates zu installieren.

   ```
   [ec2-user ~]$ sudo softwareupdate --install --all --restart
   ```

Systemadministratoren können AWS Systems Manager damit vorab genehmigte Betriebssystemupdates auf x86-Mac-Instances bereitstellen. Weitere Informationen finden Sie im AWS Systems Manager -Benutzerhandbuch.

Sie können Homebrew verwenden, um Updates für Pakete auf dem EC2 macOS zu installieren AMIs, sodass Sie die neueste Version dieser Pakete auf Ihren Instanzen haben. Sie können Homebrew auch verwenden, um gängige macOS-Anwendungen auf Amazon EC2 macOS zu installieren und auszuführen. Weitere Informationen finden Sie in der Homebrew-Dokumentation.

Installieren von Updates mit Homebrew

1. Aktualisieren Sie Homebrew mit dem folgenden Befehl.

   ```
   [ec2-user ~]$ brew update
   ```

2. Listen Sie die Pakete mit verfügbaren Updates mit dem folgenden Befehl auf.

   ```
   [ec2-user ~]$ brew outdated
   ```

3. Installieren Sie alle Updates oder nur bestimmte Updates. Verwenden Sie den folgenden Befehl, um bestimmte Updates zu installieren.

```
[ec2-user ~]$ brew upgrade package name
```

Verwenden Sie den folgenden Befehl, um stattdessen alle Updates zu installieren.

```
[ec2-user ~]$ brew upgrade
```

Erhöhen Sie die Größe eines EBS-Volumes auf Ihrer Mac-Instance

Sie können die Größe Ihrer Amazon EBS-Volumes auf Ihrer Mac-Instance erhöhen. Weitere Informationen finden Sie unter Amazon EBS Elastic Volumes im Amazon-EBS-Benutzerhandbuch.

Nachdem Sie die Größe des Volumes erhöht haben, müssen Sie die Größe Ihres APFS-Containers wie folgt erhöhen.

So stellen Sie mehr Speicherplatz zur Verfügung:

1. Stellen Sie fest, ob ein Neustart erforderlich ist. Wenn Sie ein bestehendes EBS-Volume an eine laufende Mac-Instance anschließen, müssen Sie die Instance neu starten, um die neue Größe verfügbar zu machen. Wenn während des Startzeitraums eine Änderung am Speicherplatz vorgenommen wurde, ist kein Neustart erforderlich.

   Anzeigen der aktuellen Datenträgergröße:

```
[ec2-user ~]$  diskutil list external physical
/dev/disk0 (external, physical):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:                 GUID_partition_scheme           *322.1 GB     disk0
   1:                 EFI EFI                          209.7 MB     disk0s1
   2:                 Apple_APFS Container disk2       321.9 GB     disk0s2
```

2. Kopieren Sie den folgenden Befehl und fügen Sie ihn ein.

```
[ec2-user ~]$ PDISK=$(diskutil list physical external | head -n1 | cut -d" " -f1)
APFSCONT=$(diskutil list physical external | grep "Apple_APFS" | tr -s " " | cut -
d" " -f8)
yes | sudo diskutil repairDisk $PDISK
```

3. Kopieren Sie den folgenden Befehl und fügen Sie ihn ein.

```
[ec2-user ~]$ sudo diskutil apfs resizeContainer $APFSCONT 0
```

Beenden oder beenden Sie Ihre Amazon EC2 Mac-Instance

Wenn Sie eine Mac-Instance anhalten, bleibt die Instance etwa 15 Minuten im `stopping`-Status, bevor sie in den `stopped`-Status eintritt.

Wenn Sie eine Mac-Instance stoppen oder beenden, EC2 führt Amazon einen Scrubbing-Workflow auf dem zugrunde liegenden Dedicated Host durch, um die interne SSD zu löschen, die persistenten NVRAM-Variablen zu löschen und auf die neueste Gerätefirmware zu aktualisieren. Dadurch wird sichergestellt, dass Mac-Instances die gleiche Sicherheit und den gleichen Datenschutz bieten wie andere EC2-Nitro-Instances. Außerdem können Sie damit das neueste macOS ausführen AMIs. Während des Scrubbing-Workflows geht der Dedicated Host vorübergehend in den Schwebezustand über. Bei x86-Mac-Instances kann es bis zu 50 Minuten dauern, bis der Scrubbing-Workflow abgeschlossen ist. Bei Apple-Silicon-Mac-Instances kann es bis zu 110 Minuten dauern, bis der Scrubbing-Workflow abgeschlossen ist. Wenn die Gerätefirmware aktualisiert werden muss, kann es bei x86-Mac-Instances außerdem bis zu drei Stunden dauern, bis der Scrubbing-Workflow abgeschlossen ist.

Sie können die angehaltene Mac-Instance nicht starten oder eine neue Mac-Instance starten, bis der Scrubbing-Workflow abgeschlossen ist. An diesem Punkt wechselt Dedicated Host in den `available`-Status.

Die Erfassung und Abrechnung wird angehalten, wenn der Dedicated Host in den `pending`-Status wechselt. Die Dauer des Scrubbing-Workflows wird Ihnen nicht in Rechnung gestellt.

Geben Sie die Dedicated Host für Ihre Mac-Instance frei

Wenn Sie mit Ihrer Mac-Instance fertig sind, können Sie Dedicated Host freigeben. Bevor Sie den Dedicated Host freigeben können, müssen Sie die Mac-Instance anhalten oder beenden. Sie können den Host erst freigeben, wenn der Zuweisungszeitraum das 24-Stunden-Minimum überschreitet.

So veröffentlichen Sie das Dedicated Host

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.

3. Markieren Sie die Instance und wählen Sie Instance state (Instance-Status) und wählen Sie dann entweder Stop instance (Instance anhalten) oder Terminate Instance (Instance beenden).
4. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
5. Wählen Sie Dedicated Host aus und wählen Sie Actions (Aktionen), Release host (Host veröffentlichen).
6. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Release (Veröffentlichen).

Systemintegritätsschutz für Amazon EC2 Mac-Instances konfigurieren

Sie können Systemintegritätsschutz-Einstellungen (SIP) für x86-Mac-Instances und Apple-Halbleiter-Mac-Instances konfigurieren. SIP ist ein wichtiges Sicherheitsfeature von macOS, die dazu beiträgt, unbefugte Codeausführung und Änderungen auf Systemebene zu verhindern. Weitere Informationen finden Sie unter Allgemeines zum Systemintegritätsschutz.

Sie können SIP entweder vollständig aktivieren oder deaktivieren, oder Sie können bestimmte SIP-Einstellungen selektiv aktivieren oder deaktivieren. Es wird empfohlen, SIP nur vorübergehend zu deaktivieren, um die erforderlichen Aufgaben auszuführen, und dann so bald wie möglich wieder zu aktivieren. Wenn SIP deaktiviert ist, kann Ihre Instance anfällig für bösartigen Code werden.

Die SIP-Konfiguration wird in allen AWS Regionen unterstützt, in denen Amazon EC2 Mac-Instances unterstützt werden.

Themen

- Überlegungen
- Standard-SIP-Konfigurationen
- Ihre SIP-Konfiguration überprüfen
- Voraussetzungen für Apple-Halbleiter-Mac-Instances
- SIP-Einstellungen konfigurieren
- Überprüfen Sie den Status der SIP-Konfigurationsaufgabe

Überlegungen

- Die folgenden Amazon EC2 Mac-Instance-Typen und macOS-Versionen werden unterstützt:
  - Mac1 | Mac2 | Mac2-m1ultra – macOS Ventura (Version 13,0 oder höher)
  - Mac2-m2 | Mac2-m2pro – macOS Ventura (Version 13,2 oder höher)

- Mac-m4 | Mac-m4pro – macOS Sequoia (Version 15.6 oder höher)

> **Note**
>
> Beta- und Vorschauversionen von macOS werden nicht unterstützt.

- Sie können eine benutzerdefinierte SIP-Konfiguration angeben, um einzelne SIP-Einstellungen selektiv zu aktivieren oder zu deaktivieren. Wenn Sie eine benutzerdefinierte Konfiguration implementieren, stellen Sie eine Verbindung zur Instance her und überprüfen Sie die Einstellungen, um sicherzustellen, dass Ihre Anforderungen ordnungsgemäß implementiert sind und wie vorgesehen funktionieren.

  SIP-Konfigurationen können sich mit macOS-Updates ändern. Wir empfehlen Ihnen, die benutzerdefinierten SIP-Einstellungen nach jedem Upgrade der macOS-Version zu überprüfen, um sicherzustellen, dass Ihre Sicherheitskonfigurationen weiterhin kompatibel sind und ordnungsgemäß funktionieren.
- Für x86-Mac-Instances werden SIP-Einstellungen auf Instance-Ebene angewendet. Jedes an die Instance angehängte Root-Volume erbt automatisch die konfigurierten SIP-Einstellungen.

  Bei Apple-Halbleiter-Mac-Instances werden die SIP-Einstellungen auf der Volume-Ebene angewendet. Root-Volumes, die an die Instance angehängt sind, erben die SIP-Einstellungen nicht. Wenn Sie ein anderes Root-Volume anhängen, müssen Sie die SIP-Einstellungen neu konfigurieren, um sie auf den erforderlichen Status zurücksetzen.
- Es kann bis zu 90 Minuten dauern, bis die SIP-Konfigurationsaufgaben abgeschlossen sind. Die Instance bleibt während der Ausführung der SIP-Konfigurationsaufgabe nicht erreichbar.
- SIP-Konfigurationen werden nicht in Snapshots übertragen oder AMIs die Sie anschließend aus der Instance erstellen.
- Apple-Halbleiter-Mac-Instances dürfen nur über ein bootfähiges Volume verfügen, und jedes angehängte Volume kann nur über einen zusätzlichen Administratorbenutzer verfügen.

Standard-SIP-Konfigurationen

In der folgenden Tabelle ist die Standard-SIP-Konfiguration für x86-Mac-Instances und Apple-Halbleiter-Mac-Instances aufgeführt.

	Apple-Halbleiter-Mac-Instances	x86-Mac-Instances
Apple Internal	Aktiviert	Disabled
Dateisystemschutz	Aktiviert	Disabled
Basissystem	Aktiviert	Aktiviert
Debugging-Einschränkungen	Aktiviert	Aktiviert
Dtrace-Einschränkungen	Aktiviert	Aktiviert
Kext-Signatur	Aktiviert	Aktiviert
Nvram-Schutz	Aktiviert	Aktiviert

Ihre SIP-Konfiguration überprüfen

Wir empfehlen Ihnen, Ihre SIP-Konfiguration vor und nach Änderungen zu überprüfen, um sicherzustellen, dass sie wie erwartet konfiguriert ist.

Um die SIP-Konfiguration für eine Amazon EC2 Mac-Instance zu überprüfen

Stellen Sie über SSH eine Verbindung zur Instance her und führen Sie dann den folgenden Befehl in der Befehlszeile aus.

```
$ csrutil status
```

Es folgt eine Beispielausgabe.

```
System Integrity Protection status: enabled.
```

```
Configuration:
    Apple Internal: enabled
    Kext Signing: disabled
    Filesystem Protections: enabled
    Debugging Restrictions: enabled
    DTrace Restrictions: enabled
    NVRAM Protections: enabled
    BaseSystem Verification: disabled
```

Voraussetzungen für Apple-Halbleiter-Mac-Instances

Bevor Sie die SIP-Einstellungen für Apple-Halbleiter-Mac-Instances konfigurieren können, müssen Sie ein Passwort festlegen und das sichere Token für den Administratorbenutzer des Amazon-EBS-Root-Volumes (`ec2-user`) aktivieren.

> **Note**
>
> Das Passwort und das sichere Token werden festgelegt, wenn Sie zum ersten Mal über die GUI eine Verbindung zu einer Apple-Halbleiter-Mac-Instance herstellen. Wenn Sie zuvor über die GUI eine Verbindung mit der Instance hergestellt haben oder wenn Sie eine x86-Mac-Instance verwenden, müssen Sie diese Schritte nicht ausführen.

So können Sie ein Passwort festlegen und das sichere Token für den Administratorbenutzer des EBS-Root-Volumes aktivieren

1. Stellen Sie über SSH eine Connect zur Instance her.
2. Legen Sie das Passwort für den `ec2-user`-Benutzer fest.

   ```
   $ sudo /usr/bin/dscl . -passwd /Users/ec2-user
   ```

3. Aktivieren Sie das sichere Token für den `ec2-user`-Benutzer. Geben Sie für `-oldPassword` dasselbe Passwort aus dem vorherigen Schritt an. Geben Sie für `-newPassword` ein anderes Passwort ein. Der folgende Befehl geht davon aus, dass Sie Ihre alten und neuen Passwörter in `.txt`-Dateien gespeichert haben.

   ```
   $ sysadminctl -oldPassword `cat old_password.txt` -newPassword `cat
    new_password.txt`
   ```

4. Stellen Sie sicher, dass das sichere Token aktiviert ist.

```
$ sysadminctl -secureTokenStatus ec2-user
```

SIP-Einstellungen konfigurieren

Wenn Sie die SIP-Einstellungen für Ihre Instance konfigurieren, können Sie entweder alle SIP-Einstellungen aktivieren oder deaktivieren, oder Sie können eine benutzerdefinierte Konfiguration angeben, die bestimmte SIP-Einstellungen selektiv aktiviert oder deaktiviert.

> **Note**
>
> Wenn Sie eine benutzerdefinierte Konfiguration implementieren, stellen Sie eine Verbindung zur Instance her und überprüfen Sie die Einstellungen, um sicherzustellen, dass Ihre Anforderungen ordnungsgemäß implementiert sind und wie vorgesehen funktionieren. SIP-Konfigurationen können sich mit macOS-Updates ändern. Wir empfehlen Ihnen, die benutzerdefinierten SIP-Einstellungen nach jedem Upgrade der macOS-Version zu überprüfen, um sicherzustellen, dass Ihre Sicherheitskonfigurationen weiterhin kompatibel sind und ordnungsgemäß funktionieren.

Um die SIP-Einstellungen für Ihre Instance zu konfigurieren, müssen Sie eine SIP-Konfigurationsaufgabe erstellen. Die SIP-Konfigurationsaufgabe legt die SIP-Einstellungen für Ihre Instance fest.

Wenn Sie eine SIP-Konfiguration für eine Apple-Halbleiter-Mac-Instance erstellen, müssen Sie die folgenden Anmeldeinformationen angeben:

- Administratorbenutzer der internen Festplatte
  - Benutzername – Nur der standardmäßige Administratorbenutzer (`aws-managed-user`) wird unterstützt und standardmäßig verwendet. Sie können keinen anderen Administratorbenutzer angeben.
  - Passwort – Wenn Sie das Standardpasswort für `aws-managed-user` nicht geändert haben, geben Sie das Standardpasswort ein, das leer ist. Andernfalls geben Sie Ihr Passwort ein.
- Administrator-Benutzer des Amazon-EBS-Root-Volumes

- Benutzername – Wenn Sie den standardmäßigen Administratorbenutzer nicht geändert haben, geben Sie `ec2-user` an. Geben Sie andernfalls den Benutzernamen für Ihren Administratorbenutzer an.
- Passwort – Sie müssen immer das Passwort angeben.

Verwenden Sie die folgenden Methoden, um eine SIP-Konfigurationsaufgabe zu erstellen.

Console

So erstellen Sie eine SIP-Konfigurationsaufgabe mit der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann die Amazon EC2 Mac-Instance aus.
3. Wählen Sie auf der Registerkarte Sicherheit die Optionen Mac anpassen, Systemintegritätsschutz anpassen aus.
4. Um alle SIP-Einstellungen zu aktivieren, wählen Sie SIP aktivieren aus. Um alle SIP-Einstellungen zu deaktivieren, deaktivieren Sie die Option SIP aktivieren.
5. Um eine benutzerdefinierte Konfiguration anzugeben, die bestimmte SIP-Einstellungen selektiv aktiviert oder deaktiviert, wählen Sie Benutzerdefinierte SIP-Konfiguration angeben und wählen Sie dann die SIP-Einstellungen aus, die aktiviert werden sollen, oder löschen Sie die SIP-Einstellungen, um sie zu deaktivieren.
6. Geben Sie die Anmeldeinformationen für den Benutzer des Root-Volumes und den Besitzer der internen Festplatte an.
7. Wählen Sie SIP-Änderungsaufgabe erstellen aus.

AWS CLI

Um eine SIP-Konfigurationsaufgabe mit dem zu erstellen AWS CLI

Verwenden Sie den protection-modification-task Befehl create-mac-system-integrity-.

Alle SIP-Einstellungen aktivieren/deaktivieren

Verwenden Sie nur den Parameter `--mac-system-integrity-protection-status`, um alle SIP-Einstellungen vollständig zu aktivieren oder zu deaktivieren.

Der folgende Beispielbefehl aktiviert alle SIP-Einstellungen.

```
aws ec2 create-mac-system-integrity-protection-modification-task \
--instance-id i-0abcdef9876543210 \
--mac-system-integrity-protection-status enabled \
--mac-credentials file://mac-credentials.json
```

Eine benutzerdefinierte SIP-Konfiguration angeben

Um eine benutzerdefinierte SIP-Konfiguration anzugeben, die bestimmte SIP-Einstellungen selektiv aktiviert oder deaktiviert, geben Sie die Parameter `--mac-system-integrity-protection-status` und `--mac-system-integrity-protection-configuration` an. Verwenden Sie in diesem Fall `mac-system-integrity-protection-status`, um den gesamten SIP-Status anzugeben. und `mac-system-integrity-protection-configuration`, um einzelne SIP-Einstellungen selektiv zu aktivieren oder zu deaktivieren.

Mit dem folgenden Beispielbefehl wird eine SIP-Konfigurationsaufgabe erstellt, um alle SIP-Einstellungen außer `NvramProtections` und `FilesystemProtections` zu aktivieren.

```
aws ec2 create-mac-system-integrity-protection-modification-task \
--instance-id i-0abcdef9876543210 \
--mac-system-integrity-protection-status enabled \
--mac-system-integrity-protection-configuration
 "NvramProtections=disabled, FilesystemProtections=disabled" \
--mac-credentials file://mac-credentials.json
```

Mit dem folgenden Beispielbefehl wird eine SIP-Konfigurationsaufgabe erstellt, um alle SIP-Einstellungen außer `DtraceRestrictions` zu deaktivieren.

```
aws ec2 create-mac-system-integrity-protection-modification-task \
--instance-id i-0abcdef9876543210 \
--mac-system-integrity-protection-status disabled \
--mac-system-integrity-protection-configuration "DtraceRestrictions=enabled" \
--mac-credentials file://mac-credentials.json
```

Inhalt der **`mac-credentials.json`**-Datei.

Im folgenden ist der Inhalt der in den vorherigen Beispielen referenzierten `mac-credentials.json`-Datei dargestellt.

```
{
```

```
  "internalDiskPassword":"internal-disk-admin_password",
  "rootVolumeUsername":"root-volume-admin_username",
  "rootVolumepassword":"root-volume-admin_password"
}
```

Überprüfen Sie den Status der SIP-Konfigurationsaufgabe

Verwenden Sie eine der folgenden Methoden, um den Status der SIP-Konfigurationsaufgaben zu überprüfen.

Console

So zeigen Sie Ihre SIP-Konfigurationsaufgaben mit der Konsole an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann die Amazon EC2 Mac-Instance aus.
3. Scrollen Sie auf der Registerkarte Sicherheit nach unten zum Abschnitt Mac-Änderungsaufgaben.

AWS CLI

Um den Status der SIP-Konfigurationsaufgaben zu überprüfen, verwenden Sie AWS CLI

Verwenden Sie den Befehl describe-mac-modification-tasks.

Finden Sie unterstützte macOS-Versionen für Ihren Amazon EC2 Mac Dedicated Host

Sie können sich die neuesten macOS-Versionen ansehen, die von Ihrem Amazon EC2 Mac Dedicated Host unterstützt werden. Mit dieser Funktion können Sie überprüfen, ob Ihr Dedicated Host Instance-Starts mit Ihren bevorzugten macOS-Versionen unterstützen kann.

Für jede macOS-Version ist eine minimale Firmware-Version auf dem zugrunde liegenden Apple Mac erforderlich, um erfolgreich zu booten. Die Apple-Mac-Firmware-Version kann veraltet sein, wenn ein zugewiesener Mac-Dedicated-Host über einen längeren Zeitraum inaktiv war oder wenn auf ihm eine lang ausgeführte Instance installiert ist.

Um die Unterstützung für die neuesten macOS-Versionen sicherzustellen, können Sie Instances auf Ihrem zugewiesenen Mac-Dedicated-Host anhalten oder beenden. Dadurch wird der Host-

Scrubbing-Workflow ausgelöst und die Firmware auf dem zugrunde liegenden Apple Mac aktualisiert, um die neuesten macOS-Versionen zu unterstützen. Ein Dedicated Host mit einer lang ausgeführten Instance wird automatisch aktualisiert, wenn Sie eine ausgeführte Instance anhalten oder beenden.

Weitere Informationen zu Scrubbing-Workflows finden Sie unter Beenden oder beenden Sie Ihre Amazon EC2 Mac-Instance.

Weitere Informationen über das Starten einer Mac-Instance finden Sie unter Starten Sie eine Mac-Instance mit dem AWS-Managementkonsole oder AWS CLI.

Sie können Informationen zu den neuesten macOS-Versionen, die auf Ihrem zugewiesenen Dedicated Host unterstützt werden, über die EC2 Amazon-Konsole oder die anzeigen AWS CLI.

Console

So zeigen Sie Firmware-Informationen für Dedicated Hosts mithilfe der Konsole an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Auf der Detailseite zu Dedicated Hosts finden Sie unter Aktuell unterstützte macOS-Versionen die neuesten macOS-Versionen, die der Host unterstützen kann.

AWS CLI

Um Firmwareinformationen für Dedicated Hosts mit dem AWS CLI

Verwenden Sie den `describe-mac-hosts`-Befehl und ersetzen Sie `region` durch den entsprechenden AWS-Region.

```
$ aws ec2 describe-mac-hosts --region us-east-1
  {
      "MacHosts": [
          {
              "HostId": "h-07879acf49EXAMPLE",
              "MacOSLatestSupportedVersions": [
                  "14.3",
                  "13.6.4",
                  "12.7.3"
              ]
          }
      ]
```

```
}
```

So abonnieren Sie macOS-AMI-Benachrichtigungen

Um benachrichtigt zu werden, wenn neue AMIs Produkte veröffentlicht werden oder wenn BridgeOS aktualisiert wurde, abonnieren Sie Benachrichtigungen über Amazon SNS.

Weitere Informationen zu EC2 macOS AMIs finden Sie unter AMIs Versionshinweise zu Amazon EC2 macOS.

So abonnieren Sie macOS-AMI-Benachrichtigungen

1. Öffnen Sie die Amazon SNS SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Ändern Sie, falls erforderlich, die Region in der Navigationsleiste zu US East (N. Virginia). Sie müssen diese Region verwenden, da die SNS-Benachrichtigungen, die Sie abonnieren, in dieser Region erstellt wurden.
3. Wählen Sie im Navigationsbereich Subscriptions aus.
4. Wählen Sie Create subscription.
5. Führen Sie im Dialogfeld Create subscription die folgenden Schritte aus:

   a. Kopieren Sie für das Thema ARN einen der folgenden Amazon-Ressourcennamen (ARNs) und fügen Sie ihn ein:

      - **`arn:aws:sns:us-east-1:898855652048:amazon-ec2-macos-ami-updates`**
      - **`arn:aws:sns:us-east-1:898855652048:amazon-ec2-bridgeos-updates`**

   b. Wählen Sie unter Protokoll eine der folgenden Optionen:

      - E-Mail:

        Geben Sie unter Endpoint eine E-Mail-Adresse ein, um die Benachrichtigungen zu empfangen. Nachdem Sie Ihr Abonnement erstellt haben, erhalten Sie eine Bestätigungs-Nachricht mit der Betreffzeile `AWS Notification - Subscription Confirmation`. Öffnen Sie die E-Mail und wählen Sie Confirm subscription aus, um Ihr Abonnement abzuschließen.
      - SMS:

        Geben Sie unter Endpunkt eine E-Mail-Adresse ein, um die Benachrichtigungen zu empfangen.

- AWS Lambda, Amazon SQS, Amazon Data Firehose (Benachrichtigungen werden im JSON-Format geliefert):

  Geben Sie für Endpunkt den ARN für die Lambda-Funktion, die SQS-Warteschlange oder den Firehose-Stream ein, den Sie zum Empfangen der Benachrichtigungen verwenden können.

c. Wählen Sie Create subscription (Abonnement erstellen) aus.

Immer wenn macOS AMIs veröffentlicht wird, senden wir Benachrichtigungen an die Abonnenten des `amazon-ec2-macos-ami-updates` Themas. Immer wenn bridgeOS aktualisiert wird, senden wir Benachrichtigungen an die Abonnenten des `amazon-ec2-bridgeos-updates`-Themas. Wenn Sie diese Benachrichtigungen nicht mehr erhalten möchten, führen Sie die folgenden Schritte aus, um sich abzumelden.

So melden Sie sich von den macOS-AMI-Benachrichtigungen ab

1. Öffnen Sie die Amazon SNS SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Ändern Sie, falls erforderlich, die Region in der Navigationsleiste zu US East (N. Virginia). Sie müssen diese Region verwenden, da die SNS-Benachrichtigungen in dieser Region erstellt wurden.
3. Wählen Sie im Navigationsbereich Subscriptions aus.
4. Wählen Sie die Abonnements aus und wählen Sie anschließend Actions und Delete Subscriptions. Klicken Sie zum Bestätigen auf Delete.

Rufen Sie das macOS-AMI IDs mithilfe der AWS Systems Manager Parameter Store API ab

Beim Starten einer Instance müssen Sie ein AMI angeben. Ein AMI ist spezifisch für eine AWS-Region Betriebssystem- und Prozessorarchitektur. Sie können alle macOS AMIs in einem anzeigen AWS-Region und das neueste macOS-AMI abrufen, indem Sie die AWS Systems Manager Parameter Store-API abfragen. Wenn Sie diese öffentlichen Parameter verwenden, müssen Sie das macOS-AMI nicht manuell nachschlagen IDs. Öffentliche Parameter sind sowohl x86 für macOS als auch für ARM64 macOS AMIs verfügbar und können in Ihre vorhandenen AWS CloudFormation Vorlagen integriert werden.

Erforderliche Berechtigungen

Um diese Aktion ausführen zu können, muss der IAM-Prinzipal über die erforderlichen Berechtigungen zum Aufrufen der `ssm:GetParameter`-API-Aktion verfügen.

Um eine Liste aller aktuellen macOS AMIs anzuzeigen, AWS-Region verwenden Sie den AWS CLI

Verwenden Sie den folgenden get-parameters-by-pathBefehl, um eine Liste aller macOS AMIs in der aktuellen Region anzuzeigen.

```
aws ssm get-parameters-by-path --path /aws/service/ec2-macos --recursive --query
 "Parameters[].Name"
```

Um die AMI-ID des neuesten großen macOS-AMI abzurufen, verwenden Sie den AWS CLI

Verwenden Sie den folgenden Befehl get-parameter mit dem Unterparameter `image_id`. `sonoma`Ersetzen Sie im folgenden Beispiel durch eine von macOS unterstützte Hauptversion, `x86_64_mac` durch den Prozessor und `region-code` durch eine unterstützte Version, AWS-Region für die Sie die neueste macOS-AMI-ID benötigen.

```
aws ssm get-parameter --name /aws/service/ec2-macos/sonoma/x86_64_mac/latest/image_id
 --region region-code
```

Weitere Informationen finden Sie unter Aufrufen der öffentlichen AMI-Parameter für macOS im AWS Systems Manager -Benutzerhandbuch.

AMIs Versionshinweise zu Amazon EC2 macOS

Die folgenden Informationen enthalten Details zu den Paketen, die standardmäßig in EC2 macOS enthalten sind, AMIs und fassen die Änderungen für jede EC2 macOS-AMI-Version zusammen.

Informationen zum Abonnieren von macOS-AMI-Benachrichtigungen finden Sie unter So abonnieren Sie macOS-AMI-Benachrichtigungen.

Mac-Instances können eines der folgenden Betriebssysteme ausführen:

- macOS Mojave (Version 10.14) (nur x86-Mac-Instances)
- macOS Catalina (Version 10.15) (nur x86-Mac-Instances)
- macOS Big Sur (Version 11) (x86- und M1-Mac-Instances)
- macOS Monterey (Version 12) (x86- und M1-Mac-Instances)

- macOS Ventura (Version 13) (alle Mac-Instances, M2- und M2-Pro-Mac-Instances unterstützen macOS-Ventura-Version 13.2 oder höher)
- macOS Sonoma (Version 14) (alle Mac-Instances)
- macOS Sequoia (Version 15) (alle Mac-Instances)

> **Note**
>
> M4- und M4-Pro-Mac-Instances unterstützen macOS Sequoia Version 15.6 oder höher.

Datenschutzrichtlinien für lokale Netzwerke für macOS Sequoia genehmigen

macOS Sequoia (Version 15) verfügt über eine neue Funktion zum Schutz lokaler Netzwerke, die sich auf Benutzer lokaler IP-basierter Dienste auswirkt, darunter Amazon EC2 Instance Metadata Service (IMDS).

> **Important**
>
> Gehen Sie wie folgt vor, um sicherzustellen, dass Sie ununterbrochenen Zugriff auf lokale IP-basierte Services haben, um die Datenschutzrichtlinien für lokale Netzwerke zu genehmigen.

So genehmigen Sie Datenschutzrichtlinien für lokale Netzwerke

1. Eine Verbindung mit der grafischen Benutzerschnittstelle (GUI) Ihrer Instance herstellen.
2. Folgen Sie den Anweisungen auf dem Bildschirm, um die Datenschutzrichtlinien für lokale Netzwerke zu genehmigen.
3. Nachdem Sie die Richtlinien genehmigt haben, erstellen Sie ein AMI Ihrer EC2 Mac-Instance. Weitere Informationen finden Sie unter Ein Amazon-EBS-gestütztes AMI erstellen.

Alle EC2 Mac-Instances, die über das neu erstellte AMI gestartet werden, behalten die Local Network Privacy -Berechtigungen.

In Amazon EC2 macOS enthaltene Standardpakete AMIs

In der folgenden Tabelle werden Pakete beschrieben, die standardmäßig im EC2 macOS enthalten sind AMIs.

Pakete	Versionshinweise
EC2 macOS Init	https://github.com/aws/ec2-macos-init/tags
EC2 macOS Utils	https://github.com/aws/ec2-macos-utils/tags
Amazon-SSM-Agent	https://github.com/aws/amazon-ssm-agent/releases
AWS Command Line Interface (AWS CLI) Version 2	https://raw.githubusercontent.com/aws/aws-cli/v2/CHANGELOG.rst
Befehlszeilen-Tools für Xcode	https://developer.apple.com/documentation/xcode-release-notes
Homebrew	https://github.com/Homebrew/brew/releases
EC2 Instanzverbindung	https://github.com/aws/aws-ec2-instance-connect-config/releases
Safari	https://developer.apple.com/documentation/safari-release-notes

AMI-Aktualisierungen für Amazon EC2 macOS

In der folgenden Tabelle werden die Änderungen beschrieben, die in den EC2 macOS-AMI-Versionen enthalten sind. Beachten Sie, dass einige Änderungen für alle EC2 macOS gelten AMIs, während andere nur für einen Teil davon AMIs gelten.

EC2 macOS AMI-Aktualisierungen

Veröffentlichung	Änderungen
2025.11.18	Alle AMIs • Auf `awscli` 2.31.35 aktualisiert • Auf 1.5.13 aktualisiert `ec2-macos-init` • Auf 1.0.7 aktualisiert `ec2-macos-utils`

Veröffentlichung	Änderungen

	• Homebrew wurde auf 5.0.1 aktualisiert
	
	Veröffentlichung von macOS Sonoma 14.8.1
	
	• Sicherheitsinhalt von macOS Sonoma 14.8.1
	• Safari wurde auf 26.0.1 aktualisiert
	  • Sicherheitsinhalt von Safari 26.0.1
	
	Veröffentlichung von macOS Sequoia 15.7.1
	
	• Sicherheitsinhalt von macOS Sequoia 15.7.1
	• Safari wurde auf 26.0.1 aktualisiert
	  • Sicherheitsinhalt von Safari 18.6
	• Die Befehlszeilentools wurden auf 26.0 aktualisiert
	
	Veröffentlichung von macOS Tahoe 26.0.1
	
	• Sicherheitsinhalt von macOS Tahoe 26.0.1
	• Die Befehlszeilentools wurden auf 26.0 aktualisiert

Veröffentlichung	Änderungen
2025.09.04	Alle AMIs • Auf `awscli` 2.28.19 aktualisiert • Homebrew wurde auf 4.6.7 aktualisiert Veröffentlichung von macOS Ventura 13.7.8 • Sicherheitsinhalt von macOS Ventura 13.7.8 Veröffentlichung von macOS Sonoma 14.7.8 • Sicherheitsinhalt von macOS Sonoma 14.7.8 Veröffentlichung von macOS Sequoia 15.6.1 • Sicherheitsinhalt von macOS Sequoia 15.6.1

Veröffentlichung	Änderungen

2025.08.05	Alle AMIs
	• Auf `awscli` 2.28.0 aktualisiert
	• Homebrew wurde auf 4.5.13 aktualisiert
	
	Veröffentlichung von macOS Ventura 13.7.7
	• Sicherheitsinhalt von macOS Ventura 13.7.7
	• Safari wurde auf 18.6 aktualisiert
	  • Sicherheitsinhalt von Safari 18.6
	
	Veröffentlichung von macOS Sonoma 14.7.7
	• Sicherheitsinhalt von macOS Sonoma 14.7.7
	• Safari wurde auf 18.6 aktualisiert
	  • Sicherheitsinhalt von Safari 18.6
	
	Veröffentlichung von macOS Sequoia 15.6
	• Sicherheitsinhalt von macOS Sequoia 15.6
	• AWS ENA Ethernet wurde auf 2.0.0 aktualisiert

Veröffentlichung	Änderungen

2025.06.27	Alle AMIs
	• Auf `awscli` 2.27.40 aktualisiert
	• Homebrew wurde auf 4.5.7 aktualisiert
	• x86_64-Bilder auf ENA Ethernet-Text migriert AWS
	
	Veröffentlichung von macOS Ventura 13.7.6
	• Sicherheitsinhalt von macOS Ventura 13.7.6
	• Safari wurde auf 18.5 aktualisiert
	  • Sicherheitsinhalt von Safari 18.5
	
	Veröffentlichung von macOS Sonoma 14.7.6
	• Sicherheitsinhalt von macOS Sonoma 14.7.6
	• Safari wurde auf 18.5 aktualisiert
	  • Sicherheitsinhalt von Safari 18.5
	
	Veröffentlichung von macOS Sequoia 15.5
	• Sicherheitsinhalt von macOS Sequoia 15.5
	• Die Befehlszeilentools wurden auf 16.4 aktualisiert
	• AWS ENA Ethernet wurde auf 1.0.9 aktualisiert

Veröffentlichung	Änderungen

2025.05.21	Alle AMIs
	• Auf `awscli` 2.27.7 aktualisiert
	• Auf 1.5.11 aktualisiert `ec2-macos-init`
	• Auf 1.0.5 aktualisiert `ec2-macos-utils`
	• Homebrew wurde auf 4.5.1 aktualisiert
	
	Veröffentlichung von macOS Ventura 13.7.5
	• Sicherheitsinhalt von macOS Ventura 13.7.5
	• Safari wurde auf 18.4 aktualisiert
	  • Sicherheitsinhalt von Safari 18.4
	
	Veröffentlichung von macOS Sonoma 14.7.5
	• Sicherheitsinhalt von macOS Sonoma 14.7.5
	• Safari wurde auf 18.4 aktualisiert
	  • Sicherheitsinhalt von Safari 18.4
	
	Veröffentlichung von macOS Sequoia 15.4.1
	• Sicherheitsinhalt von macOS Sequoia 15.4.1
	• Die Befehlszeilentools wurden auf 16.3 aktualisiert

Veröffentlichung	Änderungen

2025.05.05	Alle AMIs
	• Auf `awscli` 2.27.1 aktualisiert
	• Auf 1.5.11 aktualisiert `ec2-macos-init`
	• Auf 1.3.1 aktualisiert `ec2-macos-system-monitor`
	• Auf 1.0.5 aktualisiert `ec2-macos-utils`
	• Homebrew wurde auf 4.4.32 aktualisiert
	
	Veröffentlichung von macOS Ventura 13.7.5
	• Sicherheitsinhalt von macOS Ventura 13.7.5
	• Safari wurde auf 18.4 aktualisiert
	  • Sicherheitsinhalt von Safari 18.4
	
	Veröffentlichung von macOS Sonoma 14.7.5
	• Sicherheitsinhalt von macOS Sonoma 14.7.5
	• Safari wurde auf 18.4 aktualisiert
	  • Sicherheitsinhalt von Safari 18.4
	
	Veröffentlichung von macOS Sequoia 15.4.1
	• Sicherheitsinhalt von macOS Sequoia 15.4.1

Veröffentlichung	Änderungen
18.03.2025	Alle AMIs • Auf `awscli` 2.24.2 aktualisiert • Homebrew wurde auf 4.4.20 aktualisiert Veröffentlichung von macOS Sequoia 15.3.1 • Sicherheitsinhalt von macOS Sequoia 15.3.1 Veröffentlichung von macOS Sonoma 14.7.4 • Sicherheitsinhalt von macOS Sonoma 14.7.4 • Safari wurde auf 18.3 aktualisiert Veröffentlichung von macOS Ventura 13.7.4 • Sicherheitsinhalt von macOS Ventura 13.7.4 • Safari wurde auf 18.3 aktualisiert

Veröffentlichung	Änderungen
2025.01.24	Alle AMIs • Auf `awscli` 2.22.33 aktualisiert • Homebrew wurde auf 4.4.15 aktualisiert Veröffentlichung von macOS Sequoia 15.2 • Sicherheitsinhalt von macOS Sequoia 15.2 • Die Befehlszeilentools wurden auf 16.2 aktualisiert Veröffentlichung von macOS Sonoma 14.7.2 • Sicherheitsinhalt von macOS Sonoma 14.7.2 • Safari wurde auf 18.2 aktualisiert • Die Befehlszeilentools wurden auf 16.2 aktualisiert Veröffentlichung von macOS Ventura 13.7.2 • Sicherheitsinhalt von macOS Ventura 13.7.2 • Safari wurde auf 18.2 aktualisiert

Veröffentlichung	Änderungen
2024.12.20	Alle AMIs • Homebrew wurde auf 4.4.8 aktualisiert • Auf 2.22.5 aktualisiert `aws-cli` • `amazon-ssm-agent` zu 3.3.987.0 aktualisiert Veröffentlichung von macOS Sequoia 15.1.1 • Sicherheitsinhalt von macOS Sequoia 15.1.1 Veröffentlichung von macOS Sonoma 14.7.1 • Sicherheitsinhalt von macOS Sonoma 14.7.1 • Safari wurde auf 18.1.1 aktualisiert Veröffentlichung von macOS Ventura 13.7.1 • Sicherheitsinhalt von macOS Ventura 13.7.1 • Safari wurde auf 18.1.1 aktualisiert

Veröffentlichung	Änderungen

2024.10.28	Alle AMIs
	• Homebrew auf 4.4.2 aktualisiert
	• `aws-cli` zu 2.18.13 aktualisiert
	• `amazon-ssm-agent` zu 3.3.987.0 aktualisiert
	• `ec2-macos-init` zu 1.5.10 aktualisiert
	• `ec2-macos-utils` zu 1.0.4 aktualisiert
	
	Veröffentlichung von macOS Sequoia 15.0
	• Sicherheitsinhalt von macOS Sequoia 15
	
	Veröffentlichung von macOS Sonoma 14.7
	• Sicherheitsinhalt von macOS Sonoma 14.7.
	• Die Befehlszeilentools wurden auf Version 16.0 aktualisiert
	• Safari wurde auf 18.0.1 aktualisiert
	  • Sicherheitsinhalt von Safari 18
	
	Veröffentlichung von macOS Ventura 13.7
	• Sicherheitsinhalt von macOS Sonoma 13.7
	• Safari wurde auf 18.0.1 aktualisiert
	  • Sicherheitsinhalt von Safari 18

Veröffentlichung	Änderungen

2024.08.20	Alle AMIs
	• Homebrew auf 4.3.14 aktualisiert
	• `aws-cli` zu 2.17.29 aktualisiert
	
	Veröffentlichung von macOS Sonoma 14.6.1
	• Keine veröffentlichten CVE-Einträge.
	
	Veröffentlichung von macOS Ventura 13.6.9
	• Keine veröffentlichten CVE-Einträge.
	• Safari wurde auf 17.6 aktualisiert
	  • Sicherheitsinhalt von Safari 17.6
	
	Veröffentlichung von macOS Monterey 12.7.6
	• Sicherheitsinhalt von macOS Monterey 12.7.6
	• Safari wurde auf 17.6 aktualisiert
	  • Sicherheitsinhalt von Safari 17.6

Veröffentlichung	Änderungen

2024.06.07	Alle AMIs
	• Homebrew auf 4.3.1-1 aktualisiert
	• `aws-cli` zu 2.15.56 aktualisiert
	• `amazon-ssm-agent` zu 3.3.380.0-1 aktualisiert
	
	Veröffentlichung von macOS Sonoma 14.5
	• Sicherheitsinhalt von macOS Sonoma 14.5
	
	Veröffentlichung von macOS Ventura 13.6.7
	• Sicherheitsinhalt von macOS Sonoma 13.6.7
	• Safari wurde auf 17.5 aktualisiert
	  • Sicherheitsinhalt von Safari 17.5
	
	Veröffentlichung von macOS Monterey 12.7.5
	• Sicherheitsinhalt von macOS Monterey 12.7.5
	• Safari wurde auf 17.5 aktualisiert
	  • Sicherheitsinhalt von Safari 17.5

Veröffentlichung	Änderungen

2024.04.12	Alle AMIs
	• Homebrew auf 4.2.16-1 aktualisiert
	• `aws-cli` zu 2.15.36 aktualisiert
	
	Veröffentlichung von macOS Sonoma 14.4.1
	• Sicherheitsinhalt von macOS Sonoma 14.4.1
	
	Veröffentlichung von macOS Ventura 13.6.6
	• Sicherheitsinhalt von macOS Sonoma 13.6.6
	• Safari wurde auf 17.4.1 aktualisiert
	  • Sicherheitsinhalt von Safari 17.4.1
	
	Für macOS Monterey
	• Safari wurde auf 17.4.1 aktualisiert
	  • Sicherheitsinhalt von Safari 17.4.1

Für Amazon EBS optimierte Instance-Typen

Amazon EBS-optimierte Instances verwenden einen optimierten Konfigurations-Stack und bieten zusätzliche, dedizierte Bandbreite für Amazon EBS I/O. This optimization provides the best performance for your EBS volumes by minimizing contention between Amazon EBS I/O und anderen Traffic von Ihrer Instance.

Wenn sie einer EBS-optimierten Instance zugeordnet sind, sind Allzweck-SSD (`gp2` und `gp3`)-Volumes darauf ausgelegt, mindestens 90 % ihrer bereitgestellten IOPS-Leistung zu 99 % der Zeit in einem bestimmten Jahr bereitzustellen. Bereitgestellte IOPS-SSD (`io1` und `io2`)-Volumes sind darauf ausgelegt, mindestens 90 % ihrer bereitgestellten IOPS-Leistung zu 99,9 % der Zeit in einem Jahr bereitzustellen. Durchsatzoptimierte HDD (`st1`) und Cold-HDD (`sc1`) liefern mindestens 90 % ihrer erwarteten Durchsatzleistung in 99 % der Zeit in einem bestimmten Jahr. Nicht konforme Zeiträume sind ungefähr gleichmäßig verteilt, wobei 99 Prozent des erwarteten Gesamtdurchsatzes

pro Stunde angestrebt werden. Weitere Informationen finden Sie unter Amazon-EBS-Volume-Typen im Amazon-EBS-Benutzerhandbuch.

Einige Instance-Typen sind standardmäßig EBS-optimiert. Sie müssen sie nicht aktivieren und es hat auch keine Auswirkungen, wenn Sie versuchen, sie zu deaktivieren. Andere Instance-Typen unterstützen optional die EBS-Optimierung. Sie können sie während oder nach dem Start gegen eine zusätzliche Stundengebühr aktivieren. Weitere Informationen finden Sie unter Anzeigen von Instance-Typen, die EBS-Optimierung unterstützen.

Detaillierte Spezifikationen und Funktionen für Instance-Typen finden Sie im Amazon EC2 Instance Types Guide.

Überlegungen

- Die EBS-Leistung einer Instance wird durch die Leistungsgrenzen der Instance oder die aggregierte Leistung der angefügten Volumes begrenzt, je nachdem, welcher Wert kleiner ist. Um die maximale EBS-Leistung zu erreichen, muss eine Instance über angefügte Volumes verfügen, die zusammen eine Leistung bereitstellen, die der maximalen Leistung der Instance entspricht oder darüber liegt. Um beispielsweise `80,000` IOPS für `r6i.16xlarge` zu erreichen, müssen für die Instance mindestens 5 `gp2`-Volumes mit jeweils `16,000` IOPS bereitgestellt werden (5 Volumes x `16,000` IOPS = `80,000` IOPS), oder es kann 1 `gp3`-Volume mit `80,000` IOPS bereitgestellt werden. Wir empfehlen Ihnen, einen Instance-Typ zu wählen, der mehr dedizierten Amazon EBS-Durchsatz bietet, als Ihre Anwendung benötigt. Andernfalls EC2 kann die Verbindung zwischen Amazon EBS und Amazon zu einem Leistungsengpass werden.
- Die maximale Anzahl von Amazon-EBS-Volumes, die Sie einer Instance anfügen können, hängt vom Instance-Typ und der Instance-Größe ab. Weitere Informationen finden Sie unter Amazon EBS-Volumenlimits für Amazon-Instances EC2 .
- Die maximalen IOPS- und Durchsatzgrenzen hängen voneinander ab. Abhängig von Ihrer I/O Größe erreichen Sie möglicherweise ein Limit vor dem anderen, was sich auf die Gesamtleistung auswirken kann. Um optimale Ergebnisse zu erzielen, sollten Sie bei der Planung Ihrer Workload beide Limits berücksichtigen.

Standardmäßig EBS-optimiert

Die folgenden Instance-Typen sind standardmäßig EBS-optimiert. Die EBS-Optimierung muss nicht aktiviert werden, und ihre Deaktivierung hat keinerlei Auswirkungen.

Instances

- Allgemeine Zwecke
- Für Datenverarbeitung optimiert
- Arbeitsspeicher optimiert
- Speicheroptimiert
- Beschleunigtes Computing
- Datenverarbeitung in Hochleistung

Allgemeine Zwecke

> **Note**
>
> Die Instance-Typen M8a, M8g, M8gd, M8i und M8i-flex unterstützen konfigurierbare Bandbreitengewichtungen. Mit diesen Instance-Typen können Sie die Bandbreite einer Instance entweder für die Netzwerkleistung oder die Amazon-EBS-Leistung optimieren. Die folgende Tabelle zeigt die standardmäßige Amazon-EBS-Bandbreitenleistung für diese Instance-Typen. Weitere Informationen finden Sie unter EC2 Konfiguration der Gewichtung der Instanz-Bandbreite.

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
a1.medium [1]	300	3500	37,50	437,50	2500	20000
a1.large [1]	525	3500	65,62	437,50	4000	20000
a1.xlarge [1]	800	3500	100,00	437,50	6 000	20000
a1.2xlarge [1]	1750	3500	218,75	437,50	10000	20000
a1.4xlarge [2]	3500		437,5		20000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
a1.metal [2]	3500		437,5		20000	
m4.large [2]	450		56,25		3600	
m4.xlarge [2]	750		93,75		6 000	
m4.2xlarge [2]	1000		125,0		8000	
m4.4xlarge [2]	2000		250,0		16000	
m4.10xlarge [2]	4000		500,0		32000	
m4.16xlarge [2]	10000		1250,0		65000	
m5.large [1]	650	4750	81,25	593,75	3600	18750
m5.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
m5.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
m5.4xlarge [2]	4750		593,75		18750	
m5.8xlarge [2]	6800		850,0		30000	
m5.12xlarge [2]	9500		1187,5		40000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m5.16xlarge [2]	13600		1700,0		60000	
m5.24xlarge [2]	19000		2375,0		80000	
m5.metal [2]	19000		2375,0		80000	
m5a.large [1]	650	2880	81,25	360,00	3600	16000
m5a.xlarge [1]	1085	2880	135,62	360,00	6 000	16000
m5a.2xlarge [1]	1580	2880	197,50	360,00	8333	16000
m5a.4xlarge [2]	2880		360,0		16000	
m5a.8xlarge [2]	4750		593,75		20000	
m5a.12xlarge [2]	6780		847,5		30000	
m5a.16xlarge [2]	9500		1187,5		40000	
m5a.24xlarge [2]	13750		1718,75		60000	
m5ad.large [1]	650	2880	81,25	360,00	3600	16000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m5ad.xlarge [1]	1085	2880	135,62	360,00	6 000	16000
m5ad.2xlarge [1]	1580	2880	197,50	360,00	8333	16000
m5ad.4xlarge [2]	2880		360,0		16000	
m5ad.8xlarge [2]	4750		593,75		20000	
m5ad.12xlarge [2]	6780		847,5		30000	
m5ad.16xlarge [2]	9500		1187,5		40000	
m5ad.24xlarge [2]	13750		1718,75		60000	
m5d.large [1]	650	4750	81,25	593,75	3600	18750
m5d.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
m5d.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
m5d.4xlarge [2]	4750		593,75		18750	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m5d.8xlarge [2]	6800		850,0		30000	
m5d.12xlarge [2]	9500		1187,5		40000	
m5d.16xlarge [2]	13600		1700,0		60000	
m5d.24xlarge [2]	19000		2375,0		80000	
m5d.metal [2]	19000		2375,0		80000	
m5dn.large [1]	650	4750	81,25	593,75	3600	18750
m5dn.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
m5dn.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
m5dn.4xlarge [2]	4750		593,75		18750	
m5dn.8xlarge [2]	6800		850,0		30000	
m5dn.12xlarge [2]	9500		1187,5		40000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m5dn.16xlarge [2]	13600		1700,0		60000	
m5dn.24xlarge [2]	19000		2375,0		80000	
m5dn.metal [2]	19000		2375,0		80000	
m5n.large [1]	650	4750	81,25	593,75	3600	18750
m5n.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
m5n.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
m5n.4xlarge [2]	4750		593,75		18750	
m5n.8xlarge [2]	6800		850,0		30000	
m5n.12xlarge [2]	9500		1187,5		40000	
m5n.16xlarge [2]	13600		1700,0		60000	
m5n.24xlarge [2]	19000		2375,0		80000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m5n.metal [2]	19000		2375,0		80000	
m5zn.large [1]	800	3170	100,00	396,25	3333	13333
m5zn.xlarge [1]	1564	3170	195,50	396,25	6667	13333
m5zn.2xlarge [2]	3170		396,25		13333	
m5zn.3xlarge [2]	4750		593,75		20000	
m5zn.6xlarge [2]	9500		1187,5		40000	
m5zn.12xlarge [2]	19000		2375,0		80000	
m5zn.metal [2]	19000		2375,0		80000	
m6a.large [1]	650	10000	81,25	1250,00	3600	40000
m6a.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
m6a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m6a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m6a.8xlarge [2]	10000		1250,0		40000	
m6a.12xlarge [2]	15000		1875,0		60000	
m6a.16xlarge [2]	20000		2500,0		80000	
m6a.24xlarge [2]	30000		3750,0		120000	
m6a.32xlarge [2]	40000		5000,0		160000	
m6a.48xlarge [2]	40000		5000,0		240000	
m6a.metal [2]	40000		5000,0		240000	
m6g.medium [1]	315	4750	39,38	593,75	2500	20000
m6g.large [1]	630	4750	78,75	593,75	3600	20000
m6g.xlarge [1]	1188	4750	148,50	593,75	6 000	20000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m6g.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
m6g.4xlarge [2]	4750		593,75		20000	
m6g.8xlarge [2]	9500		1187,5		40000	
m6g.12xlarge [2]	14250		1781,25		50000	
m6g.16xlarge [2]	19000		2375,0		80000	
m6g.metal [2]	19000		2375,0		80000	
m6gd.medium [1]	315	4750	39,38	593,75	2500	20000
m6gd.large [1]	630	4750	78,75	593,75	3600	20000
m6gd.xlarge [1]	1188	4750	148,50	593,75	6 000	20000
m6gd.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
m6gd.4xlarge [2]	4750		593,75		20000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m6gd.8xlarge [2]	9500		1187,5		40000	
m6gd.12xlarge [2]	14250		1781,25		50000	
m6gd.16xlarge [2]	19000		2375,0		80000	
m6gd.metal [2]	19000		2375,0		80000	
m6i.large [1]	650	10000	81,25	1250,00	3600	40000
m6i.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
m6i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m6i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m6i.8xlarge [2]	10000		1250,0		40000	
m6i.12xlarge [2]	15000		1875,0		60000	
m6i.16xlarge [2]	20000		2500,0		80000	
m6i.24xlarge [2]	30000		3750,0		120000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m6i.32xlarge [2]	40000		5000,0		160000	
m6i.metal [2]	40000		5000,0		160000	
m6id.large [1]	650	10000	81,25	1250,00	3600	40000
m6id.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
m6id.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m6id.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m6id.8xlarge [2]	10000		1250,0		40000	
m6id.12xlarge [2]	15000		1875,0		60000	
m6id.16xlarge [2]	20000		2500,0		80000	
m6id.24xlarge [2]	30000		3750,0		120000	
m6id.32xlarge [2]	40000		5000,0		160000	
m6id.metal [2]	40000		5000,0		160000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m6idn.large [1]	1562	25000	195,31	3125,00	6250	100000
m6idn.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
m6idn.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
m6idn.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
m6idn.8xlarge [2]	25000		312,50		100000	
m6idn.12xlarge [2]	37500		4687,5		150000	
m6idn.16xlarge [2]	50000		6250,0		200000	
m6idn.24xlarge [2]	75000		9375,0		300000	
m6idn.32xlarge [2]	100000		12500,0		400000	
m6idn.metal [2]	100000		12500,0		400000	
m6in.large [1]	1562	25000	195,31	3125,00	6250	100000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
m6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
m6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
m6in.8xlarge [2]	25000		312,50		100000	
m6in.12xlarge [2]	37500		4687,5		150000	
m6in.16xlarge [2]	50000		6250,0		200000	
m6in.24xlarge [2]	75000		9375,0		300000	
m6in.32xlarge [2]	100000		12500,0		400000	
m6in.metal [2]	100000		12500,0		400000	
m7a.medium [1]	325	10000	40,62	1250,00	2500	40000
m7a.large [1]	650	10000	81,25	1250,00	3600	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m7a.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
m7a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m7a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7a.8xlarge [2]	10000		1250,0		40000	
m7a.12xlarge [2]	15000		1875,0		60000	
m7a.16xlarge [2]	20000		2500,0		80000	
m7a.24xlarge [2]	30000		3750,0		120000	
m7a.32xlarge [2]	40000		5000,0		160000	
m7a.48xlarge [2]	40000		5000,0		240000	
m7a.metal-48xl [2]	40000		5000,0		240000	
m7g.medium [1]	315	10000	39,38	1250,00	2500	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m7g.large [1]	630	10000	78,75	1250,00	3600	40000
m7g.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
m7g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m7g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7g.8xlarge [2]	10000		1250,0		40000	
m7g.12xlarge [2]	15000		1875,0		60000	
m7g.16xlarge [2]	20000		2500,0		80000	
m7g.metal [2]	20000		2500,0		80000	
m7gd.medium [1]	315	10000	39,38	1250,00	2500	40000
m7gd.large [1]	630	10000	78,75	1250,00	3600	40000
m7gd.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m7gd.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m7gd.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7gd.8xlarge [2]	10000		1250,0		40000	
m7gd.12xlarge [2]	15000		1875,0		60000	
m7gd.16xlarge [2]	20000		2500,0		80000	
m7gd.metal [2]	20000		2500,0		80000	
m7i.large [1]	650	10000	81,25	1250,00	3600	40000
m7i.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
m7i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m7i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7i.8xlarge [2]	10000		1250,0		40000	
m7i.12xlarge [2]	15000		1875,0		60000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m7i.16xlarge [2]	20000		2500,0		80000	
m7i.24xlarge [2]	30000		3750,0		120000	
m7i.48xlarge [2]	40000		5000,0		240000	
m7i.metal-24xl [2]	30000		3750,0		120000	
m7i.metal-48xl [2]	40000		5000,0		240000	
m7i-flex.large [1]	312	10000	39,06	1250,00	2500	40000
m7i-flex.xlarge [1]	625	10000	78,12	1250,00	3600	40000
m7i-flex.2xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
m7i-flex.4xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m7i-flex.8xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7i-flex.12xlarge 1	7500	15000	937,50	1875,00	30000	60000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m7i-flex.16x groß 1	10000	20000	1250,00	2500,00	40000	80000
m8a.mittel 1	325	10000	40,62	1250,00	2500	40000
8 m² groß 1	650	10000	81,25	1250,00	3600	40000
8 m x L 1	1250	10000	156,25	1250,00	6 000	40000
m8a.2xgroß 1	2500	10000	312,50	1250,00	12000	40000
m8a.4x groß 1	5000	10000	625,00	1250,00	20000	40000
m8 x 8 x groß 2	10000		1250,0		40000	
m8a.12x groß 2	15000		1875,0		60000	
8 m x 16 x groß 2	20000		2500,0		80000	
m8 x 24 x groß 2	30000		3750,0		120000	
m8 x 48 x groß 2	60000		7500,0		240000	
Größe: Metall, 24 x L 2	30000		3750,0		120000	
m8a.metall-48 xl 2	60000		7500,0		240000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m8g.medium [1]	315	10000	39,38	1250,00	2500	40000
m8g.large [1]	630	10000	78,75	1250,00	3600	40000
m8g.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
m8g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m8g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m8g.8xlarge [2]	10000		1250,0		40000	
m8g.12xlarge [2]	15000		1875,0		60000	
m8g.16xlarge [2]	20000		2500,0		80000	
m8g.24xlarge [2]	30000		3750,0		120000	
m8g.48xlarge [2]	40000		5000,0		240000	
m8g.metal-24xl [2]	30000		3750,0		120000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m8g.metal-48xl [2]	40000		5000,0		240000	
8 mg. Medium 1	315	10000	39,38	1250,00	2500	40000
8 g, groß 1	630	10000	78,75	1250,00	3600	40000
8 mg.xlarge 1	1250	10000	156,25	1250,00	6 000	40000
8 g, 2 x groß 1	2500	10000	312,50	1250,00	12000	40000
8 g x 4 x groß 1	5000	10000	625,00	1250,00	20000	40000
8 g x 8 x L 2	10000		1250,0		40000	
8 m g, 12 x groß 2	15000		1875,0		60000	
8 g, 16 x groß 2	20000		2500,0		80000	
m8gd.24xlarge [2]	30000		3750,0		120000	
8 m g, 48 x groß 2	40000		5000,0		240000	
m8gd.metal-24xl [2]	30000		3750,0		120000	
m8g.metal-48xl [2]	40000		5000,0		240000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
8m. groß 1	650	10000	81,25	1250,00	3600	40000
m8i.xlarge 1	1250	10000	156,25	1250,00	6 000	40000
m 8 i 2 x groß 1	2500	10000	312,50	1250,00	12000	40000
m 8i.4 x groß 1	5000	10000	625,00	1250,00	20000	40000
m 8 x 8 x groß 2	10000		1250,0		40000	
m 8i. 12 x groß 2	15000		1875,0		60000	
m 8i, 16 x groß 2	20000		2500,0		80000	
m 8i, 24 x groß 2	30000		3750,0		120000	
m8i.32x groß 2	40000		5000,0		160000	
m 8i, 48 x groß 2	60000		7500,0		240000	
m8i.96x groß 2	80000		10000,0		480000	
m8i.metall-48xl 2	60000		7500,0		240000	
M8i.Metall-96 XL 2	80000		10000,0		480000	
m8i-flex.groß 1	315	10000	39,38	1250,00	2500	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m8i-flex.xlarge 1	630	10000	78,75	1250,00	3600	40000
m8i-flex.2xgroß 1	1250	10000	156,25	1250,00	6 000	40000
m8i-flex.4xgroß 1	2500	10000	312,50	1250,00	12000	40000
m8i-flex.8xgroß 1	5000	10000	625,00	1250,00	20000	40000
m8i-flex.12xlarge 1	7500	15000	937,50	1875,00	30000	60000
m8i-flex.16xgroß 1	10000	20000	1250,00	2500,00	40000	80000
mac1.metal [2]	14000		1750,0		80000	
mac2.metal [2]	10000		1250,0		55000	
mac2-m1ultra.metal [2]	10000		1250,0		55000	
mac2-m2.metal [2]	8000		1000,0		55000	
mac2-m2pro.metal [2]	8000		1000,0		55000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
mac-m4.metal [2]	8000		1000,0		55000	
mac-m4pro.metal [2]	8000		1000,0		55000	
t3.nano [1]	43	2085	5,38	260,62	250	11800
t3.micro [1]	87	2085	10,88	260,62	500	11800
t3.small [1]	174	2085	21,75	260,62	1000	11800
t3.medium [1]	347	2085	43,38	260,62	2000	11800
t3.large [1]	695	2780	86,88	347,50	4000	15700
t3.xlarge [1]	695	2780	86,88	347,50	4000	15700
t3.2xlarge [1]	695	2780	86,88	347,50	4000	15700
t3a.nano [1]	45	2085	5,62	260,62	250	11800
t3a.micro [1]	90	2085	11,25	260,62	500	11800
t3a.small [1]	175	2085	21,88	260,62	1000	11800
t3a.medium [1]	350	2085	43,75	260,62	2000	11800
t3a.large [1]	695	2780	86,88	347,50	4000	15700
t3a.xlarge [1]	695	2780	86,88	347,50	4000	15700
t3a.2xlarge [1]	695	2780	86,88	347,50	4000	15700

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
t4g.nano [1]	43	2085	5,38	260,62	250	11800
t4g.micro [1]	87	2085	10,88	260,62	500	11800
t4g.small [1]	174	2085	21,75	260,62	1000	11800
t4g.medium [1]	347	2085	43,38	260,62	2000	11800
t4g.large [1]	695	2780	86,88	347,50	4000	15700
t4g.xlarge [1]	695	2780	86,88	347,50	4000	15700
t4g.2xlarge [1]	695	2780	86,88	347,50	4000	15700

[1] Diese Instances können mindestens einmal alle 24 Stunden für 30 Minuten die maximale Leistung erbringen, danach fallen sie auf ihre Basisleistung zurück.

[2] Diese Instances können ihre angegebene Leistung auf unbestimmte Zeit aufrechterhalten. Wenn Ihre Workload länger als 30 Minuten anhaltende maximale Leistung erfordert, verwenden Sie eine dieser Instances.

Für Datenverarbeitung optimiert

> **Note**
>
> Die Instance-Typen C8a, C8g, C8GD, C8i, C8i-Flex unterstützen konfigurierbare Bandbreitengewichtungen. Mit diesen Instance-Typen können Sie die Bandbreite einer Instance entweder für die Netzwerkleistung oder die Amazon-EBS-Leistung optimieren. Die folgende Tabelle zeigt die standardmäßige Amazon-EBS-Bandbreitenleistung für diese Instance-Typen. Weitere Informationen finden Sie unter EC2 Konfiguration der Gewichtung der Instanz-Bandbreite.

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c4.large [2]	500		62,5		4000	
c4.xlarge [2]	750		93,75		6 000	
c4.2xlarge [2]	1000		125,0		8000	
c4.4xlarge [2]	2000		250,0		16000	
c4.8xlarge [2]	4000		500,0		32000	
c5.large [1]	650	4750	81,25	593,75	4000	20000
c5.xlarge [1]	1150	4750	143,75	593,75	6 000	20000
c5.2xlarge [1]	2300	4750	287,50	593,75	10000	20000
c5.4xlarge [2]	4750		593,75		20000	
c5.9xlarge [2]	9500		1187,5		40000	
c5.12xlarge [2]	9500		1187,5		40000	
c5.18xlarge [2]	19000		2375,0		80000	
c5.24xlarge [2]	19000		2375,0		80000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c5.metal [2]	19000		2375,0		80000	
c5a.large [1]	200	3170	25,00	396,25	800	13300
c5a.xlarge [1]	400	3170	50,00	396,25	1600	13300
c5a.2xlarge [1]	800	3170	100,00	396,25	3200	13300
c5a.4xlarge [1]	1580	3170	197,50	396,25	6600	13300
c5a.8xlarge [2]	3170		396,25		13300	
c5a.12xlarge [2]	4750		593,75		20000	
c5a.16xlarge [2]	6300		787,5		26700	
c5a.24xlarge [2]	9500		1187,5		40000	
c5ad.large [1]	200	3170	25,00	396,25	800	13300
c5ad.xlarge [1]	400	3170	50,00	396,25	1600	13300
c5ad.2xlarge [1]	800	3170	100,00	396,25	3200	13300

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c5ad.4xlarge [1]	1580	3170	197,50	396,25	6600	13300
c5ad.8xlarge [2]	3170		396,25		13300	
c5ad.12xlarge [2]	4750		593,75		20000	
c5ad.16xlarge [2]	6300		787,5		26700	
c5ad.24xlarge [2]	9500		1187,5		40000	
c5d.large [1]	650	4750	81,25	593,75	4000	20000
c5d.xlarge [1]	1150	4750	143,75	593,75	6 000	20000
c5d.2xlarge [1]	2300	4750	287,50	593,75	10000	20000
c5d.4xlarge [2]	4750		593,75		20000	
c5d.9xlarge [2]	9500		1187,5		40000	
c5d.12xlarge [2]	9500		1187,5		40000	
c5d.18xlarge [2]	19000		2375,0		80000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c5d.24xlarge [2]	19000		2375,0		80000	
c5d.metal [2]	19000		2375,0		80000	
c5n.large [1]	650	4750	81,25	593,75	4000	20000
c5n.xlarge [1]	1150	4750	143,75	593,75	6 000	20000
c5n.2xlarge [1]	2300	4750	287,50	593,75	10000	20000
c5n.4xlarge [2]	4750		593,75		20000	
c5n.9xlarge [2]	9500		1187,5		40000	
c5n.18xlarge [2]	19000		2375,0		80000	
c5n.metal [2]	19000		2375,0		80000	
c6a.large [1]	650	10000	81,25	1250,00	3600	40000
c6a.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
c6a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c6a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c6a.8xlarge [2]	10000		1250,0		40000	
c6a.12xlarge [2]	15000		1875,0		60000	
c6a.16xlarge [2]	20000		2500,0		80000	
c6a.24xlarge [2]	30000		3750,0		120000	
c6a.32xlarge [2]	40000		5000,0		160000	
c6a.48xlarge [2]	40000		5000,0		240000	
c6a.metal [2]	40000		5000,0		240000	
c6g.medium [1]	315	4750	39,38	593,75	2500	20000
c6g.large [1]	630	4750	78,75	593,75	3600	20000
c6g.xlarge [1]	1188	4750	148,50	593,75	6 000	20000
c6g.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
c6g.4xlarge [2]	4750		593,75		20000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c6g.8xlarge [2]	9500		1187,5		40000	
c6g.12xlarge [2]	14250		1781,25		50000	
c6g.16xlarge [2]	19000		2375,0		80000	
c6g.metal [2]	19000		2375,0		80000	
c6gd.medium [1]	315	4750	39,38	593,75	2500	20000
c6gd.large [1]	630	4750	78,75	593,75	3600	20000
c6gd.xlarge [1]	1188	4750	148,50	593,75	6 000	20000
c6gd.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
c6gd.4xlarge [2]	4750		593,75		20000	
c6gd.8xlarge [2]	9500		1187,5		40000	
c6gd.12xlarge [2]	14250		1781,25		50000	
c6gd.16xlarge [2]	19000		2375,0		80000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c6gd.metal [2]	19000		2375,0		80000	
c6gn.medium [1]	760	9500	95,00	1187,50	2500	40000
c6gn.large [1]	1235	9500	154,38	1187,50	5000	40000
c6gn.xlarge [1]	2375	9500	296,88	1187,50	10000	40000
c6gn.2xlarge [1]	4750	9500	593,75	1187,50	20000	40000
c6gn.4xlarge [2]	9500		1187,5		40000	
c6gn.8xlarge [2]	19000		2375,0		80000	
c6gn.12xlarge [2]	28500		3562,5		120000	
c6gn.16xlarge [2]	38000		4750,0		160000	
c6i.large [1]	650	10000	81,25	1250,00	3600	40000
c6i.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
c6i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c6i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c6i.8xlarge [2]	10000		1250,0		40000	
c6i.12xlarge [2]	15000		1875,0		60000	
c6i.16xlarge [2]	20000		2500,0		80000	
c6i.24xlarge [2]	30000		3750,0		120000	
c6i.32xlarge [2]	40000		5000,0		160000	
c6i.metal [2]	40000		5000,0		160000	
c6id.large [1]	650	10000	81,25	1250,00	3600	40000
c6id.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
c6id.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c6id.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c6id.8xlarge [2]	10000		1250,0		40000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c6id.12xlarge [2]	15000		1875,0		60000	
c6id.16xlarge [2]	20000		2500,0		80000	
c6id.24xlarge [2]	30000		3750,0		120000	
c6id.32xlarge [2]	40000		5000,0		160000	
c6id.metal [2]	40000		5000,0		160000	
c6in.large [1]	1562	25000	195,31	3125,00	6250	100000
c6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
c6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
c6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
c6in.8xlarge [2]	25000		312,50		100000	
c6in.12xlarge [2]	37500		4687,5		150000	
c6in.16xlarge [2]	50000		6250,0		200000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c6in.24xlarge [2]	75000		9375,0		300000	
c6in.32xlarge [2]	100000		12500,0		400000	
c6in.metal [2]	100000		12500,0		400000	
c7a.medium [1]	325	10000	40,62	1250,00	2500	40000
c7a.large [1]	650	10000	81,25	1250,00	3600	40000
c7a.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
c7a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c7a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7a.8xlarge [2]	10000		1250,0		40000	
c7a.12xlarge [2]	15000		1875,0		60000	
c7a.16xlarge [2]	20000		2500,0		80000	
c7a.24xlarge [2]	30000		3750,0		120000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c7a.32xlarge [2]	40000		5000,0		160000	
c7a.48xlarge [2]	40000		5000,0		240000	
c7a.metal-48xl [2]	40000		5000,0		240000	
c7g.medium [1]	315	10000	39,38	1250,00	2500	40000
c7g.large [1]	630	10000	78,75	1250,00	3600	40000
c7g.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
c7g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c7g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7g.8xlarge [2]	10000		1250,0		40000	
c7g.12xlarge [2]	15000		1875,0		60000	
c7g.16xlarge [2]	20000		2500,0		80000	
c7g.metal [2]	20000		2500,0		80000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c7gd.medium [1]	315	10000	39,38	1250,00	2500	40000
c7gd.large [1]	630	10000	78,75	1250,00	3600	40000
c7gd.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
c7gd.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c7gd.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7gd.8xlarge [2]	10000		1250,0		40000	
c7gd.12xlarge [2]	15000		1875,0		60000	
c7gd.16xlarge [2]	20000		2500,0		80000	
c7gd.metal [2]	20000		2500,0		80000	
c7gn.medium [1]	521	10000	65,12	1250,00	2083	40000
c7gn.large [1]	1042	10000	130,25	1250,00	4167	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c7gn.xlarge [1]	2083	10000	260,38	1250,00	8333	40000
c7gn.2xlarge [1]	4167	10000	520,88	1250,00	16667	40000
c7gn.4xlarge [1]	833	10000	1041,62	1250,00	33333	40000
c7gn.8xlarge [1]	16667	20000	2083,38	2500,00	66667	80000
c7gn.12xlarge [1]	25000	30000	3125,00	3750,00	100000	120000
c7gn.16xlarge [1]	33333	40000	4166,62	5000,00	133333	160000
c7gn.metal [1]	33333	40000	4166,62	5000,00	133333	160000
c7i.large [1]	650	10000	81,25	1250,00	3600	40000
c7i.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
c7i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c7i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7i.8xlarge [2]	10000		1250,0		40000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c7i.12xlarge [2]	15000		1875,0		60000	
c7i.16xlarge [2]	20000		2500,0		80000	
c7i.24xlarge [2]	30000		3750,0		120000	
c7i.48xlarge [2]	40000		5000,0		240000	
c7i.metal-24xl [2]	30000		3750,0		120000	
c7i.metal-48xl [2]	40000		5000,0		240000	
c7i-flex.large [1]	312	10000	39,06	1250,00	2500	40000
c7i-flex.xlarge [1]	625	10000	78,12	1250,00	3600	40000
c7i-flex.2xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
c7i-flex.4xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c7i-flex.8xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c7i-flex. 12xlarge 1	7500	15000	937,50	1875,00	30000	60000
c7i-flex.16x groß 1	10000	20000	1250,00	2500,00	40000	80000
c8a.mittel 1	325	10000	40,62	1250,00	2500	40000
c8a.groß 1	650	10000	81,25	1250,00	3600	40000
c8a.xlarge 1	1250	10000	156,25	1250,00	6 000	40000
c8a.2xgroß 1	2500	10000	312,50	1250,00	12000	40000
c8a.4x groß 1	5000	10000	625,00	1250,00	20000	40000
ca. 8 x 8 x groß 2	10000		1250,0		40000	
c8a.12xlarge 2	15000		1875,0		60000	
c8a.16x groß 2	20000		2500,0		80000	
c8a.24x groß 2	30000		3750,0		120000	
ca 8 x 48 x groß 2	60000		7500,0		240000	
c8a.metall-24xl 2	30000		3750,0		120000	
c8a.metal-48 xl 2	60000		7500,0		240000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c8g.medium [1]	315	10000	39,38	1250,00	2500	40000
c8g.large [1]	630	10000	78,75	1250,00	3600	40000
c8g.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
c8g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c8g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c8g.8xlarge [2]	10000			1250,0	40000	
c8g.12xlarge [2]	15000			1875,0	60000	
c8g.16xlarge [2]	20000			2500,0	80000	
c8g.24xlarge [2]	30000			3750,0	120000	
c8g.48xlarge [2]	40000			5000,0	240000	
c8g.metal-24xl [2]	30000			3750,0	120000	
c8g.metal-48xl [2]	40000			5000,0	240000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c 8 GB. Medium 1	1562	25000	195,31	3125,00	7500	120000
8 GB, groß 1	3125	25000	390,62	3125,00	15000	120000
c8gb.xlarge 1	6250	25000	781,25	3125,00	30000	120000
c 8 GB. 2 x groß 1	12500	25000	1562,50	3125,00	60000	120000
c 8 GB. 4 x groß 2	25000		312,50		120000	
c 8 GB. 8 x groß 2	50000		6250,0		240000	
8 GB. 12 x groß 2	75000		9375,0		360000	
8 GB. 16 x groß 2	100000		12500,0		480000	
8 GB. 24 x groß 2	150000		18750,0		720000	
C 8 GB, Metall, 24 XL 2	150000		18750,0		720000	
c8gd.medium [1]	315	10000	39,38	1250,00	2500	40000
c8gd.large 1	630	10000	78,75	1250,00	3600	40000
c8gd.xlarge 1	1250	10000	156,25	1250,00	6 000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
cm 8 g, 2 x groß 1	2500	10000	312,50	1250,00	12000	40000
c8gd.4xgroß 1	5000	10000	625,00	1250,00	20000	40000
cm 8 g, 8 x groß 2	10000		1250,0		40000	
8 g, 12 x groß 2	15000		1875,0		60000	
8 g, 16 x groß 2	20000		2500,0		80000	
c8gd.24xlarge [2]	30000		3750,0		120000	
c8gd.48xlarge [2]	40000		5000,0		240000	
c8gd.metal-24xl [2]	30000		3750,0		120000	
c8gd.metal-48xl [2]	40000		5000,0		240000	
c8gn.medium 1	760	10000	95,00	1250,00	2500	40000
8 g, groß 1	1250	10000	156,25	1250,00	5000	40000
c8gn.xlarge 1	2500	10000	312,50	1250,00	10000	40000
8 g n.2 x groß 1	5000	10000	625,00	1250,00	20000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
8 g n.4 x groß 2	10000		1250,0		40000	
8 g n.8 x groß 2	20000		2500,0		80000	
8 g n, 12 x groß 2	30000		3750,0		120000	
c8gn.16x groß 2	40000		5000,0		160000	
c8gn.24xlarge [2]	60000		7500,0		240000	
c8gn.48xlarge [2]	60000		7500,0		240000	
c8gn.metal-24xl [2]	60000		7500,0		240000	
c8gn.metal-48xl [2]	60000		7500,0		240000	
c8i.groß 1	650	10000	81,25	1250,00	3600	40000
c8i.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
c8i.2 x groß 1	2500	10000	312,50	1250,00	12000	40000
c8i.4x groß 1	5000	10000	625,00	1250,00	20000	40000
c8i.8xgroß 2	10000		1250,0		40000	
c8i.12xlarge 2	15000		1875,0		60000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c8i.16x groß 2	20000		2500,0		80000	
c8i.24x groß 2	30000		3750,0		120000	
c8i.32x groß 2	40000		5000,0		160000	
c8i.48x groß 2	60000		7500,0		240000	
c8i.96xlarge [2]	80000		10000,0		480000	
c8i.metall-48xl 2	60000		7500,0		240000	
c8i.metall-96 xl 2	80000		10000,0		480000	
c8i-flex.groß 1	315	10000	39,38	1250,00	2500	40000
c8i-flex.xlarge 1	630	10000	78,75	1250,00	3600	40000
c8i-flex.2xgroß 1	1250	10000	156,25	1250,00	6 000	40000
c8i-flex.4x groß 1	2500	10000	312,50	1250,00	12000	40000
c8i-flex.8xgroß 1	5000	10000	625,00	1250,00	20000	40000
c8i-flex. 12xlarge 1	7500	15000	937,50	1875,00	30000	60000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	MB/s, 128 KiB I/OBasisdurchsatz ()	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c8i-flex.16xlarge [1]	10000	20000	1250,00	2500,00	40000	80000

[1] Diese Instances können mindestens einmal alle 24 Stunden für 30 Minuten die maximale Leistung erbringen, danach fallen sie auf ihre Basisleistung zurück.

[2] Diese Instances können ihre angegebene Leistung auf unbestimmte Zeit aufrechterhalten. Wenn Ihre Workload länger als 30 Minuten anhaltende maximale Leistung erfordert, verwenden Sie eine dieser Instances.

Arbeitsspeicher optimiert

> **Note**
>
> - Die Instance-Typen R8a, R8g, R8gd, R8i, R8i-Flex, x8G, x8AEDZ unterstützen konfigurierbare Bandbreitengewichtungen. Mit diesen Instance-Typen können Sie die Bandbreite einer Instance entweder für die Netzwerkleistung oder die Amazon-EBS-Leistung optimieren. Die folgende Tabelle zeigt die standardmäßige Amazon-EBS-Bandbreitenleistung für diese Instance-Typen. Weitere Informationen finden Sie unter EC2 Konfiguration der Gewichtung der Instanz-Bandbreite.
> - Für eine maximale IOPS-Leistung mit U7i-Instances empfehlen wir die Verwendung BlockExpress von io2-Volumes.

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r4.large [2]	425		53.125		3000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r4.xlarge [2]	850		106,25		6 000	
r4.2xlarge [2]	1700		212,5		12000	
r4.4xlarge [2]	3500		437,5		18750	
r4.8xlarge [2]	7000		875,0		37500	
r4.16xlarge [2]	14000		1750,0		75000	
r5.large [1]	650	4750	81,25	593,75	3600	18750
r5.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
r5.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
r5.4xlarge [2]	4750		593,75		18750	
r5.8xlarge [2]	6800		850,0		30000	
r5.12xlarge [2]	9500		1187,5		40000	
r5.16xlarge [2]	13600		1700,0		60000	
r5.24xlarge [2]	19000		2375,0		80000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r5.metal [2]	19000		2375,0		80000	
r5a.large [1]	650	2880	81,25	360,00	3600	16000
r5a.xlarge [1]	1085	2880	135,62	360,00	6 000	16000
r5a.2xlarge [1]	1580	2880	197,50	360,00	8333	16000
r5a.4xlarge [2]	2880		360,0		16000	
r5a.8xlarge [2]	4750		593,75		20000	
r5a.12xlarge [2]	6780		847,5		30000	
r5a.16xlarge [2]	9500		1187,5		40000	
r5a.24xlarge [2]	13570		1696,25		60000	
r5ad.large [1]	650	2880	81,25	360,00	3600	16000
r5ad.xlarge [1]	1085	2880	135,62	360,00	6 000	16000
r5ad.2xlarge [1]	1580	2880	197,50	360,00	8333	16000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r5ad.4xlarge [2]	2880		360,0		16000	
r5ad.8xlarge [2]	4750		593,75		20000	
r5ad.12xlarge [2]	6780		847,5		30000	
r5ad.16xlarge [2]	9500		1187,5		40000	
r5ad.24xlarge [2]	13570		1696,25		60000	
r5b.large [1]	1250	10000	156,25	1250,00	5417	43333
r5b.xlarge [1]	2500	10000	312,50	1250,00	10833	43333
r5b.2xlarge [1]	5000	10000	625,00	1250,00	21667	43333
r5b.4xlarge [2]	10000		1250,0		43333	
r5b.8xlarge [2]	20000		2500,0		86667	
r5b.12xlarge [2]	30000		3750,0		130000	
r5b.16xlarge [2]	40000		5000,0		173333	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r5b.24xlarge [2]	60000		7500,0		260000	
r5b.metal [2]	60000		7500,0		260000	
r5d.large [1]	650	4750	81,25	593,75	3600	18750
r5d.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
r5d.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
r5d.4xlarge [2]	4750		593,75		18750	
r5d.8xlarge [2]	6800		850,0		30000	
r5d.12xlarge [2]	9500		1187,5		40000	
r5d.16xlarge [2]	13600		1700,0		60000	
r5d.24xlarge [2]	19000		2375,0		80000	
r5d.metal [2]	19000		2375,0		80000	
r5dn.large [1]	650	4750	81,25	593,75	3600	18750
r5dn.xlarge [1]	1150	4750	143,75	593,75	6 000	18750

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r5dn.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
r5dn.4xlarge [2]	4750		593,75		18750	
r5dn.8xlarge [2]	6800		850,0		30000	
r5dn.12xlarge [2]	9500		1187,5		40000	
r5dn.16xlarge [2]	13600		1700,0		60000	
r5dn.24xlarge [2]	19000		2375,0		80000	
r5dn.metal [2]	19000		2375,0		80000	
r5n.large [1]	650	4750	81,25	593,75	3600	18750
r5n.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
r5n.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
r5n.4xlarge [2]	4750		593,75		18750	
r5n.8xlarge [2]	6800		850,0		30000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r5n.12xlarge [2]	9500		1187,5		40000	
r5n.16xlarge [2]	13600		1700,0		60000	
r5n.24xlarge [2]	19000		2375,0		80000	
r5n.metal [2]	19000		2375,0		80000	
r6a.large [1]	650	10000	81,25	1250,00	3600	40000
r6a.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
r6a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r6a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r6a.8xlarge [2]	10000		1250,0		40000	
r6a.12xlarge [2]	15000		1875,0		60000	
r6a.16xlarge [2]	20000		2500,0		80000	
r6a.24xlarge [2]	30000		3750,0		120000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r6a.32xlarge [2]	40000		5000,0		160000	
r6a.48xlarge [2]	40000		5000,0		240000	
r6a.metal [2]	40000		5000,0		240000	
r6g.medium [1]	315	4750	39,38	593,75	2500	20000
r6g.large [1]	630	4750	78,75	593,75	3600	20000
r6g.xlarge [1]	1188	4750	148,50	593,75	6 000	20000
r6g.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
r6g.4xlarge [2]	4750		593,75		20000	
r6g.8xlarge [2]	9500		1187,5		40000	
r6g.12xlarge [2]	14250		1781,25		50000	
r6g.16xlarge [2]	19000		2375,0		80000	
r6g.metal [2]	19000		2375,0		80000	
r6gd.medium [1]	315	4750	39,38	593,75	2500	20000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r6gd.large [1]	630	4750	78,75	593,75	3600	20000
r6gd.xlarge [1]	1188	4750	148,50	593,75	6 000	20000
r6gd.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
r6gd.4xlarge [2]	4750		593,75		20000	
r6gd.8xlarge [2]	9500		1187,5		40000	
r6gd.12xlarge [2]	14250		1781,25		50000	
r6gd.16xlarge [2]	19000		2375,0		80000	
r6gd.metal [2]	19000		2375,0		80000	
r6i.large [1]	650	10000	81,25	1250,00	3600	40000
r6i.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
r6i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r6i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r6i.8xlarge [2]	10000		1250,0		40000	
r6i.12xlarge [2]	15000		1875,0		60000	
r6i.16xlarge [2]	20000		2500,0		80000	
r6i.24xlarge [2]	30000		3750,0		120000	
r6i.32xlarge [2]	40000		5000,0		160000	
r6i.metal [2]	40000		5000,0		160000	
r6id.large [1]	650	10000	81,25	1250,00	3600	40000
r6id.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
r6id.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r6id.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r6id.8xlarge [2]	10000		1250,0		40000	
r6id.12xlarge [2]	15000		1875,0		60000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r6id.16xlarge [2]	20000		2500,0		80000	
r6id.24xlarge [2]	30000		3750,0		120000	
r6id.32xlarge [2]	40000		5000,0		160000	
r6id.metal [2]	40000		5000,0		160000	
r6idn.large [1]	1562	25000	195,31	3125,00	6250	100000
r6idn.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
r6idn.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
r6idn.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
r6idn.8xlarge [2]	25000		312,50		100000	
r6idn.12xlarge [2]	37500		4687,5		150000	
r6idn.16xlarge [2]	50000		6250,0		200000	
r6idn.24xlarge [2]	75000		9375,0		300000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r6idn.32xlarge [2]	100000		12500,0		400000	
r6idn.metal [2]	100000		12500,0		400000	
r6in.large [1]	1562	25000	195,31	3125,00	6250	100000
r6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
r6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
r6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
r6in.8xlarge [2]	25000		312,50		100000	
r6in.12xlarge [2]	37500		4687,5		150000	
r6in.16xlarge [2]	50000		6250,0		200000	
r6in.24xlarge [2]	75000		9375,0		300000	
r6in.32xlarge [2]	100000		12500,0		400000	
r6in.metal [2]	100000		12500,0		400000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r7a.medium [1]	325	10000	40,62	1250,00	2500	40000
r7a.large [1]	650	10000	81,25	1250,00	3600	40000
r7a.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
r7a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r7a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7a.8xlarge [2]	10000		1250,0		40000	
r7a.12xlarge [2]	15000		1875,0		60000	
r7a.16xlarge [2]	20000		2500,0		80000	
r7a.24xlarge [2]	30000		3750,0		120000	
r7a.32xlarge [2]	40000		5000,0		160000	
r7a.48xlarge [2]	40000		5000,0		240000	
r7a.metal-48xl [2]	40000		5000,0		240000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r7g.medium [1]	315	10000	39,38	1250,00	2500	40000
r7g.large [1]	630	10000	78,75	1250,00	3600	40000
r7g.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
r7g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r7g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7g.8xlarge [2]	10000		1250,0		40000	
r7g.12xlarge [2]	15000		1875,0		60000	
r7g.16xlarge [2]	20000		2500,0		80000	
r7g.metal [2]	20000		2500,0		80000	
r7gd.medium [1]	315	10000	39,38	1250,00	2500	40000
r7gd.large [1]	630	10000	78,75	1250,00	3600	40000
r7gd.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r7gd.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r7gd.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7gd.8xlarge [2]	10000		1250,0		40000	
r7gd.12xlarge [2]	15000		1875,0		60000	
r7gd.16xlarge [2]	20000		2500,0		80000	
r7gd.metal [2]	20000		2500,0		80000	
r7i.large [1]	650	10000	81,25	1250,00	3600	40000
r7i.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
r7i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r7i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7i.8xlarge [2]	10000		1250,0		40000	
r7i.12xlarge [2]	15000		1875,0		60000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r7i.16xlarge [2]	20000		2500,0		80000	
r7i.24xlarge [2]	30000		3750,0		120000	
r7i.48xlarge [2]	40000		5000,0		240000	
r7i.metal-24xl [2]	30000		3750,0		120000	
r7i.metal-48xl [2]	40000		5000,0		240000	
r7iz.large [1]	792	10000	99,00	1250,00	3600	40000
r7iz.xlarge [1]	1584	10000	198,00	1250,00	6667	40000
r7iz.2xlarge [1]	3168	10000	396,00	1250,00	13333	40000
r7iz.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7iz.8xlarge [2]	10000		1250,0		40000	
r7iz.12xlarge [2]	19000		2375,0		76000	
r7iz.16xlarge [2]	20000		2500,0		80000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r7iz.32xlarge [2]	40000		5000,0		160000	
r7iz.metal-16xl [2]	20000		2500,0		80000	
r7iz.metal-32xl [2]	40000		5000,0		160000	
r8a.medium [1]	325	10000	40,62	1250,00	2500	40000
R8a.groß 1	650	10000	81,25	1250,00	3600	40000
r8a.xlarge 1	1250	10000	156,25	1250,00	6 000	40000
r8a.2xgroß 1	2500	10000	312,50	1250,00	12000	40000
r8a.4x groß 1	5000	10000	625,00	1250,00	20000	40000
r8a.8 x groß 2	10000		1250,0		40000	
r8a.12xlarge 2	15000		1875,0		60000	
r8a.16x groß 2	20000		2500,0		80000	
r8a.24x groß 2	30000		3750,0		120000	
r8a.48x groß 2	60000		7500,0		240000	
r8a.metal-24 xl 2	30000		3750,0		120000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r8a.metal-48 xl [2]	60000		7500,0		240000	
r8g.medium [1]	315	10000	39,38	1250,00	2500	40000
r8g.large [1]	630	10000	78,75	1250,00	3600	40000
r8g.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
r8g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r8g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r8g.8xlarge [2]	10000		1250,0		40000	
r8g.12xlarge [2]	15000		1875,0		60000	
r8g.16xlarge [2]	20000		2500,0		80000	
r8g.24xlarge [2]	30000		3750,0		120000	
r8g.48xlarge [2]	40000		5000,0		240000	
r8g.metal-24xl [2]	30000		3750,0		120000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r8g.metal-48xl [2]	40000		5000,0		240000	
r8gb.medium [1]	1562	25000	195,31	3125,00	7500	120000
r8gb.large [1]	3125	25000	390,62	3125,00	15000	120000
r8gb.xlarge [1]	6250	25000	781,25	3125,00	30000	120000
r8gb.2xlarge [1]	12500	25000	1562,50	3125,00	60000	120000
r8gb.4xlarge [2]	25000		312,50		120000	
r8gb.8xlarge [2]	50000		6250,0		240000	
r8gb.12xlarge [2]	75000		9375,0		360000	
r8gb.16xlarge [2]	100000		12500,0		480000	
r8gb.24xlarge [2]	150000		18750,0		720000	
r8gb.metal-24xl [2]	150000		18750,0		720000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r8gd.medium [1]	315	10000	39,38	1250,00	2500	40000
8 g, groß 1	630	10000	78,75	1250,00	3600	40000
r8gd.xlarge 1	1250	10000	156,25	1250,00	6 000	40000
r 8 g d.2 x groß 1	2500	10000	312,50	1250,00	12000	40000
r8gd.4xgroß 1	5000	10000	625,00	1250,00	20000	40000
r 8 g d 8 x groß 2	10000		1250,0		40000	
R 8 g D, 12 x groß 2	15000		1875,0		60000	
R 8 g D, 16 x groß 2	20000		2500,0		80000	
r8gd.24xlarge [2]	30000		3750,0		120000	
r8gd.48xlarge [2]	40000		5000,0		240000	
r8gd.metal-24xl [2]	30000		3750,0		120000	
r8gd.metal-48xl [2]	40000		5000,0		240000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r8gn.medium [1]	760	10000	95,00	1250,00	2500	40000
r8gn.large [1]	1250	10000	156,25	1250,00	5000	40000
r8gn.xlarge [1]	2500	10000	312,50	1250,00	10000	40000
r8gn.2xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r8gn.4xlarge [2]	10000		1250,0		40000	
r8gn.8xlarge [2]	20000		2500,0		80000	
r8gn.12xlarge [2]	30000		3750,0		120000	
r8gn.16xlarge [2]	40000		5000,0		160000	
r8gn.24xlarge [2]	60000		7500,0		240000	
r8gn.48xlarge [2]	60000		7500,0		240000	
r8gn.metal-24xl [2]	60000		7500,0		240000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r8gn.metal-48xl [2]	60000		7500,0		240000	
R8i. Groß 1	650	10000	81,25	1250,00	3600	40000
r8i.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
r8i.2 x groß 1	2500	10000	312,50	1250,00	12000	40000
r8i.4x groß 1	5000	10000	625,00	1250,00	20000	40000
r8i.8 x groß 2	10000		1250,0		40000	
r8i.12xlarge 2	15000		1875,0		60000	
r8i.16x groß 2	20000		2500,0		80000	
r8i.24x groß 2	30000		3750,0		120000	
r8i.32x groß 2	40000		5000,0		160000	
r8i.48x groß 2	60000		7500,0		240000	
r8i.96xlarge [2]	80000		10000,0		480000	
r8i.metall-48xl 2	60000		7500,0		240000	
r8i.metal-96xl 2	80000		10000,0		480000	
r8i-flex.large [1]	315	10000	39,38	1250,00	2500	40000
r8i-flex.xlarge [1]	630	10000	78,75	1250,00	3600	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r8i-flex.2xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
r8i-flex.4xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r8i-flex.8xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r8i-flex.12xlarge [1]	7500	15000	937,50	1875,00	30000	60000
r8i-flex.16xlarge [1]	10000	20000	1250,00	2500,00	40000	80000
u-3tb1.56xlarge [2]	19000		2375,0		80000	
u-6tb1.56xlarge [2]	38000		4750,0		160000	
u-6tb1.112xlarge [2]	38000		4750,0		160000	
u-6tb1.metal [2]	38000		4750,0		160000	
u-9tb1.112xlarge [2]	38000		4750,0		160000	
u-9tb1.metal [2]	38000		4750,0		160000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
u-12tb1.112xlarge [2]	38000		4750,0		160000	
u-12tb1.metal [2]	38000		4750,0		160000	
u-18tb1.112xlarge [2]	38000		4750,0		160000	
u-18tb1.metal [2]	38000		4750,0		160000	
u-24tb1.112xlarge [2]	38000		4750,0		160000	
u-24tb1.metal [2]	38000		4750,0		160000	
u7i-6tb.112xlarge [2]	100000		12500,0		560000	
u7i-8tb.112xlarge [2]	100000		12500,0		560000	
u7i-12tb.224xlarge [2]	100000		12500,0		560000	
u7in-16tb.224xlarge [2]	100000		12500,0		560000	
u7in-24tb.224xlarge [2]	100000		12500,0		560000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
u7in-32tb.224xlarge [2]	100000		12500,0		560000	
u7inh-32tb.480xlarge [2]	160000		20000,0		840000	
x1.16xlarge [2]	7000		875,0		40000	
x1.32xlarge [2]	14000		1750,0		80000	
x1e.xlarge [2]	500		62,5		3700	
x1e.2xlarge [2]	1000		125,0		7400	
x1e.4xlarge [2]	1750		218,75		10000	
x1e.8xlarge [2]	3500		437,5		20000	
x1e.16xlarge [2]	7000		875,0		40000	
x1e.32xlarge [2]	14000		1750,0		80000	
x2gd.medium [1]	315	4750	39,38	593,75	2500	20000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
x2gd.large [1]	630	4750	78,75	593,75	3600	20000
x2gd.xlarge [1]	1188	4750	148,50	593,75	6 000	20000
x2gd.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
x2gd.4xlarge [2]	4750		593,75		20000	
x2gd.8xlarge [2]	9500		1187,5		40000	
x2gd.12xlarge [2]	14250		1781,25		60000	
x2gd.16xlarge [2]	19000		2375,0		80000	
x2gd.metal [2]	19000		2375,0		80000	
x2idn.16xlarge [2]	40000		5000,0		173333	
x2idn.24xlarge [2]	60000		7500,0		260000	
x2idn.32xlarge [2]	80000		10000,0		260000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
x2idn.metal [2]	80000		10000,0		260000	
x2iedn.xlarge [1]	2500	20000	312,50	2500,00	8125	65000
x2iedn.2xlarge [1]	5000	20000	625,00	2500,00	16250	65000
x2iedn.4xlarge [1]	10000	20000	1250,00	2500,00	32500	65000
x2iedn.8xlarge [2]	20000		2500,0		65000	
x2iedn.16xlarge [2]	40000		5000,0		130000	
x2iedn.24xlarge [2]	60000		7500,0		195000	
x2iedn.32xlarge [2]	80000		10000,0		260000	
x2iedn.metal [2]	80000		10000,0		260000	
x2iezn.2xlarge [2]	3170		396,25		13333	
x2iezn.4xlarge [2]	4750		593,75		20000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
x2iezn.6xlarge [2]	9500		1187,5		40000	
x2iezn.8xlarge [2]	12000		1500,0		55000	
x2iezn.12xlarge [2]	19000		2375,0		80000	
x2iezn.metal [2]	19000		2375,0		80000	
x8g.medium [1]	315	10000	39,38	1250,00	2500	40000
x8g.large [1]	630	10000	78,75	1250,00	3600	40000
x8g.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
x8g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
x8g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
x8g.8xlarge [2]	10000		1250,0		40000	
x8g.12xlarge [2]	15000		1875,0		60000	
x8g.16xlarge [2]	20000		2500,0		80000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
x8g.24xlarge [2]	30000		3750,0		120000	
x8g.48xlarge [2]	40000		5000,0		240000	
x8g.metal-24xl [2]	30000		3750,0		120000	
x8g.metal-48xl [2]	40000		5000,0		240000	
x8aedz.large 1	1250	15000	156,25	1875,00	5000	60000
x8aedz.xlarge 1	2500	15000	312,50	1875,00	10000	60000
x8aedz.3xgroß 1	7500	15000	937,50	1875,00	30000	60000
x8aedz.6xgroß 2	15000		1875,0		60000	
x8aedz.12xlarge 2	30000		3750,0		120000	
x8aedz.24xlarge 2	60000		7500,0		240000	
x8aedz.metall-12xl 2	30000		3750,0		120000	
x8aedz.metall-24xl 2	60000		7500,0		240000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Basisdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
z1d.large [1]	800	3170	100,00	396,25	3333	13333
z1d.xlarge [1]	1580	3170	197,50	396,25	6667	13333
z1d.2xlarge [2]	3170		396,25		13333	
z1d.3xlarge [2]	4750		593,75		20000	
z1d.6xlarge [2]	9500		1187,5		40000	
z1d.12xlarge [2]	19000		2375,0		80000	
z1d.metal [2]	19000		2375,0		80000	

[1] Diese Instances können mindestens einmal alle 24 Stunden für 30 Minuten die maximale Leistung erbringen, danach fallen sie auf ihre Basisleistung zurück.

[2] Diese Instances können ihre angegebene Leistung auf unbestimmte Zeit aufrechterhalten. Wenn Ihre Workload länger als 30 Minuten anhaltende maximale Leistung erfordert, verwenden Sie eine dieser Instances.

Speicheroptimiert

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
d2.xlarge [2]	750		93,75		6 000	
d2.2xlarge [2]	1000		125,0		8000	
d2.4xlarge [2]	2000		250,0		16000	
d2.8xlarge [2]	4000		500,0		32000	
d3.xlarge [1]	850	2800	106,25	350,00	5000	15000
d3.2xlarge [1]	1700	2800	212,50	350,00	10000	15000
d3.4xlarge [2]	2800		350,0		15000	
d3.8xlarge [2]	5000		625,0		30000	
d3en.xlarge [1]	850	2800	106,25	350,00	5000	15000
d3en.2xlarge [1]	1700	2800	212,50	350,00	10000	15000
d3en.4xlarge [2]	2800		350,0		15000	
d3en.6xlarge [2]	4000		500,0		25000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
d3en.8xlarge [2]	5000		625,0		30000	
d3en.12xlarge [2]	7000		875,0		40000	
h1.2xlarge [2]	1750		218,75		12000	
h1.4xlarge [2]	3500		437,5		20000	
h1.8xlarge [2]	7000		875,0		40000	
h1.16xlarge [2]	14000		1750,0		80000	
i3.large [2]	425		53.125		3000	
i3.xlarge [2]	850		106,25		6 000	
i3.2xlarge [2]	1700		212,5		12000	
i3.4xlarge [2]	3500		437,5		16000	
i3.8xlarge [2]	7000		875,0		32500	
i3.16xlarge [2]	14000		1750,0		65000	
i3.metal [2]	19000		2375,0		80000	
i3en.large [1]	576	4750	72,10	593,75	3000	20000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
i3en.xlarge [1]	1153	4750	144,20	593,75	6 000	20000
i3en.2xlarge [1]	2307	4750	288,39	593,75	12000	20000
i3en.3xlarge [1]	3800	4750	475,00	593,75	15000	20000
i3en.6xlarge [2]	4750		593,75		20000	
i3en.12xlarge [2]	9500		1187,5		40000	
i3en.24xlarge [2]	19000		2375,0		80000	
i3en.metal [2]	19000		2375,0		80000	
i4g.large [1]	625	10000	78,12	1250,00	2500	40000
i4g.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i4g.2xlarge [1]	2500	10000	312,50	1250,00	10000	40000
i4g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
i4g.8xlarge [2]	10000		1250,0		40000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
i4g.16xlarge [2]	20000		2500,0		80000	
i4i.large [1]	625	10000	78,12	1250,00	2500	40000
i4i.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i4i.2xlarge [1]	2500	10000	312,50	1250,00	10000	40000
i4i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
i4i.8xlarge [2]	10000		1250,0		40000	
i4i.12xlarge [2]	15000		1875,0		60000	
i4i.16xlarge [2]	20000		2500,0		80000	
i4i.24xlarge [2]	30000		3750,0		120000	
i4i.32xlarge [2]	40000		5000,0		160000	
i4i.metal [2]	40000		5000,0		160000	
i7i.groß 1	625	10000	78,12	1250,00	2500	40000
i7i.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i7i.2 x groß 1	2500	10000	312,50	1250,00	10000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
i7i.4x groß 1	5000	10000	625,00	1250,00	20000	40000
i7i.8 x groß 2	10000		1250,0		40000	
i7i.12xlarge 2	15000		1875,0		60000	
i7i.16x groß 2	20000		2500,0		80000	
i7i.24x groß 2	30000		3750,0		120000	
i7i.48xlarge 2	60000		7500,0		240000	
i7i.metal -24xl [2]	30000		3750,0		120000	
i7i.metal -48xl [2]	60000		7500,0		240000	
i7ie.large [1]	625	10000	78,12	1250,00	2500	40000
i7ie.xlarge 1	1250	10000	156,25	1250,00	5000	40000
i7ie.2xlarge 1	2500	10000	312,50	1250,00	10000	40000
i7ie.3xlarge 1	3750	10000	468,75	1250,00	15000	40000
i7ie.6xlarge 1	7500	10000	937,50	1250,00	30000	40000
i7ie.12xlarge [2]	15000		1875,0		60000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
i7ie.18xlarge [2]	2500		2812,5		90000	
i7ie.24xlarge [2]	30000		3750,0		120000	
i7ie.48xlarge [2]	60000		7500,0		240000	
i7ie.metal-24xl [2]	30000		3750,0		120000	
i7ie.metal-48xl [2]	60000		7500,0		240000	
i8g.large [1]	625	10000	78,12	1250,00	2500	40000
i8g.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i8g.2xlarge [1]	2500	10000	312,50	1250,00	10000	40000
i8g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
i8g.8xlarge [2]	10000		1250,0		40000	
i8g.12xlarge [2]	15000		1875,0		60000	
i8g.16xlarge [2]	20000		2500,0		80000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
i8g.24xlarge [2]	30000		3750,0		120000	
i 8 g, 48 x groß 2	60000		7500,0		240000	
i8g.metal-24xl [2]	30000		3750,0		120000	
i8ge.large [1]	625	10000	78,12	1250,00	2500	40000
i8ge.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i8ge.2xlarge [1]	2500	10000	312,50	1250,00	10000	40000
i8ge.3xlarge [1]	3750	10000	468,75	1250,00	15000	40000
i8ge.6xlarge [1]	7500	10000	937,50	1250,00	30000	40000
i8ge.12xlarge [2]	15000		1875,0		60000	
i8ge.18xlarge [2]	2500		2812,5		90000	
i8ge.24xlarge [2]	30000		3750,0		120000	
i8ge.48xlarge [2]	60000		7500,0		240000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
i8ge.metal-24xl [2]	30000		3750,0		120000	
i8ge.metal-48xl [2]	60000		7500,0		240000	
im4gn.large [1]	1250	10000	156,25	1250,00	5000	40000
im4gn.xlarge [1]	2500	10000	312,50	1250,00	10000	40000
im4gn.2xlarge [1]	5000	10000	625,00	1250,00	20000	40000
im4gn.4xlarge [2]	10000		1250,0		40000	
im4gn.8xlarge [2]	20000		2500,0		80000	
im4gn.16xlarge [2]	40000		5000,0		160000	
is4gen.medium [1]	625	10000	78,12	1250,00	2500	40000
is4gen.large [1]	1250	10000	156,25	1250,00	5000	40000
is4gen.xlarge [1]	2500	10000	312,50	1250,00	10000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
is4gen.2xlarge [1]	5000	10000	625,00	1250,00	20000	40000
is4gen.4xlarge [2]	10000		1250,0		40000	
is4gen.8xlarge [2]	20000		2500,0		80000	

[1] Diese Instances können mindestens einmal alle 24 Stunden für 30 Minuten die maximale Leistung erbringen, danach fallen sie auf ihre Basisleistung zurück.

[2] Diese Instances können ihre angegebene Leistung auf unbestimmte Zeit aufrechterhalten. Wenn Ihre Workload länger als 30 Minuten anhaltende maximale Leistung erfordert, verwenden Sie eine dieser Instances.

Beschleunigtes Computing

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
dl1.24xlarge [2]	19000		2375,0		80000	
dl2q.24xlarge [2]	19000		2375,0		80000	
f1.2xlarge [2]	1700		212,5		12000	
f1.4xlarge [2]	3500		437,5		44000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
f1.16xlarge [2]	14000		1750,0		75000	
f2.6 x groß 2	7500		937,5		30000	
f2.12xlarge [2]	15000		1875,0		60000	
f2.48xlarge [2]	60000		7500,0		240000	
g3.4xlarge [2]	3500		437,5		20000	
g3.8xlarge [2]	7000		875,0		40000	
g3.16xlarge [2]	14000		1750,0		80000	
g4ad.xlarge [1]	400	3170	50,00	396,25	1700	13333
g4ad.2xlarge [1]	800	3170	100,00	396,25	3400	13333
g4ad.4xlarge [1]	1580	3170	197,50	396,25	6700	13333
g4ad.8xlarge [2]	3170		396,25		13333	
g4ad.16xlarge [2]	6300		787,5		26667	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
g4dn.xlarge [1]	950	3500	118,75	437,50	3000	20000
g4dn.2xlarge [1]	1150	3500	143,75	437,50	6 000	20000
g4dn.4xlarge [2]	4750		593,75		20000	
g4dn.8xlarge [2]	9500		1187,5		40000	
g4dn.12xlarge [2]	9500		1187,5		40000	
g4dn.16xlarge [2]	9500		1187,5		40000	
g4dn.metal [2]	19000		2375,0		80000	
g5.xlarge [1]	700	3500	87,50	437,50	3000	15000
g5.2xlarge [1]	850	3500	106,25	437,50	3500	15000
g5.4xlarge [2]	4750		593,75		20000	
g5.8xlarge [2]	16000		2000,0		65000	
g5.12xlarge [2]	16000		2000,0		65000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
g5.16xlarge [2]	16000		2000,0		65000	
g5.24xlarge [2]	19000		2375,0		80000	
g5.48xlarge [2]	19000		2375,0		80000	
g5g.xlarge [1]	1188	4750	148,50	593,75	6 000	20000
g5g.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
g5g.4xlarge [2]	4750		593,75		20000	
g5g.8xlarge [2]	9500		1187,5		40000	
g5g.16xlarge [2]	19000		2375,0		80000	
g5g.metal [2]	19000		2375,0		80000	
g6.xlarge [1]	1000	5000	125,00	625,00	4000	20000
g6.2xlarge [1]	2000	5000	250,00	625,00	8000	20000
g6.4xlarge [2]	8000		1000,0		32000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
g6.8xlarge [2]	16000		2000,0		64000	
g6.12xlarge [2]	20000		2500,0		80000	
g6.16xlarge [2]	20000		2500,0		80000	
g6.24xlarge [2]	30000		3750,0		120000	
g6.48xlarge [2]	60000		7500,0		240000	
g6e.xlarge [1]	1000	5000	125,00	625,00	4000	20000
g6e.2xlarge [1]	2000	5000	250,00	625,00	8000	20000
g6e.4xlarge [2]	8000		1000,0		32000	
g6e.8xlarge [2]	16000		2000,0		64000	
g6e.12xlarge [2]	20000		2500,0		80000	
g6e.16xlarge [2]	20000		2500,0		80000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
g6e.24xlarge [2]	30000		3750,0		120000	
g6e.48xlarge [2]	60000		7500,0		240000	
g6f.large [1]	936	5000	117,00	625,00	3750	20000
g6f.xlarge [1]	1000	5000	125,00	625,00	4000	20000
g6f.2xlarge [1]	2000	5000	250,00	625,00	8000	20000
g6f.4xlarge [2]	6 000		750,0		24000	
gr6.4xlarge [2]	8000		1000,0		32000	
gr6.8xlarge [2]	16000		2000,0		64000	
gr6f.4xlarge [2]	8000		1000,0		32000	
inf1.xlarge [1]	1190	4750	148,75	593,75	4000	20000
inf1.2xlarge [1]	1190	4750	148,75	593,75	6 000	20000
inf1.6xlarge [2]	4750		593,75		20000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
inf1.24xlarge [2]	19000		2375,0		80000	
inf2.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
inf2.8xlarge [2]	10000		1250,0		40000	
inf2.24xlarge [2]	30000		3750,0		120000	
inf2.48xlarge [2]	60000		7500,0		240000	
p3.2xlarge [2]	1750		218,75		10000	
p3.8xlarge [2]	7000		875,0		40000	
p3.16xlarge [2]	14000		1750,0		80000	
p3dn.24xlarge [2]	19000		2375,0		80000	
p4d.24xlarge [2]	19000		2375,0		80000	
p4de.24xlarge [2]	19000		2375,0		80000	
p 5.4 x groß 2	10000		1250,0		32500	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
p5.48xlarge [2]	80000		10000,0		260000	
p5e.48xlarge [2]	80000		10000,0		260000	
p5en.48xlarge [2]	100000		12500,0		400000	
p6-b200.48xlarge [2]	100000		12500,0		400000	
p6-b300.48xlarge 2	100000		12500,0		400000	
p6e-gb200.36xlarge [2]	60000		7500,0		240000	
trn1.2xlarge [1]	5000	20000	625,00	2500,00	16250	65000
trn1.32xlarge [2]	80000		10000,0		260000	
trn1n.32xlarge [2]	80000		10000,0		260000	
trn2.48xlarge [2]	80000		10000,0		260000	
trn2u.48xlarge [2]	80000		10000,0		260000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
vt1.3xlarge [1]	2375	4750	296,88	593,75	10000	20000
vt1.6xlarge [2]	4750		593,75		20000	
vt1.24xlarge [2]	19000		2375,0		80000	

[1] Diese Instances können mindestens einmal alle 24 Stunden für 30 Minuten die maximale Leistung erbringen, danach fallen sie auf ihre Basisleistung zurück.

[2] Diese Instances können ihre angegebene Leistung auf unbestimmte Zeit aufrechterhalten. Wenn Ihre Workload länger als 30 Minuten anhaltende maximale Leistung erfordert, verwenden Sie eine dieser Instances.

Datenverarbeitung in Hochleistung

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
hpc6a.48xlarge [1]	87	2085	10,88	260,62	500	11000
hpc6id.32xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7a.12xlarge [1]	87	2085	10,88	260,62	500	11000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Ausgangsdurchsatz () MB/s, 128 KiB I/O	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
hpc7a.24xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7a.48xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7a.96xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7g.4xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7g.8xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7g.16xlarge [1]	87	2085	10,88	260,62	500	11000

[1] Diese Instances können mindestens einmal alle 24 Stunden für 30 Minuten die maximale Leistung erbringen, danach fallen sie auf ihre Basisleistung zurück.

[2] Diese Instances können ihre angegebene Leistung auf unbestimmte Zeit aufrechterhalten. Wenn Ihre Workload länger als 30 Minuten anhaltende maximale Leistung erfordert, verwenden Sie eine dieser Instances.

EBS-Optimierung unterstützt

Die folgenden Instance-Typen unterstützen die EBS-Optimierung, aber die EBS-Optimierung ist standardmäßig nicht aktiviert. Sie müssen die EBS-Optimierung während oder nach dem Start gegen eine zusätzliche Stundengebühr aktivieren, um die beschriebene EBS-Leistung zu erreichen.

Instance-Größe	Maximale Bandbreite (Mbit/s)	Maximaler Durchsatz () MB/s, 128 KiB I/O	Maximale IOPS-Anzahl (16 KiB I/O)
c1.xlarge	1000	125,0	8000
c3.xlarge	500	62,5	4000
c3.2xlarge	1000	125,0	8000
c3.4xlarge	2000	250,0	16000
i2.xlarge	500	62,5	4000
i2.2xlarge	1000	125,0	8000
i2.4xlarge	2000	250,0	16000
m1.large	500	62,5	4000
m1.xlarge	1000	125,0	8000
m2.2xlarge	500	62,5	4000
m2.4xlarge	1000	125,0	8000
m3.xlarge	500	62,5	4000
m3.2xlarge	1000	125,0	8000
r3.xlarge	500	62,5	4000
r3.2xlarge	1000	125,0	8000
r3.4xlarge	2000	250,0	16000

Note

Die Instances `i2.8xlarge`, `c3.8xlarge` und `r3.8xlarge` haben keine dedizierte EBS-Bandbreite und bieten daher keine EBS-Optimierung. In diesen Instances wird der

Netzwerkdatenverkehr zusammen mit dem Amazon EBS-Datenverkehr durch dieselbe 10-Gigabit-Netzwerkschnittstelle geleitet.

Die maximale Amazon EBS-optimierte Leistung erhalten

Die EBS-Leistung einer Instance wird durch die Leistungsgrenzen der Instance oder die aggregierte Leistung der angefügten Volumes begrenzt, je nachdem, welcher Wert kleiner ist. Um die maximale EBS-Leistung zu erreichen, muss eine Instance über angefügte Volumes verfügen, die zusammen eine Leistung bereitstellen, die der maximalen Leistung der Instance entspricht oder darüber liegt. Um beispielsweise `80,000` IOPS für `r6i.16xlarge` zu erreichen, müssen für die Instance mindestens `5` gp2-Volumes mit jeweils `16,000` IOPS bereitgestellt werden (`5` Volumes x `16,000` IOPS = `80,000` IOPS), oder es kann `1` gp3-Volume mit `80,000` IOPS bereitgestellt werden. Wir empfehlen Ihnen, einen Instance-Typ zu wählen, der mehr dedizierten Amazon EBS-Durchsatz bietet, als Ihre Anwendung benötigt. Andernfalls EC2 kann die Verbindung zwischen Amazon EBS und Amazon zu einem Leistungsengpass werden.

Important

Wenn Sie konfigurierbare Bandbreitengewichtungen verwenden, können sich die EBS-Bandbreitenlimits für Ihre Instance ändern. Bei Instances mit der Gewichtungskonfiguration `VPC-1`, die die Netzwerkbandbreite erhöht, kann es bei EBS-Volumes zu niedrigeren IOPS-Werten als erwartet kommen, da das EBS-Bandbreitenlimit vor dem IOPS-Limit erreicht wird. Dies macht sich besonders bei größeren Größen bemerkbar. I/O Testen Sie immer Ihren spezifischen Workload, um sicherzustellen, dass er Ihren Leistungsanforderungen mit der von Ihnen ausgewählten Bandbreitengewichtung entspricht. Weitere Informationen finden Sie unter EC2 Konfiguration der Gewichtung der Instanz-Bandbreite.

Mithilfe der Metriken `EBSIOBalance%` und `EBSByteBalance%` können Sie leichter ermitteln, ob Ihre Instances korrekt dimensioniert sind. Sie können diese Messwerte in der CloudWatch Konsole anzeigen und einen Alarm einrichten, der auf der Grundlage eines von Ihnen angegebenen Schwellenwerts ausgelöst wird. Diese Metriken werden als Prozentsatz angezeigt. Instances mit einem dauerhaft niedrigen Saldoprozentsatz sind Kandidaten für eine Vergrößerung. Instances, bei denen der Saldoprozentsatz nie unter 100 % fällt, sind Kandidaten für eine Verkleinerung. Weitere Informationen finden Sie unter Überwachen Sie Ihre Instances mit CloudWatch.

Die High Memory-Instances sind so konzipiert, dass große In-Memory-Datenbanken, einschließlich Produktionsbereitstellungen der SAP HANA-In-Memory-Datenbank in der Cloud, ausgeführt werden. Um die EBS-Leistung zu maximieren, verwenden Sie High Memory-Instances mit einer geraden Anzahl von `io1`- oder `io2`-Volumes mit identischer bereitgestellter Leistung. Verwenden Sie beispielsweise für hohe IOPS-Workloads vier `io1`- oder `io2`-Volumes mit 40 000 bereitgestellten IOPS, um die maximal 160 000 Instance-IOPS zu erhalten. In ähnlicher Weise sollten Sie bei Workloads mit hohem Durchsatz sechs `io1` oder `io2` Volumes mit 48.000 bereitgestellten IOPS verwenden, um den maximalen Durchsatz von 4.750 zu erzielen. MB/s Weitere Empfehlungen finden Sie unter Speicherkonfiguration für SAP HANA.

Überlegungen

- G4dn-, I3en-, Inf1-, M5a-, M5ad-, R5a-, R5ad-, T3-, T3a- und Z1d-Instances, welche nach dem 26. Februar 2020 gestartet wurden, bieten die maximale EBS-optimierte Leistung. Um die maximale Leistung einer Instance zu erhalten, die vor dem 26. Februar 2020 gestartet wurde, beenden und starten Sie sie.
- C5-, C5d-, C5n-, M5-, M5d-, M5n-, M5dn-, R5-, R5d-, R5n-, R5dn- und P3dn-Instances, die nach dem 3. Dezember 2019 gestartet wurden, bieten die maximale EBS-optimierte Leistung. Um die maximale Leistung einer Instance zu erhalten, die vor dem 3. Dezember 2019 gestartet wurde, beenden und starten Sie sie.
- Die Instances `u-6tb1.metal`, `u-9tb1.metal` und `u-12tb1.metal`, die nach dem 12. März 2020 gestartet wurden, bieten die maximale EBS-optimierte Leistung. Instances dieser Typen, die vor dem 12. März 2020 gestartet wurden, bieten möglicherweise eine geringere Leistung. Um die maximale Leistung einer Instance zu erhalten, die vor dem 12. März 2020 gestartet wurde, wenden Sie sich an Ihr Kontoteam, um die Instance ohne zusätzliche Kosten zu aktualisieren.

EC2 Finden Sie EBS-optimierte Instance-Typen

Sie können die Instance-Typen in jeder Region anzeigen, die EBS-Optimierung unterstützen.

Console

So suchen Sie Instance-Typen, die standardmäßig für EBS optimiert sind

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instance Types (Instance-Typen) aus.

3. Fügen Sie den Filter EBS-Optimierungsunterstützung = Standard hinzu.
4. (Optional) Wählen Sie das Symbol Einstellungen und aktivieren Sie dann die entsprechenden Spalten, z. B. EBS Maximum IOPS und EBS Baseline IOPS.
5. (Optional) Fügen Sie Filter hinzu, um den Anwendungsbereich auf bestimmte Instance-Typen von Interesse zu erweitern.

AWS CLI

So suchen Sie Instance-Typen, die standardmäßig für EBS optimiert sind

Verwenden Sie den folgenden describe-instance-types-Befehl.

```
aws ec2 describe-instance-types \
--filters Name=ebs-info.ebs-optimized-support,Values=default  \
--query 'InstanceTypes[].{InstanceType:InstanceType,
 "MaxBandwidth(Mb/s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,
 MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIops, "MaxThroughput(MB/
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--output=table
```

So suchen Sie Instance-Typen, die optional die EBS-Optimierung unterstützen

Verwenden Sie den folgenden describe-instance-types-Befehl.

```
aws ec2 describe-instance-types \
--filters Name=ebs-info.ebs-optimized-support,Values=supported \
--query 'InstanceTypes[].{InstanceType:InstanceType,
 "MaxBandwidth(Mb/s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,
 MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIops, "MaxThroughput(MB/
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--output=table
```

Es folgt eine Beispielausgabe für `eu-west-1`.

```
-------------------------------------------------------------------------
|                        DescribeInstanceTypes                          |
+--------------+----------------------+----------+----------------------+
| InstanceType | MaxBandwidth(Mb/s)   | MaxIOPS  |  MaxThroughput(MB/s)  |
+--------------+----------------------+----------+----------------------+
|  i2.2xlarge  |  1000                |  8000    |  125.0                |
|  m2.4xlarge  |  1000                |  8000    |  125.0                |
```

```
|  m2.2xlarge  |  500                 |  4000    |  62.5                 |
|  c1.xlarge   |  1000                |  8000    |  125.0                |
|  i2.xlarge   |  500                 |  4000    |  62.5                 |
|  m3.xlarge   |  500                 |  4000    |  62.5                 |
|  m1.xlarge   |  1000                |  8000    |  125.0                |
|  r3.4xlarge  |  2000                |  16000   |  250.0                |
|  r3.2xlarge  |  1000                |  8000    |  125.0                |
|  c3.xlarge   |  500                 |  4000    |  62.5                 |
|  m3.2xlarge  |  1000                |  8000    |  125.0                |
|  r3.xlarge   |  500                 |  4000    |  62.5                 |
|  i2.4xlarge  |  2000                |  16000   |  250.0                |
|  c3.4xlarge  |  2000                |  16000   |  250.0                |
|  c3.2xlarge  |  1000                |  8000    |  125.0                |
|  m1.large    |  500                 |  4000    |  62.5                 |
+--------------+----------------------+----------+-----------------------+
```

PowerShell

So suchen Sie Instance-Typen, die standardmäßig für EBS optimiert sind

Verwenden Sie das cmdlet Get-EC2InstanceType.

```
Get-EC2InstanceType `
    -Filter @{Name="ebs-info.ebs-optimized-support"; Values="default"} | `
    Select InstanceType, `
        @{Name="MaxBandwidth(Mb/s)";
 Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps)}}, `
        @{Name="MaxIOPS"; Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumIops)}}, `
        @{Name="MaxThroughput (MB/s)";
 Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps)}}
```

So suchen Sie Instance-Typen, die optional die EBS-Optimierung unterstützen

Verwenden Sie das cmdlet Get-EC2InstanceType.

```
Get-EC2InstanceType `
    -Filter @{Name="ebs-info.ebs-optimized-support"; Values="supported"} | `
    Select InstanceType, `
        @{Name="MaxBandwidth(Mb/s)";
 Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps)}}, `
        @{Name="MaxIOPS"; Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumIops)}}, `
        @{Name="MaxThroughput (MB/s)";
 Expression={($_.EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps)}}
```

Es folgt eine Beispielausgabe für `eu-west-1`.

```
InstanceType MaxBandwidth(Mb/s) MaxIOPS MaxThroughput (MB/s)
------------ ------------------ ------- --------------------
m2.4xlarge                 1000    8000              125.000
i2.2xlarge                 1000    8000              125.000
c1.xlarge                  1000    8000              125.000
m2.2xlarge                  500    4000               62.500
r3.2xlarge                 1000    8000              125.000
m3.xlarge                   500    4000               62.500
r3.4xlarge                 2000   16000              250.000
m1.xlarge                  1000    8000              125.000
i2.xlarge                   500    4000               62.500
c3.xlarge                   500    4000               62.500
c3.4xlarge                 2000   16000              250.000
c3.2xlarge                 1000    8000              125.000
i2.4xlarge                 2000   16000              250.000
r3.xlarge                   500    4000               62.500
m3.2xlarge                 1000    8000              125.000
m1.large                    500    4000               62.500
```

EBS-Optimierung für eine EC2 Amazon-Instance aktivieren

Sie können die EBS-Optimierung nur für Instance-Typen der vorherigen Generation manuell aktivieren, die optional die EBS-Optimierung unterstützen. Wenn Sie die EBS-Optimierung für diese Instance-Typen aktivieren, fällt eine zusätzliche Stundengebühr an.

Voraussetzungen

- Stellen Sie sicher, dass der Instance-Typ erfordert, dass Sie die EBS-Optimierung aktivieren. Weitere Informationen finden Sie unter EBS-Optimierung unterstützt.
- Um die EBS-Optimierung nach dem Start zu aktivieren, müssen Sie die Instance anhalten.

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

Console

So aktivieren Sie die Amazon-EBS-Optimierung während des Starts

Wählen Sie im Launch Instance Wizard den erforderlichen Instance-Typ aus. Erweitern Sie den Abschnitt Erweiterte Details und wählen Sie dann für EBS-optimierte Instance die Option Aktivieren aus.

Wenn der ausgewählte Instance-Typ die Amazon-EBS-Optimierung nicht unterstützt, ist das Drop-down-Menü deaktiviert. Wenn der Instance-Typ standardmäßig Amazon-EBS-optimiert ist, ist „Aktivieren“ bereits ausgewählt.

So aktivieren Sie die Amazon EBS-Optimierung nach dem Start

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie die Instance aus.
3. Halten Sie die Instance an. Wählen Sie Aktionen, Instance-Status, Instance anhalten aus.
4. Während die Instance noch ausgewählt ist, wählen Sie Aktionen, Instance-Einstellungen, Instance-Typ ändern aus.
5. Wählen Sie EBS-Optimized und dann Anwenden aus.

   Wenn der Instance-Typ standardmäßig Amazon-EBS-optimiert ist oder die Option Amazon-EBS-Optimierung nicht unterstützt, ist das Kontrollkästchen deaktiviert.
6. Starten Sie die Instance neu. Wählen Sie Instance state (Instance-Status), Start instance (Instance starten).

AWS CLI

So aktivieren Sie die Amazon-EBS-Optimierung während des Starts

Verwenden den Befehl run-instances mit der Option `--ebs-optimized`.

So aktivieren Sie die Amazon EBS-Optimierung nach dem Start

1. Wenn die Instance ausgeführt wird, verwenden Sie den Befehl stop-instances, um sie anzuhalten.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

2. Aktivieren Sie die EBS-Optimierung, indem Sie den modify-instance-attributeBefehl mit der `--ebs-optimized` Option verwenden.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --ebs-optimized
```

PowerShell

So aktivieren Sie die Amazon-EBS-Optimierung während des Starts

Verwenden Sie das New-EC2InstanceCmdlet mit der Option. `-EbsOptimized`

So aktivieren Sie die Amazon EBS-Optimierung nach dem Start

1. Wenn die Instanz ausgeführt wird, beenden Sie sie mit dem Stop-EC2InstanceCmdlet.

```
Stop-EC2Instance -InstanceId i-1234567890abcdef0
```

2. Aktivieren Sie die EBS-Optimierung, indem Sie das Edit-EC2InstanceAttributeCmdlet mit der Option verwenden. `-EbsOptimized`

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -EbsOptimized $true
```

CPU-Optionen für EC2 Amazon-Instances

Viele EC2 Amazon-Instances unterstützen Simultaneous Multithreading (SMT), wodurch mehrere Threads gleichzeitig auf einem einzigen CPU-Kern ausgeführt werden können. Jeder Thread wird als virtuelle CPU (vCPU) auf der Instance dargestellt. Eine Instance hat eine Standardanzahl von CPU-Kernen, die je nach Instance-Typ variiert. Beispielsweise hat ein `m5.xlarge` Instance-Typ standardmäßig zwei CPU-Kerne und zwei Threads pro Kern — insgesamt also vier V. CPUs

In den meisten Fällen gibt es einen EC2 Amazon-Instance-Typ mit einer Kombination aus Arbeitsspeicher und Anzahl von vCPUs , die Ihren Workloads entspricht. Sie können jedoch die folgenden CPU-Optionen während und nach dem Start der Instance angeben, um Ihre Instance für bestimmte Workloads oder Geschäftsanforderungen zu optimieren:

- Anzahl der CPU-Kerne: Sie können die Anzahl der CPU-Kerne für die Instance anpassen. Sie könnten dies tun, um die Lizenzkosten Ihrer Software mit einer Instance zu optimieren, die genügend RAM für speicherintensive Workloads, aber weniger CPU-Kerne hat.
- Threads pro Kern: Sie können SMT deaktivieren, indem Sie einen einzelnen Thread pro CPU-Kern angeben. Sie können dies für bestimmte Workloads tun, z. B. für High Performance Computing (HPC)-Workloads.

Überlegungen

- Sie können die Anzahl der Threads pro Kern für T2-, C7a-, M7a-, R7a- und Apple Silicon Mac-Instances sowie für Instances, die auf dem Graviton-Prozessor basieren, nicht ändern. AWS
- Die Anzahl der Instances, die Sie ausführen können, basiert auf dem Standard v CPUs für die verwendeten Instance-Typen. Die Art und Weise, wie wir das von einer Instance CPUs verbrauchte v berechnen, wird durch eine Änderung der CPU-Optionen nicht beeinflusst.

Preisgestaltung

Es gibt keine zusätzlichen Kosten für die Angabe von CPU-Optionen. Für EC2 Instances, die von Windows und SQL Server aus gestartet werden, die in der Lizenz enthalten sind AMIs, können Sie die CPU-Optionen anpassen, um mithilfe der EC2 CPUs Optimize-Funktion Lizenzgebühren zu zahlen, die auf der Anzahl von v basierenCPUs , die für Ihre Instanz konfiguriert sind. Für andere EC2 Instances werden Ihnen die gleichen Gebühren berechnet wie für Instances, die mit den Standard-CPU-Optionen gestartet wurden.

Inhalt

- Regeln für die Angabe von CPU-Optionen für eine EC2 Amazon-Instance
- Unterstützte CPU-Optionen für EC2 Amazon-Instance-Typen
- CPU-Optionen für eine EC2 Amazon-Instance angeben
- CPU-Threads und Kerne für eine EC2 Amazon-Instance anzeigen
- Optimieren Sie CPUs für Instances, die in der Lizenz enthalten sind

Regeln für die Angabe von CPU-Optionen für eine EC2 Amazon-Instance

Um die CPU-Optionen für Ihre Instance festzulegen, beachten Sie die folgenden Regeln:

- Für Bare-Metal-Instances können Sie keine CPU-Optionen angeben.

- Sie können CPU-Optionen sowohl beim Start der Instance angeben, als auch danach.
- Um CPU-Optionen anzugeben, müssen Sie sowohl die Anzahl der CPU-Kerne als auch Threads pro Kern in der Anforderung angeben. Beispielanforderungen finden Sie unter CPU-Optionen für eine EC2 Amazon-Instance angeben.
- Die Anzahl von v CPUs für die Instance ist die Anzahl der CPU-Kerne multipliziert mit den Threads pro Kern. Um eine benutzerdefinierte Anzahl von v anzugebenCPUs, müssen Sie eine gültige Anzahl von CPU-Kernen und Threads pro Kern für den Instance-Typ angeben. Sie können die Standardanzahl von v CPUs für die Instanz nicht überschreiten. Weitere Informationen finden Sie unter Unterstützte CPU-Optionen für EC2 Amazon-Instance-Typen.
- Um Simultaneous Multithreading (SMT), auch Hyperthreading genannt, zu deaktivieren, geben Sie einen Thread pro Kern an.
- Wenn Sie in der Konsole den Instance-Typ einer vorhandenen Instance ändern, EC2 wendet Amazon nach Möglichkeit die CPU-Optionseinstellungen der vorhandenen Instance auf die neue Instance an. Wenn der neue Instance-Typ diese Einstellungen nicht unterstützt, werden die CPU-Optionen auf Standard-CPU-Optionen verwenden zurückgesetzt. Diese Option verwendet die Standardzahl v CPUs für den neuen Instance-Typ.

  Um die Einstellungen für die neue Instance zu aktualisieren, wählen Sie in der Ansicht Instance-Typ ändern unter Erweiterte Details die Option CPU-Optionen angeben aus.
- Die CPU-Optionen, die Sie angeben, bleiben nach dem Stoppen, Starten oder Neustarten einer Instance erhalten.
- Wenn Sie Reserved Instances verwenden, werden Rabatte möglicherweise nicht gewährt, wenn Sie Optimize CPUs für Instances konfigurieren, die über Windows mit einer Lizenz gestartet wurden, und zwar AMIs auf demselben Zahlerkonto. Wir empfehlen Ihnen, Savings Plans zu verwenden, um die vCPU-basierten Lizenzkosten zu senken und vergleichbare Einsparungen bei Ihren Rechenkosten zu erzielen.
- Um Lizenzkosten für Instances zu sparen, die über Windows gestartet werden, und die SQL Server-Lizenz enthalten AMIs, müssen Sie mindestens vier v konfigurieren. CPUs Wenn Sie weniger als vier V konfigurierenCPUs, wird die Standardabrechnung angewendet.
- CPUs Für Instances mit eingeschlossener Lizenz optimieren wird auf T3-Instance-Typen nicht unterstützt.

Unterstützte CPU-Optionen für EC2 Amazon-Instance-Typen

Die folgenden Tabellen listen die Instance-Typen auf, die die Angabe von CPU-Optionen unterstützen.

Inhalt

- Instances für allgemeine Zwecke
- Für Datenverarbeitung optimierte Instances
- RAM-optimierte Instances
- Speicheroptimierte Instances
- Beschleunigte Computing-Instances
- Instances für Datenverarbeitung in Hochleistung

Instances für allgemeine Zwecke

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m2.xlarge	2	2	1	1, 2	1
m2.2xlarge	4	4	1	1, 2, 3, 4	1
m2.4xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m3.large	2	1	2	1	1, 2
m3.xlarge	4	2	2	1, 2	1, 2
m3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.large	2	1	2	1	1, 2
m4.xlarge	4	2	2	1, 2	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m4.10xlarge	40	20	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20	1, 2
m4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5.large	2	1	2	1	1, 2
m5.xlarge	4	2	2	2	1, 2
m5.2xlarge	8	4	2	2, 4	1, 2
m5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5a.large	2	1	2	1	1, 2
m5a.xlarge	4	2	2	2	1, 2
m5a.2xlarge	8	4	2	2, 4	1, 2
m5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5ad.large	2	1	2	1	1, 2
m5ad.xlarge	4	2	2	2	1, 2
m5ad.2xlarge	8	4	2	2, 4	1, 2
m5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5d.large	2	1	2	1	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m5d.xlarge	4	2	2	2	1, 2
m5d.2xlarge	8	4	2	2, 4	1, 2
m5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5dn.large	2	1	2	1	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m5dn.xlarge	4	2	2	1, 2	1, 2
m5dn.2xlarge	8	4	2	2, 4	1, 2
m5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5n.large	2	1	2	1	1, 2
m5n.xlarge	4	2	2	1, 2	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m5n.2xlarge	8	4	2	2, 4	1, 2
m5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5zn.large	2	1	2	1	1, 2
m5zn.xlarge	4	2	2	1, 2	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m5zn.2xlarge	8	4	2	2, 4	1, 2
m5zn.3xlarge	12	6	2	2, 4, 6	1, 2
m5zn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
m5zn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6a.large	2	1	2	1	1, 2
m6a.xlarge	4	2	2	1, 2	1, 2
m6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
m6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
m6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
m6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
m6g.large	2	2	1	1, 2	1
m6g.xlarge	4	4	1	1, 2, 3, 4	1
m6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6gd.large	2	2	1	1, 2	1
m6gd.xlarge	4	4	1	1, 2, 3, 4	1
m6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6i.large	2	1	2	1	1, 2
m6i.xlarge	4	2	2	1, 2	1, 2
m6i.2xlarge	8	4	2	2, 4	1, 2
m6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6id.large	2	1	2	1	1, 2
m6id.xlarge	4	2	2	1, 2	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6id.2xlarge	8	4	2	2, 4	1, 2
m6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6idn.large	2	1	2	1	1, 2
m6idn.xlarge	4	2	2	1, 2	1, 2
m6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6in.large	2	1	2	1	1, 2
m6in.xlarge	4	2	2	1, 2	1, 2
m6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m7a.large	2	2	1	1, 2	1
m7a.xlarge	4	4	1	1, 2, 3, 4	1
m7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
m7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
m7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
m7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
m7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
m7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
m7g.large	2	2	1	1, 2	1
m7g.xlarge	4	4	1	1, 2, 3, 4	1
m7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7gd.large	2	2	1	1, 2	1
m7gd.xlarge	4	4	1	1, 2, 3, 4	1
m7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7i.large	2	1	2	1	1, 2
m7i.xlarge	4	2	2	1, 2	1, 2
m7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
m7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m7i-flex.large	2	1	2	1	1, 2
m7i-flex.xlarge	4	2	2	1, 2	1, 2
m7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m7i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m7i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m8a.medium	1	1	1	1	1
m8a.large	2	2	1	1, 2	1
m8a.xlarge	4	4	1	1, 2, 3, 4	1
m8a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
m8a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
m8a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
m8a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
m8a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m8a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
m8g.large	2	2	1	1, 2	1
m8g.xlarge	4	4	1	1, 2, 3, 4	1
m8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
m8gd.large	2	2	1	1, 2	1
m8gd.xlarge	4	4	1	1, 2, 3, 4	1
m8gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m8gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m8gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m8gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m8gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m8gd.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m8gd.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
m8i.large	2	1	2	1	1, 2
m8i.xlarge	4	2	2	1, 2	1, 2
m8i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m8i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m8i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m8i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m8i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m8i.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m8i.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m8i.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2
m8i.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
m8i-flex.large	2	1	2	1	1, 2
m8i-flex.xlarge	4	2	2	1, 2	1, 2
m8i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m8i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m8i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m8i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m8i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
t3.nano	2	1	2	1	1, 2
t3.micro	2	1	2	1	1, 2
t3.small	2	1	2	1	1, 2
t3.medium	2	1	2	1	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
t3.large	2	1	2	1	1, 2
t3.xlarge	4	2	2	2	1, 2
t3.2xlarge	8	4	2	2, 4	1, 2
t3a.nano	2	1	2	1	1, 2
t3a.micro	2	1	2	1	1, 2
t3a.small	2	1	2	1	1, 2
t3a.medium	2	1	2	1	1, 2
t3a.large	2	1	2	1	1, 2
t3a.xlarge	4	2	2	2	1, 2
t3a.2xlarge	8	4	2	2, 4	1, 2
t4g.nano	2	2	1	1, 2	1
t4g.micro	2	2	1	1, 2	1
t4g.small	2	2	1	1, 2	1
t4g.medium	2	2	1	1, 2	1
t4g.large	2	2	1	1, 2	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
t4g.xlarge	4	4	1	1, 2, 3, 4	1
t4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Für Datenverarbeitung optimierte Instances

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c3.large	2	1	2	1	1, 2
c3.xlarge	4	2	2	1, 2	1, 2
c3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c4.large	2	1	2	1	1, 2
c4.xlarge	4	2	2	1, 2	1, 2
c4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c4.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.large	2	1	2	1	1, 2
c5.xlarge	4	2	2	2	1, 2
c5.2xlarge	8	4	2	2, 4	1, 2
c5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c5.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5a.large	2	1	2	1	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c5a.xlarge	4	2	2	1, 2	1, 2
c5a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5a.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2
c5a.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5a.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2
c5a.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5a.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5ad.large	2	1	2	1	1, 2
c5ad.xlarge	4	2	2	1, 2	1, 2
c5ad.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5ad.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c5ad.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5ad.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2
c5ad.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5ad.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5d.large	2	1	2	1	1, 2
c5d.xlarge	4	2	2	2	1, 2
c5d.2xlarge	8	4	2	2, 4	1, 2
c5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5d.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c5d.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c5d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5n.large	2	1	2	1	1, 2
c5n.xlarge	4	2	2	2	1, 2
c5n.2xlarge	8	4	2	2, 4	1, 2
c5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5n.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5n.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6a.large	2	1	2	1	1, 2
c6a.xlarge	4	2	2	1, 2	1, 2
c6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
c6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
c6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
c6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
c6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
c6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
c6g.large	2	2	1	1, 2	1
c6g.xlarge	4	4	1	1, 2, 3, 4	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gd.large	2	2	1	1, 2	1
c6gd.xlarge	4	4	1	1, 2, 3, 4	1
c6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gn.medium	1	1	1	1	1
c6gn.large	2	2	1	1, 2	1
c6gn.xlarge	4	4	1	1, 2, 3, 4	1
c6gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6i.large	2	1	2	1	1, 2
c6i.xlarge	4	2	2	1, 2	1, 2
c6i.2xlarge	8	4	2	2, 4	1, 2
c6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6id.large	2	1	2	1	1, 2
c6id.xlarge	4	2	2	1, 2	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6id.2xlarge	8	4	2	2, 4	1, 2
c6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6in.large	2	1	2	1	1, 2
c6in.xlarge	4	2	2	1, 2	1, 2
c6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c7a.large	2	2	1	1, 2	1
c7a.xlarge	4	4	1	1, 2, 3, 4	1
c7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
c7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
c7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
c7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
c7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
c7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
c7g.large	2	2	1	1, 2	1
c7g.xlarge	4	4	1	1, 2, 3, 4	1
c7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gd.large	2	2	1	1, 2	1
c7gd.xlarge	4	4	1	1, 2, 3, 4	1
c7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gn.large	2	2	1	1, 2	1
c7gn.xlarge	4	4	1	1, 2, 3, 4	1
c7gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7i.large	2	1	2	1	1, 2
c7i.xlarge	4	2	2	1, 2	1, 2
c7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
c7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7i-flex.large	2	1	2	1	1, 2
c7i-flex.xlarge	4	2	2	1, 2	1, 2
c7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c7i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c7i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8a.medium	1	1	1	1	1
c8a.large	2	2	1	1, 2	1
c8a.xlarge	4	4	1	1, 2, 3, 4	1
c8a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
c8a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
c8a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
c8a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
c8a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
c8g.large	2	2	1	1, 2	1
c8g.xlarge	4	4	1	1, 2, 3, 4	1
c8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
c8gb.large	2	2	1	1, 2	1
c8gb.xlarge	4	4	1	1, 2, 3, 4	1
c8gb.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8gb.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c8gb.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8gb.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8gb.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8gb.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8gd.large	2	2	1	1, 2	1
c8gd.xlarge	4	4	1	1, 2, 3, 4	1
c8gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c8gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8gd.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8gd.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
c8gn.large	2	2	1	1, 2	1
c8gn.xlarge	4	4	1	1, 2, 3, 4	1
c8gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c8gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c8gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8gn.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8gn.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
c8i.large	2	1	2	1	1, 2
c8i.xlarge	4	2	2	1, 2	1, 2
c8i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c8i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c8i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c8i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c8i.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c8i.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8i.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2
c8i.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
c8i-flex.large	2	1	2	1	1, 2
c8i-flex.xlarge	4	2	2	1, 2	1, 2
c8i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c8i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c8i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c8i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c8i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

RAM-optimierte Instances

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r3.large	2	1	2	1	1, 2
r3.xlarge	4	2	2	1, 2	1, 2
r3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r4.large	2	1	2	1	1, 2
r4.xlarge	4	2	2	1, 2	1, 2
r4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r4.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r5.large	2	1	2	1	1, 2
r5.xlarge	4	2	2	2	1, 2
r5.2xlarge	8	4	2	2, 4	1, 2
r5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5a.large	2	1	2	1	1, 2
r5a.xlarge	4	2	2	2	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r5a.2xlarge	8	4	2	2, 4	1, 2
r5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5ad.large	2	1	2	1	1, 2
r5ad.xlarge	4	2	2	2	1, 2
r5ad.2xlarge	8	4	2	2, 4	1, 2
r5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5b.large	2	1	2	1	1, 2
r5b.xlarge	4	2	2	1, 2	1, 2
r5b.2xlarge	8	4	2	2, 4	1, 2
r5b.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5b.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5b.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5b.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r5b.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5d.large	2	1	2	1	1, 2
r5d.xlarge	4	2	2	2	1, 2
r5d.2xlarge	8	4	2	2, 4	1, 2
r5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5dn.large	2	1	2	1	1, 2
r5dn.xlarge	4	2	2	1, 2	1, 2
r5dn.2xlarge	8	4	2	2, 4	1, 2
r5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5n.large	2	1	2	1	1, 2
r5n.xlarge	4	2	2	1, 2	1, 2
r5n.2xlarge	8	4	2	2, 4	1, 2
r5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6a.large	2	1	2	1	1, 2
r6a.xlarge	4	2	2	1, 2	1, 2
r6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
r6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
r6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
r6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
r6g.large	2	2	1	1, 2	1
r6g.xlarge	4	4	1	1, 2, 3, 4	1
r6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6gd.large	2	2	1	1, 2	1
r6gd.xlarge	4	4	1	1, 2, 3, 4	1
r6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6i.large	2	1	2	1	1, 2
r6i.xlarge	4	2	2	1, 2	1, 2
r6i.2xlarge	8	4	2	2, 4	1, 2
r6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6id.large	2	1	2	1	1, 2
r6id.xlarge	4	2	2	1, 2	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6id.2xlarge	8	4	2	2, 4	1, 2
r6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6idn.large	2	1	2	1	1, 2
r6idn.xlarge	4	2	2	1, 2	1, 2
r6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6in.large	2	1	2	1	1, 2
r6in.xlarge	4	2	2	1, 2	1, 2
r6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r7a.large	2	2	1	1, 2	1
r7a.xlarge	4	4	1	1, 2, 3, 4	1
r7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
r7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
r7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
r7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
r7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
r7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
r7g.large	2	2	1	1, 2	1
r7g.xlarge	4	4	1	1, 2, 3, 4	1
r7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7gd.large	2	2	1	1, 2	1
r7gd.xlarge	4	4	1	1, 2, 3, 4	1
r7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7i.large	2	1	2	1	1, 2
r7i.xlarge	4	2	2	1, 2	1, 2
r7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
r7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7iz.large	2	1	2	1	1, 2
r7iz.xlarge	4	2	2	1, 2	1, 2
r7iz.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7iz.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r7iz.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7iz.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7iz.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7iz.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r8a.medium	1	1	1	1	1
r8a.large	2	2	1	1, 2	1
r8a.xlarge	4	4	1	1, 2, 3, 4	1
r8a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
r8a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
r8a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
r8a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
r8a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
r8g.large	2	2	1	1, 2	1
r8g.xlarge	4	4	1	1, 2, 3, 4	1
r8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
r8gb.large	2	2	1	1, 2	1
r8gb.xlarge	4	4	1	1, 2, 3, 4	1
r8gb.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8gb.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r8gb.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8gb.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8gb.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8gb.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8gd.large	2	2	1	1, 2	1
r8gd.xlarge	4	4	1	1, 2, 3, 4	1
r8gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r8gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8gd.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8gd.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
r8gn.large	2	2	1	1, 2	1
r8gn.xlarge	4	4	1	1, 2, 3, 4	1
r8gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r8gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r8gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8gn.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8gn.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
r8i.large	2	1	2	1	1, 2
r8i.xlarge	4	2	2	1, 2	1, 2
r8i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r8i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r8i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r8i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r8i.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r8i.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8i.48xlarge	192	96	2	6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96	1, 2
r8i.96xlarge	384	192	2	12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102, 108, 114, 120, 126, 132, 138, 144, 150, 156, 162, 168, 174, 180, 186, 192	1, 2
r8i-flex.large	2	1	2	1	1, 2
r8i-flex.xlarge	4	2	2	1, 2	1, 2
r8i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r8i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r8i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r8i-flex.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r8i-flex.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
u-3tb1.56xlarge	224	112	2	8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112	1, 2
u-6tb1.56xlarge	224	224	1	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1
u-6tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
u-9tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-12tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
u-18tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-24tb1.112xlarge	448	224	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
u7i-6tb.112xlarge	448	224	2	8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 148, 152, 156, 160, 164, 168, 172, 176, 180, 184, 188, 192, 196, 200, 204, 208, 212, 216, 220, 224	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
u7i-8tb.112xlarge	448	224	2	8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 148, 152, 156, 160, 164, 168, 172, 176, 180, 184, 188, 192, 196, 200, 204, 208, 212, 216, 220, 224	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
u7i-12tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
u7in-16tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
u7in-24tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
u7in-32tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
u7inh-32tb.480xlarge	1920	960	2	32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240, 256, 272, 288, 304, 320, 336, 352, 368, 384, 400, 416, 432, 448, 464, 480, 496, 512, 528, 544, 560, 576, 592, 608, 624, 640, 656, 672, 688, 704, 720, 736, 752, 768, 784, 800, 816, 832, 848, 864, 880, 896, 912, 928, 944, 960	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
x1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x1.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
x1e.xlarge	4	2	2	1, 2	1, 2
x1e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
x1e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
x1e.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
x1e.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
x1e.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
x2gd.large	2	2	1	1, 2	1
x2gd.xlarge	4	4	1	1, 2, 3, 4	1
x2gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
x2gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
x2gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
x2gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
x2gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
x2idn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
x2idn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2idn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iedn.xlarge	4	2	2	1, 2	1, 2
x2iedn.2xlarge	8	4	2	2, 4	1, 2
x2iedn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iedn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
x2iedn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x2iedn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2iedn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iezn.2xlarge	8	4	2	2, 4	1, 2
x2iezn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iezn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
x2iezn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
x2iezn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
x8g.large	2	2	1	1, 2	1
x8g.xlarge	4	4	1	1, 2, 3, 4	1
x8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
x8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
x8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
x8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
x8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
x8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
x8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
x8aedz.large	2	2	1	1, 2	1
x8aedz.xlarge	4	4	1	1, 2, 3, 4	1
x8aedz.3xlarge	12	12	1	1, 2, 4, 6, 8, 10, 12	1
x8aedz.6xlarge	24	24	1	1, 2, 3, 4, 8, 12, 16, 20, 24	1
x8aedz.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48	1
x8aedz.24xlarge	96	96	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96	1
z1d.large	2	1	2	1	1, 2
z1d.xlarge	4	2	2	1, 2	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
z1d.2xlarge	8	4	2	2, 4	1, 2
z1d.3xlarge	12	6	2	2, 4, 6	1, 2
z1d.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
z1d.12xlarge	48	24	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Speicheroptimierte Instances

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
d2.xlarge	4	2	2	1, 2	1, 2
d2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
d2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
d2.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
d3.xlarge	4	2	2	1, 2	1, 2
d3.2xlarge	8	4	2	2, 4	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
d3.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.xlarge	4	2	2	1, 2	1, 2
d3en.2xlarge	8	4	2	2, 4	1, 2
d3en.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
d3en.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
h1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
h1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
h1.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
h1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i2.xlarge	4	2	2	1, 2	1, 2
i2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i2.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
i3.large	2	1	2	1	1, 2
i3.xlarge	4	2	2	1, 2	1, 2
i3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i3en.large	2	1	2	1	1, 2
i3en.xlarge	4	2	2	1, 2	1, 2
i3en.2xlarge	8	4	2	2, 4	1, 2
i3en.3xlarge	12	6	2	2, 4, 6	1, 2
i3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
i3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
i3en.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
i4g.large	2	2	1	1, 2	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i4g.xlarge	4	4	1	1, 2, 3, 4	1
i4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i4g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
i4g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i4g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
i4i.large	2	1	2	1	1, 2
i4i.xlarge	4	2	2	1, 2	1, 2
i4i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i4i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i4i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i4i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
i4i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i4i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i4i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
i7i.large	2	1	2	1	1, 2
i7i.xlarge	4	2	2	1, 2	1, 2
i7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
i7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
i7ie.large	2	1	2	1	1, 2
i7ie.xlarge	4	2	2	1, 2	1, 2
i7ie.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i7ie.3xlarge	12	6	2	1, 2, 3, 4, 5, 6	1, 2
i7ie.6xlarge	24	12	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i7ie.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
i7ie.18xlarge	72	36	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i7ie.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
i7ie.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
i8g.large	2	2	1	1, 2	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i8g.xlarge	4	4	1	1, 2, 3, 4	1
i8g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i8g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
i8g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i8g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i8g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i8g.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i8g.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
i8ge.large	2	2	1	1, 2	1
i8ge.xlarge	4	4	1	1, 2, 3, 4	1
i8ge.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i8ge.3xlarge	12	12	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12	1
i8ge.6xlarge	24	24	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i8ge.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i8ge.18xlarge	72	72	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i8ge.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i8ge.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164,	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
				166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192	
im4gn.large	2	2	1	1, 2	1
im4gn.xlarge	4	4	1	1, 2, 3, 4	1
im4gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
im4gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
im4gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
im4gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
is4gen.medium	1	1	1	1	1
is4gen.large	2	2	1	1, 2	1
is4gen.xlarge	4	4	1	1, 2, 3, 4	1
is4gen.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
is4gen.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
is4gen.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Beschleunigte Computing-Instances

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
dl1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
dl2q.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28,	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
				30, 32, 34, 36, 38, 40, 42, 44, 46, 48	
f1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
f1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
f1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
f2.6xlarge	24	12	2	1, 2, 3, 6, 9, 12	1, 2
f2.12xlarge	48	24	2	1, 2, 3, 6, 9, 12, 15, 18, 21, 24	1, 2
f2.48xlarge	192	96	2	4, 6, 8, 10, 12, 24, 36, 48, 60, 72, 84, 96	1, 2
g3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
g3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g4ad.xlarge	4	2	2	2	1, 2
g4ad.2xlarge	8	4	2	2, 4	1, 2
g4ad.4xlarge	16	8	2	2, 4, 8	1, 2
g4ad.8xlarge	32	16	2	2, 4, 8, 16	1, 2
g4ad.16xlarge	64	32	2	2, 4, 8, 16, 32	1, 2
g4dn.xlarge	4	2	2	2	1, 2
g4dn.2xlarge	8	4	2	2, 4	1, 2
g4dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
g4dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
g4dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
g4dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g5g.xlarge	4	4	1	1, 2, 3, 4	1
g5g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
g5g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
g5g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
g5g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
g6.xlarge	4	2	2	1, 2	1, 2
g6.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
g6.12xlarge	48	24	2	1, 2, 3, 6, 9, 12, 15, 18, 21, 24	1, 2
g6.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
g6.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1, 2
g6.48xlarge	192	96	2	4, 6, 8, 10, 12, 24, 36, 48, 60, 72, 84, 96	1, 2
g6e.xlarge	4	2	2	1, 2	1, 2
g6e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g6e.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
g6e.12xlarge	48	24	2	3, 6, 9, 12, 15, 18, 21, 24	1, 2
g6e.16xlarge	64	32	2	4, 8, 12, 16, 20, 24, 28, 32	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
g6e.24xlarge	96	48	2	6, 12, 18, 24, 30, 36, 42, 48	1, 2
g6e.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2
g6f.large	2	1	2	1	1, 2
g6f.xlarge	4	2	2	1, 2	1, 2
g6f.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6f.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
gr6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
gr6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2
gr6f.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
inf1.xlarge	4	2	2	2	1, 2
inf1.2xlarge	8	4	2	2, 4	1, 2
inf1.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
inf1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
inf2.xlarge	4	2	2	1, 2	1, 2
inf2.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
inf2.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
inf2.48xlarge	192	96	2	4, 8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
p3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
p3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
p3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
p3dn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p4d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p4de.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p5.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
p5.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2
p5e.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2
p5en.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
p6-b200.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
p6-b300.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
p6e-gb200.36xlarge	144	144	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100,	1

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
				101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144	
`trn1.2xlarge`	8	4	2	2, 4	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
trn1.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
trn1n.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
trn2.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2
trn2u.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
vt1.3xlarge	12	6	2	6	1, 2
vt1.6xlarge	24	12	2	6, 12	1, 2
vt1.24xlarge	96	48	2	6, 12, 48	1, 2

Instances für Datenverarbeitung in Hochleistung

Instance-Typ	Standard v CPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
hpc6id.32xlarge	64	64	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1

CPU-Optionen für eine EC2 Amazon-Instance angeben

Sie können CPU-Optionen sowohl beim Start der Instance angeben, als auch danach.

Aufgaben

- Gleichzeitiges Multithreading deaktivieren

- Geben Sie CPUs beim Start eine benutzerdefinierte Zahl von v an
- Geben Sie eine benutzerdefinierte Anzahl von v CPUs in einer Startvorlage an
- Ändern Sie die CPU-Optionen für Ihre EC2 Instance

Gleichzeitiges Multithreading deaktivieren

Um Simultanes Multithreading (SMT), auch Hyperthreading genannt, zu deaktivieren, geben Sie 1 Thread pro Kern an.

Console

SMT während des Instance-Starts deaktivieren

1. Befolgen Sie das EC2-Instance mit dem Launch Instance Wizard in der Konsole starten-Verfahren und konfigurieren Sie Ihre Instance nach Bedarf.
2. Erweitern Sie Erweiterte Details und aktivieren Sie das Kontrollkästchen CPU-Optionen festlegen.
3. Wählen Sie für Core count (Anzahl Kerne) die Anzahl der benötigten CPU-Kerne aus. Um in diesem Beispiel die Standard-CPU-Kernanzahl für einer`5.4xlarge`-Instance festzulegen, wählen Sie 8 aus.
4. Um Multithreading für Threads pro Kern zu deaktivieren, wählen Sie 1.
5. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten.

AWS CLI

SMT während des Instance-Starts deaktivieren

Verwenden Sie den AWS CLI Befehl run-instances und geben Sie für den Parameter den Wert 1 for `ThreadsPerCore` an. `--cpu-options` Geben Sie für `CoreCount` die Anzahl der CPU-Kerne an. Um in diesem Beispiel die standardmäßige CPU-Kernanzahl für eine `r7i.4xlarge`-Instance festzulegen, geben Sie den Wert 8 an.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type r7i.4xlarge \
    --cpu-options "CoreCount=8,ThreadsPerCore=1" \
```

```
    --key-name my-key-pair
```

PowerShell

SMT während des Instance-Starts deaktivieren

Verwenden Sie den New-EC2InstanceBefehl und geben Sie für den Parameter den Wert 1 `ThreadsPerCore` for an`-CpuOptions`. Geben Sie für `CoreCount` die Anzahl der CPU-Kerne an. Um in diesem Beispiel die standardmäßige CPU-Kernanzahl für eine `r7i.4xlarge`-Instance festzulegen, geben Sie den Wert 8 an.

```
New-EC2Instance `
    -ImageId 'ami-0abcdef1234567890' `
    -InstanceType 'r7i.4xlarge' `
    -CpuOptions @{CoreCount=8; ThreadsPerCore=1} `
    -KeyName 'my-key-pair'
```

> **Note**
>
> Um SMT für eine bestehende Instance zu deaktivieren, gehen Sie wie unter Ändern Sie die CPU-Optionen für Ihre EC2 Instance beschrieben vor und ändern Sie die Anzahl der Threads, die pro Kern ausgeführt werden, auf 1.

Geben Sie CPUs beim Start eine benutzerdefinierte Zahl von v an

Sie können die Anzahl der CPU-Kerne und Threads pro Kern anpassen, wenn Sie eine Instance von der EC2 Konsole aus starten oder AWS CLI. Die Beispiele in diesem Abschnitt verwenden einen `r5.4xlarge`-Instance-Typ, der folgende Standardeinstellungen aufweist:

- CPU-Kerne: 8
- Threads pro Kern: 2

Instances werden standardmäßig mit der maximalen Anzahl von v gestartet, die für den Instance-Typ CPUs verfügbar ist. Für diesen Instance-Typ sind das insgesamt 16 v CPUs (8 Kerne mit jeweils 2 Threads). Weitere Informationen zu den Instance-Typen finden Sie unter RAM-optimierte Instances.

Im folgenden Beispiel wird eine `r5.4xlarge` Instanz mit 4 v gestartetCPUs.

Console

Um CPUs beim Start einer Instanz eine benutzerdefinierte Zahl von v anzugeben

1. Befolgen Sie das EC2-Instance mit dem Launch Instance Wizard in der Konsole starten-Verfahren und konfigurieren Sie Ihre Instance nach Bedarf.
2. Erweitern Sie Erweiterte Details und aktivieren Sie das Kontrollkästchen CPU-Optionen festlegen.
3. Um 4 V zu erhaltenCPUs, geben Sie 2 CPU-Kerne und 2 Threads pro Kern wie folgt an:
   - Für Anzahl Kerne wählen Sie 2 aus.
   - Wählen Sie für Threads per core (Threads pro Kern) wählen Sie 2 aus.
4. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten.

AWS CLI

Um CPUs beim Start der Instanz eine benutzerdefinierte Anzahl von v anzugeben

Verwenden Sie den AWS CLI Befehl run-instances und geben Sie die Anzahl der CPU-Kerne und die Anzahl der Threads im `--cpu-options` Parameter an. Sie können 2 CPU-Kerne und 2 Threads pro Kern angeben, um 4 V zu erhalten. CPUs

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type r7i.4xlarge \
    --cpu-options "CoreCount=2,ThreadsPerCore=2" \
    --key-name my-key-pair
```

Alternativ können Sie 4 CPU-Kerne und 1 Thread pro Kern angeben (SMT deaktivieren), um 4 V CPUs zu erhalten:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type r7i.4xlarge \
    --cpu-options "CoreCount=4,ThreadsPerCore=1" \
    --key-name my-key-pair
```

PowerShell

So geben Sie CPUs beim Start der Instanz eine benutzerdefinierte Anzahl von v an

Verwenden Sie den New-EC2InstanceBefehl und geben Sie die Anzahl der CPU-Kerne und die Anzahl der Threads im `-CpuOptions` Parameter an. Sie können 2 CPU-Kerne und 2 Threads pro Kern angeben, um 4 V zu erhaltenCPUs.

```
New-EC2Instance `
    -ImageId 'ami-0abcdef1234567890' `
    -InstanceType 'r7i.4xlarge' `
    -CpuOptions @{CoreCount=2; ThreadsPerCore=2} `
    -KeyName 'my-key-pair'
```

Alternativ können Sie 4 CPU-Kerne und 1 Thread pro Kern angeben (SMT deaktivieren), um 4 V CPUs zu erhalten:

```
New-EC2Instance `
    -ImageId 'ami-0abcdef1234567890' `
    -InstanceType 'r7i.4xlarge' `
    -CpuOptions @{CoreCount=4; ThreadsPerCore=1} `
    -KeyName 'my-key-pair'
```

Geben Sie eine benutzerdefinierte Anzahl von v CPUs in einer Startvorlage an

Sie können die Anzahl der CPU-Kerne und -Threads pro Kern für die Instance in einer Startvorlage anpassen. Die Beispiele in diesem Abschnitt verwenden einen `r5.4xlarge`-Instance-Typ, der folgende Standardeinstellungen aufweist:

- CPU-Kerne: 8
- Threads pro Kern: 2

Instances werden standardmäßig mit der maximalen Anzahl von v gestartet, die für den Instance-Typ CPUs verfügbar ist. Für diesen Instance-Typ sind das insgesamt 16 v CPUs (8 Kerne mit jeweils 2 Threads). Weitere Informationen zu den Instance-Typen finden Sie unter RAM-optimierte Instances.

Im folgenden Beispiel wird eine Startvorlage erstellt, die die Konfiguration für eine `r5.4xlarge` Instance mit 4 v spezifiziertCPUs.

Console

Um eine benutzerdefinierte Zahl von v CPUs in einer Startvorlage anzugeben

1. Befolgen Sie das Startvorlage durch Angabe von Parametern erstellen-Verfahren und konfigurieren Sie Ihre Startvorlage nach Bedarf.
2. Erweitern Sie Erweiterte Details und aktivieren Sie das Kontrollkästchen CPU-Optionen festlegen.
3. Um 4 V zu erhaltenCPUs, geben Sie 2 CPU-Kerne und 2 Threads pro Kern wie folgt an:
   - Für Anzahl Kerne wählen Sie 2 aus.
   - Wählen Sie für Threads per core (Threads pro Kern) wählen Sie 2 aus.
4. Überprüfen Sie im Bereich Zusammenfassung die Konfiguration Ihrer Instance und wählen Sie dann Startvorlage erstellen aus. Weitere Informationen finden Sie unter Instance-Startparameter in EC2 Amazon-Startvorlagen speichern.

AWS CLI

Um eine benutzerdefinierte Anzahl von v CPUs in einer Startvorlage anzugeben

Verwenden Sie den create-launch-template AWS CLI Befehl und geben Sie die Anzahl der CPU-Kerne und die Anzahl der Threads im `CpuOptions` Parameter an. Sie können 2 CPU-Kerne und 2 Threads pro Kern angeben, um 4 V zu erhaltenCPUs.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForCPUOptions \
    --version-description CPUOptionsVersion1 \
    --launch-template-data file://template-data.json
```

Nachfolgend finden Sie eine JSON-Beispieldatei, die die Startvorlagedaten, einschließlich der CPU-Optionen, für die Konfiguration der Instance für dieses Beispiel enthält.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-0abcdef1234567890"
    }],
```

```
    "ImageId": "ami-0abcdef1234567890",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":2,
        "ThreadsPerCore":2
    }
}
```

Alternativ können Sie 4 CPU-Kerne und 1 Thread pro Kern angeben (SMT deaktivieren), um 4 V CPUs zu erhalten:

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-0abcdef1234567890"
    }],
    "ImageId": "ami-0abcdef1234567890",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":4,
        "ThreadsPerCore":1
    }
}
```

PowerShell

Um eine benutzerdefinierte Anzahl von v CPUs in einer Startvorlage anzugeben

Verwenden Sie die New-EC2LaunchTemplate.

```
New-EC2LaunchTemplate `
    -LaunchTemplateName 'TemplateForCPUOptions' `
    -VersionDescription 'CPUOptionsVersion1' `
    -LaunchTemplateData (Get-Content -Path 'template-data.json' | ConvertFrom-Json)
```

Ändern Sie die CPU-Optionen für Ihre EC2 Instance

Da sich Ihre Anforderungen im Laufe der Zeit ändern, möchten Sie möglicherweise die Konfiguration der CPU-Optionen für eine bestehende Instance ändern. Jeder Thread, der auf Ihrer Instance ausgeführt wird, wird als virtuelle CPU (vCPU) bezeichnet. Sie können die Anzahl der vCPUs , die für eine bestehende Instance ausgeführt werden, in der EC2 Amazon-Konsole AWS CLI, API oder ändern SDKs. Bevor Sie diese Änderung vornehmen können, muss der Instance-Status `Stopped` erreicht sein.

Wählen Sie die Registerkarte aus, die Ihrer Umgebung entspricht, um die Konsolen- oder Befehlszeilenschritte anzuzeigen. Informationen zu API-Anfragen und Antworten finden Sie ModifyInstanceCpuOptionsin der Amazon EC2 API-Referenz.

Console

Gehen Sie wie folgt vor, um die Anzahl der aktiven V CPUs für Ihre Instance von der zu ändern AWS-Managementkonsole.

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus. Dadurch wird die Liste der Instances geöffnet, die für die aktuelle AWS-Region definiert sind.
3. Wählen Sie in der Liste der Instances die gewünschte Instance aus. Alternativ können Sie den Instance-Link auswählen, um die Instance-Detailseite zu öffnen.
4. Wenn die Instance ausgeführt wird, müssen Sie sie zuerst anhalten. Wählen Sie im Menü Instance-Status die Option Instance anhalten aus.
5. Um die vCPU-Konfiguration zu ändern, wählen Sie in den Instance-Einstellungen im Menü Aktionen die Option CPU-Optionen ändern aus. Dadurch wird die Seite CPU-Optionen ändern geöffnet.
6. Wählen Sie eine der folgenden CPU-Optionen aus, um die Konfiguration für Ihre Instance zu ändern.

Standard-CPU-Optionen verwenden

Diese Option setzt Ihre Instance auf die Standardzahl v CPUs für den Instance-Typ zurück. Standardmäßig werden alle Threads für alle CPU-Kerne ausgeführt.

CPU-Optionen angeben

Diese Option ermöglicht die Konfiguration der Anzahl von vCPUs , die auf Ihrer Instance ausgeführt werden.

7. Wenn Sie CPU-Optionen angeben ausgewählt haben, werden die CPUs Felder Active v angezeigt.

   - Verwenden Sie den ersten Selektor, um die Anzahl der Threads für jeden CPU-Kern zu konfigurieren. Um gleichzeitiges Multithreading zu deaktivieren, wählen Sie 1.
   - Verwenden Sie den zweiten Selektor, um die Anzahl der Läufe CPUs auf Ihrer Instance zu konfigurieren.

   Die folgenden Felder werden dynamisch aktualisiert, wenn Sie Änderungen an den CPU-Options-Selektoren vornehmen.

   - Active v CPUs: Die Anzahl der CPU-Kerne multipliziert mit den Threads pro Kern, basierend auf den von Ihnen getroffenen Auswahlen. Wenn Sie beispielsweise 2 Threads und 4 Kerne auswählen, entspricht das 8 V. CPUs
   - Summe v CPUs: Die maximale Anzahl von v CPUs für den Instanztyp. Für einen `m6i.4xlarge` Instance-Typ sind dies beispielsweise 16 v CPUs (8 Kerne mit jeweils 2 Threads).

8. Um Ihre Updates anzuwenden, wählen Sie Ändern aus.

AWS CLI

Gehen Sie wie folgt vor, um die Anzahl der aktiven V CPUs für Ihre Instance gegenüber dem zu ändern AWS CLI.

Verwenden Sie den modify-instance-cpu-optionsBefehl und geben Sie im `--core-count` Parameter die Anzahl der CPU-Kerne an, die ausgeführt werden, sowie die Anzahl der Threads, die `--threads-per-core` pro Kern ausgeführt werden.

Die folgenden Beispiele zeigen zwei mögliche Konfigurationen für einen `m6i.4xlarge` Instanztyp, um 8 v CPUs auf der angegebenen Instanz auszuführen. Die Standardeinstellung für diesen Instance-Typ ist 16 V CPUs (8 Kerne mit jeweils 2 Threads).

Beispiel 1: Führen Sie 4 CPU-Kerne mit 2 Threads pro Kern aus, also insgesamt 8 vCPUs.

```
aws ec2 modify-instance-cpu-options \
    --instance-id i-1234567890abcdef0 \

    --core-count=4 \
    --threads-per-core=2
```

Beispiel 2: Deaktivieren Sie gleichzeitiges Multithreading, indem Sie die Anzahl der Threads, die pro Kern ausgeführt werden, auf 1 ändern. In der resultierenden Konfiguration werden außerdem insgesamt 8 V ausgeführt CPUs (8 CPU-Kerne mit 1 Thread pro Kern).

```
aws ec2 modify-instance-cpu-options \
    --instance-id 1234567890abcdef0 \
    --core-count=8 \
    --threads-per-core=1
```

PowerShell

Um die Anzahl der aktiven V CPUs für eine Instanz zu ändern

Verwenden Sie das Edit-EC2InstanceCpuOptionCmdlet und geben Sie im `-CoreCount` Parameter die Anzahl der CPU-Kerne an, die ausgeführt werden, sowie die Anzahl der Threads, die pro Kern ausgeführt werden. `ThreadsPerCore`

Beispiel 1: Führen Sie 4 CPU-Kerne mit 2 Threads pro Kern aus, also insgesamt 8 vCPUs.

```
Edit-EC2InstanceCpuOption `
    -InstanceId 'i-1234567890abcdef0' `
    -CoreCount 4 `
    -ThreadsPerCore 2
```

Beispiel 2: Deaktivieren Sie gleichzeitiges Multithreading, indem Sie die Anzahl der Threads, die pro Kern ausgeführt werden, auf 1 ändern. In der resultierenden Konfiguration werden außerdem insgesamt 8 V CPUs (8 CPU-Kerne mit 1 Thread pro Kern) ausgeführt.

```
Edit-EC2InstanceCpuOption `
    -InstanceId 'i-1234567890abcdef0' `
    -CoreCount 8 `
    -ThreadsPerCore 1
```

CPU-Threads und Kerne für eine EC2 Amazon-Instance anzeigen

Sie können die CPU-Optionen für eine vorhandene Instance anzeigen, indem Sie die Instance beschreiben.

Console

So zeigen Sie die CPU-Optionen für eine Instance an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im linken Navigationsbereich auf Instances und wählen Sie die Instance aus.
3. Suchen Sie auf der Registerkarte Details unter Host und Platzierungsgruppe nach Nummer von CPUs v.

AWS CLI

So zeigen Sie die CPU-Optionen für eine Instance an

Verwenden Sie den Befehl describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].CpuOptions
```

Es folgt eine Beispielausgabe. Das Feld `CoreCount` gibt die Anzahl der Kerne für die Instance an. Das Feld `ThreadsPerCore` gibt die Anzahl der Threads pro Kern an.

```
[
    {
        "CoreCount": 24,
        "ThreadsPerCore": 2
    },
]
```

PowerShell

So zeigen Sie die CPU-Optionen für eine Instance an

Verwenden Sie das cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId 'i-1234567890abcdef0').Instances.CpuOptions
```

Es folgt eine Beispielausgabe.

```
AmdSevSnp CoreCount ThreadsPerCore
--------- --------- --------------
          24        2
```

Um CPU-Informationen anzuzeigen, können Sie alternativ eine Verbindung zu Ihrer Instance herstellen und eines der folgenden Systemtools verwenden:

- Windows `Task Manager` auf Ihrer Windows-Instance
- Der lscpu-Befehl auf Ihrer Linux-Instance

Sie können AWS Config es verwenden, um Konfigurationsänderungen für Instances, einschließlich beendeter Instances, aufzuzeichnen, zu bewerten, zu prüfen und auszuwerten. Weitere Informationen finden Sie unter Erste Schritte mit AWS Config im AWS Config -Developerhandbuch.

Optimieren Sie CPUs für Instances, die in der Lizenz enthalten sind

Workloads wie Microsoft SQL Server erfordern häufig viel Arbeitsspeicher und IOPS, aber eine geringe Anzahl an vCPUs. AWS bietet eine breite Palette von Instance-Typen, die die meisten Ihrer Infrastrukturanforderungen abdecken können. Um jedoch die vCPU-basierten Lizenzkosten für Windows und Microsoft SQL Server zu reduzieren, können Sie die Anzahl der auf Ihrer EC2 Instanz CPUs ausgeführten v anpassen und dabei denselben Arbeitsspeicher und dieselbe IOPS beibehalten. Verwenden Sie die Optimize-Funktion, um CPU-Optionen auf Ihrer Instance zu konfigurieren und vCPU-basierte Lizenzkosten sowohl für Workloads mit Lizenz als auch für Workloads Bring-Your-Own-License (BYOL) einzusparen. CPUs

Weitere Informationen finden Sie in diesem Blogbeitrag über bewährte Methoden zur Optimierung für SQL Server-Workloads. CPUs

Unterstützte Lizenztypen

Optimize CPUs unterstützt die Abrechnung auf der Grundlage der Anzahl der aktiven CPUs für die folgenden Arten von Lizenzkonfigurationen für Instances, die über ein AMI mit Lizenz gestartet wurden. Weitere Informationen zu Lizenztypen finden Sie unter Felder für AMI-Fakturierungsdaten.

Fakutierung von lizenzinbegriffenen AMI-Instances

Lizenzen enthalten	Verwendungsvorgang	Preis pro vCPU-Stunde
Windows Server	RunInstancesOptimize unterstützt die Abrechnung auf der Grundlage der Anzahl der aktiven für die folgenden Arten von Lizenzkonfiguratio nen für Instances, die über ein in der Lizenz enthaltenes AMI gestartet wurden. ----sep-- --:0002	0,046$
Windows Server mit SQL Server Enterprise	RunInstances0,046$ ----sep-- --:0102	0,421$
Windows Server mit SQL Server Standard	RunInstances0,421$ ----sep-- --:0006	0,166$
Windows Server mit SQL Server Web	RunInstances0,166$ ----sep-- --:0202	0,063$

Unterstützte Kaufoptionen

Optimize CPUs unterstützt die folgenden Kaufoptionen für Instanzen, die eine Lizenz enthalten:

- On-Demand
- Savings Plans

> **Warning**
>
> Wenn Sie Reserved Instances verwenden, werden Rabatte möglicherweise nicht gewährt, wenn Sie Optimize CPUs für Instances mit Lizenz auf demselben Zahlerkonto konfigurieren. Wir empfehlen Ihnen, Savings Plans zu verwenden, um die vCPU-basierten Lizenzkosten zu senken und vergleichbare Einsparungen bei Ihren Rechenkosten zu erzielen.
> Konten, die vor dem 15. Oktober 2025 CPUs sowohl Optimize als auch Reserved Instances for Windows und SQL Server auf demselben Instanztyp verwendet haben, wurden zu einer Opt-Out-Liste hinzugefügt, um ihre aktuelle Abrechnungserfahrung beizubehalten. Wenn Sie die Vorteile von Optimize CPUs für Lizenzeinsparungen nutzen möchten, wenden Sie sich an das AWS -Support Center, um sich von der Opt-Out-Liste streichen zu lassen.

So CPUs funktioniert Optimize, um Lizenzgebühren zu sparen

Die folgenden Beispiele verdeutlichen die Kosteneinsparungen, die durch die Konfiguration Ihrer CPU-Auslastung möglich sind.

Beispiel 1: Standardabrechnung Dieses Beispiel zeigt eine r7i.8xlarge-Instance, die von einem Windows- und SQL Server Enterprise-AMI aus gestartet wurde, das 100 Stunden lang mit der Standard-CPU-Konfiguration von 32 V CPUs für den Instance-Typ (3200 vCPU-Stunden) lief.

Die Rechnung enthält einen Einzelposten mit einem kombinierten Tarif, der sowohl Nutzungs- als auch Lizenzgebühren beinhaltet.

For illustration purposes only **Amazon Web Services, Inc. charges by service** **Total services: 1** **Description**	**Usage Quantity**	**Total charges** **$1,558.88** **Amount in USD**
Elastic Compute Cloud		$1,558.88
|- US East (N. Virginia)		$1,558.88
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$1,558.88
| |- $15.5888 per On Demand Windows with SQL Server Enterprise r7i.8xlarge Instance Hour	100 Hrs	$1,558.88

Beispiel 2: CPUs Abrechnung optimieren Dieses Beispiel zeigt eine r7i.8xlarge-Instance, die über ein Windows- und SQL Server Enterprise-AMI gestartet wurde, das in der Lizenz enthalten ist. Um Lizenzgebühren zu sparen, wurde die Anzahl der aktiven Benutzer auf CPUs 16 v reduziert. CPUs Dann lief die Instanz 100 Stunden lang mit der neuen Konfiguration.

Die Rechnung enthält die folgenden zwei Einzelposten.

Beschreibung der Fakturierung: Elastic Compute Cloud

Die erste Zeile zeigt die Basiskosten der Windows- und SQL-Server-Instance, die 100 Stunden lang ausgeführt wurde (211,68 USD).

Beschreibung der Abrechnung: Amazon EC2 Optimize CPU-Lizenz inklusive Gebühren von Drittanbietern

Die zweite Position deckt Lizenzgebühren ab, die auf der Anzahl der V basierenCPUs , die im Abrechnungszeitraum aktiv waren (673,60 USD).

For illustration purposes only **Amazon Web Services, Inc. charges by service** **Total services: 2** **Description**	**Usage Quantity**	**Total charges** **$885.28** **Amount in USD**
Elastic Compute Cloud		$211.68
|- US East (N. Virginia)		$211.68
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$211.68
| |- $2.1168 per On Demand Windows and SQL Server Enterprise without licenses r7i.8xlarge Instance Hr	100 Hrs	$211.68
Amazon EC2 Optimize CPU License Included Third Party Fees		$673.60
|- US East (N. Virginia)		$673.60
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$673.60
| |- $0.421 per vCPU-Hour of On Demand Windows with SQL Server licenses on r7i Instance	1,600 vCPU-Hrs	$673.60

Beispiel 3: Optimieren Sie die CPUs Abrechnung mit Savings Plans Dieses Beispiel zeigt eine r7i.8xlarge-Instance, die über ein Windows- und SQL Server Enterprise-AMI gestartet wurde, das in der Lizenz enthalten ist. Um Lizenzgebühren zu sparen, wurde die Anzahl der aktiven Benutzer auf CPUs 16 v reduziert. CPUs Dann lief die Instanz 100 Stunden lang mit der neuen Konfiguration.

Ein einjähriger Compute Savings Plan ohne Vorauszahlung mit einer Verpflichtung von 1,60 USD pro Stunde (gerundet) bietet weitere Kosteneinsparungen, die die Basiskosten der Windows- und SQL-Server-Instance senken. Das Savings-Plan-Abonnement deckt die volle 100-stündige Nutzung der r7i.8xlarge-Instance bei einem Savings-Plan-Tarif von 1,53362 USD pro Stunde ab.

Die Rechnung enthält die folgenden Einzelposten.

Beschreibung der Fakturierung: Savings Plans für die Datenverarbeitung

Die erste Zeile zeigt die Savings-Plan-Verpflichtung für die volle Nutzung von 100 Stunden (160,00 USD).

Beschreibung der Fakturierung: Elastic Compute Cloud

Die zweite Posten enthält zwei Einträge. Der erste Eintrag zeigt, wie hoch die Basiskosten der Windows- und SQL-Server-Instance, die 100 Stunden lang ausgeführt wurde, ohne den Savings

Plan gewesen wären (211,68 USD). Der zweite Eintrag zeigt, dass die gesamten Basiskosten durch den Compute Savings Plan gedeckt wurden (-211,68 USD), was Nettokosten von Null für diesen Posten ergibt.

Beschreibung der Abrechnung: Amazon EC2 Optimize CPU-Lizenz inklusive Gebühren von Drittanbietern

Die dritte Position deckt Lizenzgebühren ab, die auf der Anzahl der V basierenCPUs , die im Abrechnungszeitraum aktiv waren (673,60 USD).

For illustration purposes only **Amazon Web Services, Inc. charges by service** **Total services: 3** **Description**	**Usage Quantity**	**Total charges** **$833.60** **Amount in USD**
Savings Plans for Compute usage		$160.00
|- Any		$160.00
|- Compute Savings Plans		$160.00
| |- 1 year No Upfront Compute Savings Plan	100 Hrs	$160.00
Elastic Compute Cloud		$0.00
|- US East (N. Virginia)		$0.00
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$0.00
| |- $2.1168 per On Demand Windows and SQL Server Enterprise without licenses r7i.8xlarge Instance Hr	100 Hrs	$211.68
| |- r7i.8xlarge Windows with SQL Server Enterprise without licenses instance usage covered by CSP	100 Hrs	($211.68)
Amazon EC2 Optimize CPU License Included Third Party Fees		$673.60
|- US East (N. Virginia)		$673.60
|- Amazon Elastic Compute Cloud running Windows and SQL Server Enterprise		$673.60
| |- $0.421 per vCPU-Hour of On Demand Windows with SQL Server licenses on r7i Instance	1,600 vCPU-Hrs	$673.60

AMD SEV-SNP für Amazon-EC2-Instances

AMD Secure Encrypted Virtualization-Secure Nested Paging (AMD SEV-SNP) ist ein CPU-Feature, das die folgenden Eigenschaften bietet:

- Bescheinigung – Mit AMD SEV-SNP können Sie einen signierten Bescheinigungsbericht abrufen, der eine kryptografische Maßnahme enthält, mit welcher der Status und die Identität der Instance sowie die Ausführung auf echter AMD-Hardware überprüft werden kann. Weitere Informationen finden Sie unter Eine Amazon-EC2-Instance mit AMD SEV-SNP bescheinigen.
- Speicherverschlüsselung – Ab den folgenden Prozessoren ist der Instance-Speicher immer verschlüsselt: AMD EPYC (Milan), AWS Graviton2 und Intel Xeon Scalable (Ice Lake). Für AMD SEV-SNP aktivierte Instances verwenden einen Instance-spezifischen Schlüssel für ihre Speicherverschlüsselung.

Inhalt

- Konzepte und Terminologie

- Voraussetzungen
- Überlegungen
- Preisgestaltung
- EC2-Instance-Typen suchen, die AMD SEV-SNP unterstützen
- AMD SEV-SNP für eine EC2-Instance aktivieren
- Eine Amazon-EC2-Instance mit AMD SEV-SNP bescheinigen

Konzepte und Terminologie

Bevor Sie mit AMD SEV-SNP beginnen, sollten Sie mit den folgenden Konzepten und Begriffen vertraut sein:

Bescheinigungsbericht von AMD SEV-SNP

Der Bescheinigungsbericht von AMD SEV-SNP ist ein Dokument, das eine Instance von der CPU anfordern kann. Der Bescheinigungsbericht von AMD SEV-SNP kann verwendet werden, um den Status und die Identität einer Instance zu überprüfen und sicherzustellen, ob sie in einer genehmigten AMD-Umgebung ausgeführt wird. Der Bericht enthält eine Startmessung, bei der es sich um einen kryptografischen Hash des anfänglichen Startstatus einer Instance handelt, einschließlich des ursprünglichen Speicherinhalts der Instance und des Anfangsstatus der vCPUs. Der Bescheinigungsbericht von AMD SEV-SNP ist mit einer VLEK-Signatur signiert, die auf eine AMD-Stammvertrauenstellung zurückgeht.

VLEK

Der VLEK (Versioned Loaded Endorsement Key) ist ein Signaturschlüssel mit Versionsverwaltung, der von AMD zertifiziert ist und von der AMD-CPU zum Signieren der Bescheinigungsberichte von AMD SEV-SNP verwendet wird. VLEK-Signaturen können mit den von AMD bereitgestellten Zertifikaten validiert werden.

OVMF-Binärdatei

OVMF (Open Virtual Machine Firmware) ist der Frühstartcode, der verwendet wird, um eine UEFI-Umgebung für die Instance bereitzustellen. Der Frühstartcode wird ausgeführt, bevor der Code im AMI gestartet wird. Die OVMF findet und führt auch das im AMI bereitgestellte Startladeprogramm aus. Weitere Informationen finden Sie im OMVF-Repository.

Voraussetzungen

Zur Verwendung von AMD SEV-SNP müssen Sie folgende Voraussetzungen erfüllen:

- Verwenden Sie einen der folgenden unterstützten Instance-Typen:
  - Universell: `m6a.large` | `m6a.xlarge` | `m6a.2xlarge` | `m6a.4xlarge` | `m6a.8xlarge`
  - Für Datenverarbeitung optimiert: `c6a.large` | `c6a.xlarge` | `c6a.2xlarge` | `c6a.4xlarge` | `c6a.8xlarge` | `c6a.12xlarge` | `c6a.16xlarge`
  - Speicheroptimiert: `r6a.large` | `r6a.xlarge` | `r6a.2xlarge` | `r6a.4xlarge`
- Starten Sie Ihre Instance in einer unterstützten AWS-Region. Derzeit werden nur USA Ost (Ohio) und Europa (Irland) unterstützt.
- Verwenden Sie ein AMI mit dem Startmodus `uefi` oder`uefi-preferred` und einem Betriebssystem, das AMD SEV-SNP unterstützt. Weitere Informationen zur Unterstützung von AMD SEV-SNP unter Ihrem Betriebssystem finden Sie in der Dokumentation des jeweiligen Betriebssystems. Für AWS wird AMD SEV-SNP auf AL2023, RHEL 9.3, SLES 15 SP4 und Ubuntu 23.04 und höher unterstützt.

Überlegungen

AMD SEV-SNP kann nur beim Start einer Instance aktiviert werden. Wenn AMD SEV-SNP für den Start Ihrer Instance aktiviert ist, gelten die folgenden Regeln.

- Sobald es aktiviert ist, kann AMD SEV-SNP nicht mehr deaktiviert werden. Es bleibt während des gesamten Instance-Lebenszyklus aktiviert.
- Sie können den Instance-Typ nur in einen anderen Instance-Typ ändern, der AMD SEV-SNP unterstützt.
- Ruhezustand und Nitro Enclaves werden nicht unterstützt.
- Dedicated Hosts werden nicht unterstützt.
- Wenn für den zugrundeliegenden Host Ihrer Instance eine Wartung geplant ist, erhalten Sie 14 Tage im Voraus eine Benachrichtigung über ein geplantes Ereignis. Sie müssen Ihre Instance manuell stoppen oder neu starten, um sie auf einen neuen Host zu verschieben.

Preisgestaltung

Wenn Sie eine Amazon-EC2-Instance mit aktiviertem AMD SEV-SNP starten, wird Ihnen eine zusätzliche stündliche Nutzungsgebühr in Höhe von 10 Prozent des On-Demand-Stundensatzes des ausgewählten Instance-Typs berechnet.

Diese Nutzungsgebühr für AMD SEV-SNP ist eine separate Gebühr für die Nutzung Ihrer Amazon-EC2-Instance. Reserved Instances, Savings Plans und die Nutzung des Betriebssystems haben keinen Einfluss auf diese Gebühr.

Wenn Sie eine Spot Instance konfigurieren, mit aktiviertem AMD SEV-SNP zu starten, wird Ihnen eine zusätzliche stündliche Nutzungsgebühr in Höhe von 10 % des On-Demand-Stundensatzes des ausgewählten Instance-Typs berechnet. Wenn die Zuweisungsstrategie den Preis als Eingabewert verwendet, berücksichtigt die Spot-Flotte diese zusätzliche Gebühr nicht. Es wird nur der Spot-Preis verwendet.

EC2-Instance-Typen suchen, die AMD SEV-SNP unterstützen

Sie können Instance-Typen suchen, die AMD SEV-SNP unterstützen. Die Amazon-EC2-Konsole zeigt diese Informationen für einen Instance-Typ nicht an.

AWS CLI

So suchen Sie Instance-Typen, die AMD SEV-SNP unterstützen

Verwenden Sie den folgenden describe-instance-types-Befehl.

```
aws ec2 describe-instance-types \
    --filters Name=processor-info.supported-features,Values=amd-sev-snp \
    --query 'InstanceTypes[*].[InstanceType]' \
    --output text | sort
```

Es folgt eine Beispielausgabe.

```
c6a.12xlarge
c6a.16xlarge
c6a.2xlarge
c6a.4xlarge
c6a.8xlarge
c6a.large
c6a.xlarge
m6a.2xlarge
```

```
m6a.4xlarge
m6a.8xlarge
m6a.large
m6a.xlarge
r6a.2xlarge
r6a.4xlarge
r6a.large
r6a.xlarge
```

PowerShell

So suchen Sie Instance-Typen, die AMD SEV-SNP unterstützen

Verwenden Sie das cmdlet Get-EC2InstanceType.

```
(Get-EC2InstanceType `
    -Filter @{Name="processor-info.supported-features"; Values="amd-sev-
snp"}).InstanceType.Value | Sort-Object
```

Es folgt eine Beispielausgabe.

```
c6a.12xlarge
c6a.16xlarge
c6a.2xlarge
c6a.4xlarge
c6a.8xlarge
c6a.large
c6a.xlarge
m6a.2xlarge
m6a.4xlarge
m6a.8xlarge
m6a.large
m6a.xlarge
r6a.2xlarge
r6a.4xlarge
r6a.large
r6a.xlarge
```

AMD SEV-SNP für eine EC2-Instance aktivieren

Sie können eine Instance mit aktiviertem AMD SEV-SNP starten. AMD SEV-SNP kann nach dem Start nicht mehr aktiviert werden.

Eine Instance mit aktiviertem AMD SEV-SNP starten

AMD SEV-SNP kann nicht mit der Amazon-EC2-Konsole aktiviert werden.

AWS CLI

So starten Sie eine Instance mit aktiviertem AMD SEV-SNP

Verwenden Sie den Befehl run-instances mit der Option `--cpu-options`. Weitere Anforderungen finden Sie unter Anforderungen für AMD SEV-SNP.

```
--cpu-options AmdSevSnp=enabled
```

PowerShell

So starten Sie eine Instance mit aktiviertem AMD SEV-SNP

Verwenden Sie das Cmdlet New-EC2Instance mit dem `-CpuOption`-Parameter.

```
-CpuOption @{AmdSevSnp="enabled"}
```

Prüfen, ob eine EC2-Instance für AMD SEV-SNP aktiviert ist

Sie können Instances suchen, die für AMD SEV-SNP aktiviert sind. Die Amazon-EC2-Konsole zeigt diese Informationen nicht an.

AWS CLI

So prüfen Sie, ob AMD SEV-SNP für eine Instance aktiviert ist

Verwenden Sie den describe-instances-Befehl.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].CpuOptions
```

Es folgt eine Beispielausgabe. Wenn `AmdSevSnp` nicht in `CpuOptions` vorhanden ist, ist AMD SEV-SNP deaktiviert.

```
[
```

```
    {
        "AmdSevSnp": "enabled",
        "CoreCount": 1,
        "ThreadsPerCore": 2
    }
]
```

PowerShell

So prüfen Sie, ob AMD SEV-SNP für eine Instance aktiviert ist

Verwenden Sie das cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.CpuOptions
```

Es folgt eine Beispielausgabe. Wenn der Wert von `AmdSevSnp` nicht vorhanden ist, ist AMD SEV-SNP deaktiviert.

```
AmdSevSnp CoreCount ThreadsPerCore
--------- --------- --------------
enabled   1         2
```

AWS CloudTrail

Im AWS CloudTrail-Ereignis für die Instance-Startanforderung zeigt die folgende Eigenschaft an, dass AMD SEV-SNP für die Instance aktiviert ist.

```
"cpuOptions": {"AmdSevSnp": "enabled"}
```

Eine Amazon-EC2-Instance mit AMD SEV-SNP bescheinigen

Die Bescheinigung ist ein Prozess, mit dem Ihre Instance ihren Status und ihre Identität nachweisen kann. Nachdem Sie AMD SEV-SNP für Ihre Instance aktivieren, können Sie vom zugrunde liegenden Prozessor einen AMD-SEV-SNP-Bestätigungsbericht anfordern. Der AMD-SEV-SNP-Bescheinigungsbericht enthält einen kryptografischen Hash, die sogenannte Startmessung, die den anfänglichen Inhalt des Gastspeichers und den anfänglichen vCPU-Status anzeigt. Der Bescheinigungsbericht ist mit einer VLEK-Signatur signiert, die auf eine AMD-Stammvertrauenstellung zurückgeht. Sie können anhand der im Bescheinigungsbericht enthaltenen

Startmessung überprüfen, ob die Instance in einer echten AMD-Umgebung ausgeführt wird, und den anfänglichen Startcode überprüfen, der zum Starten der Instance verwendet wurde.

Voraussetzung

Starten Sie eine Instance, die für AMD SEV-SNP aktiviert ist. Weitere Informationen finden Sie unter AMD SEV-SNP für eine EC2-Instance aktivieren.

Schritte

- Schritt 1: Abrufen des Bescheinigungsberichts
- Schritt 2: Signatur des Bestätigungsbericht validieren

Schritt 1: Abrufen des Bescheinigungsberichts

In diesem Schritt installieren und erstellen Sie das `snpguest`-Hilfsprogramm und verwenden es dann, um den Bestätigungsbericht von AMD SEV-SNP anzufordern.

1. Verbinden Sie sich mit der Instance.
2. Führen Sie die folgenden Befehle aus, um das `snpguest`-Hilfsprogramm vom snpguest repository zu installieren.

   ```
   $ git clone https://github.com/virtee/snpguest.git
   $ cd snpguest
   $ cargo build -r
   $ cd target/release
   ```

3. Generieren Sie eine Anfrage für den Bestätigungsbericht. Das Hilfsprogramm fordert den Bestätigungsbericht vom Host an und schreibt ihn mit den bereitgestellten Anforderungsdaten in eine Binärdatei.

   Das folgende Beispiel erstellt eine zufällige Anforderungszeichenfolge und verwendet sie als Anforderungsdatei (`request-file.txt`). Wenn der Befehl den Bestätigungsbericht zurückgibt, wird er in dem von Ihnen angegebenen Dateipfad gespeichert (`report.bin`). In diesem Fall speichert das Hilfsprogramm den Bericht im aktuellen Verzeichnis.

   ```
   $ ./snpguest report report.bin request-file.txt --random
   ```

4. Fordern Sie die Zertifikate aus dem Host-Speicher an und speichern Sie sie als PEM-Dateien. Im folgenden Beispiel werden die Dateien im selben Verzeichnis wie das `snpguest`-Hilfsprogramm

gespeichert. Wenn im angegebenen Verzeichnis bereits Zertifikate vorhanden sind, werden diese Zertifikate überschrieben.

```
$ ./snpguest certificates PEM ./
```

Schritt 2: Signatur des Bestätigungsbericht validieren

Der Bescheinigungsbericht ist mit einem Zertifikat signiert, dem sogenannten Versioned Loaded Endorsement Key (VLEK), das von AMD für AWS ausgestellt wird. In diesem Schritt können Sie überprüfen, ob das VLEK-Zertifikat von AMD ausgestellt wurde und ob der Bestätigungsbericht mit diesem VLEK-Zertifikat signiert ist.

1. Laden Sie die VLEK-Zertifikate der Root-Vertrauenstellung von der offiziellen AMD-Website in das aktuelle Verzeichnis herunter.

   ```
   $ sudo curl --proto '=https' --tlsv1.2 -sSf https://kdsintf.amd.com/vlek/v1/Milan/
   cert_chain -o ./cert_chain.pem
   ```

2. Verwenden Sie `openssl`, um zu überprüfen, ob das VLEK-Zertifikat von den Zertifikaten der AMD-Stammvertrauenstellung signiert ist.

   ```
   $ sudo openssl verify --CAfile ./cert_chain.pem vlek.pem
   ```

   Es folgt eine Beispielausgabe.

   ```
   vlek.pem: OK
   ```

3. Verwenden Sie das Dienstprogramm `snpguest`, um zu überprüfen, ob der Bescheinigungsbericht mit dem VLEK-Zertifikat signiert ist.

   ```
   $ ./snpguest verify attestation ./ report.bin
   ```

   Es folgt eine Beispielausgabe.

   ```
   Reported TCB Boot Loader from certificate matches the attestation report.
   Reported TCB TEE from certificate matches the attestation report.
   Reported TCB SNP from certificate matches the attestation report.
   Reported TCB Microcode from certificate matches the attestation report.
   ```

```
VEK signed the Attestation Report!
```

Kontrolle des Prozessorstatus für Amazon EC2 Linux-Instances

C-Status steuern die Ruhezustände, in die ein Kern eintreten kann, wenn er sich im Leerlauf befindet. C-Zustände sind von C0 (Arbeitszustand, in dem der Core „wach“ ist und Anweisungen ausführt) bis C6 („tiefster“ Leerlaufzustand, in dem ein Core ausgeschaltet ist) nummeriert.

P-Status steuern die gewünschte Leistung (in CPU-Frequenz) eines Kerns. P-Zustände sind ab P0 (höchste Performancestufe, in der Intel Turbo Boost-Technologie für den Core eingesetzt werden kann, um ggf. die Frequenz zu erhöhen) über P1 (in diesem P-Zustand wird die maximale Basisfrequenz angefordert) bis P15 (geringstmögliche Frequenz) nummeriert.

> **Note**
>
> AWS Graviton-Prozessoren verfügen über integrierte Energiesparmodi und arbeiten mit einer festen Frequenz. Daher bieten sie dem Betriebssystem nicht die Möglichkeit, C-States und P-States zu überwachen.

C-Staaten und P-Staaten

Bei den folgenden Instance-Typen besteht für ein Betriebssystem die Möglichkeit, den C- und P-Zustand von Prozessoren zu steuern:

- Allzweck: `m4.10xlarge` | `m4.16xlarge`
- Für Datenverarbeitung optimiert: `c4.8xlarge`
- Für Arbeitsspeicher optimiert: `r4.8xlarge` | `r4.16xlarge` | `x1.16xlarge` | `x1.32xlarge` | `x1e.8xlarge` | `x1e.16xlarge` | `x1e.32xlarge`
- Speicheroptimiert: `d2.8xlarge` | `i3.8xlarge` | `i3.16xlarge` | `h1.8xlarge` | `h1.16xlarge`
- Beschleunigte Datenverarbeitung: `f1.16xlarge` | `g3.16xlarge` | `p2.16xlarge` | `p3.16xlarge`
- Bare Metal: Alle Bare-Metal-Instances mit Intel- und AMD-Prozessoren

Nur C-Staaten

Bei den folgenden Instance-Typen besteht für ein Betriebssystem die Möglichkeit, den C-Zustand von Prozessoren zu steuern:

- Allgemeiner Zweck: m5.12xlarge m5.24xlarge | m5d.12xlarge | | m5d.24xlarge | m5n.12xlarge | m5n.24xlarge | m5dn.12xlarge | m5dn.24xlarge | m5zn.6xlarge | m5zn.12xlarge | m6a.24xlarge | m6a.48xlarge | m6i.16xlarge | m6i.32xlarge | m6id.16xlarge | m6id.32xlarge | | m6idn.16xlarge | m6in.16xlarge | m6in.32xlarge | m7a.medium | m7a.large | m7a.xlarge | m7a.2xlarge | m7a.4xlarge | m7a.8xlarge | m7a.12xlarge | m7a.16xlarge | m7a.24xlarge | m7a.32xlarge | | m7a.48xlarge | m7i.large | m7i.xlarge | m7i.2xlarge | m7i.4xlarge | m7i.8xlarge | m7i.12xlarge m7i.16xlarge| m7i.24xlarge | m7i.48xlarge | m8a.medium | m8a.large | m8a.xlarge | m8a.2xlarge | m8a.4xlarge | m8a.8xlarge | m8a.12xlarge | m8a.16xlarge m8a.24xlarge | m8a.48xlarge | m8i.large | m8i.xlarge | m8i.2xlarge | m8i.4xlarge | m8i.8xlarge | m8i.12xlarge | m8i.16xlarge | m8i.24xlarge | m8i.32xlarge | m8i.48xlarge | m8i.96xlarge
- Computeroptimiert: c5.9xlarge | c5.12xlarge | c5.18xlarge | | c5.24xlarge | c5a.24xlarge | c5ad.24xlarge | c5d.9xlarge | c5d.12xlarge | c5d.18xlarge | c5d.24xlarge | c5n.9xlarge | c5n.18xlarge | c6a.24xlarge | c6a.32xlarge | c6a.48xlarge | c6i.16xlarge | c6i.32xlarge | | c6id.24xlarge | c6id.32xlarge | c6in.32xlarge | c7a.medium | c7a.large | c7a.xlarge | c7a.2xlarge | c7a.4xlarge | c7a.8xlarge | c7a.12xlarge | c7a.16xlarge | c7a.24xlarge | c7a.32xlarge | | c7a.48xlarge | c7i.large | c7i.xlarge | c7i.2xlarge | c7i.4xlarge | c7i.8xlarge | c7i.12xlarge| c7i.16xlarge | c7i.24xlarge | c7i.48xlarge | c8a.medium | c8a.large | c8a.xlarge | c8a.2xlarge | c8a.4xlarge | c8a.8xlarge | c8a.12xlarge c8a.16xlarge | c8a.24xlarge | c8a.48xlarge | c8i.large | c8i.xlarge | c8i.2xlarge | c8i.4xlarge | c8i.8xlarge | c8i.12xlarge | c8i.16xlarge | c8i.24xlarge | c8i.32xlarge | c8i.48xlarge | c8i.96xlarge
- Speicheroptimiert: r5.12xlarge r5.24xlarge | r5b.12xlarge | r5d.12xlarge | r5d.24xlarge | r5n.12xlarge | r5n.24xlarge | r5dn.12xlarge | r5dn.24xlarge | r6a.24xlarge | r6a.48xlarge r6i.16xlarge | r6i.32xlarge | r6id.16xlarge | r6id.32xlarge | r6in.16xlarge | r6in.32xlarge | r7a.medium | r7a.large | r7a.xlarge | r7a.2xlarge r7a.4xlarge | r7a.8xlarge | r7a.12xlarge | r7a.16xlarge | r7a.24xlarge | r7a.32xlarge | r7a.48xlarge | r7i.large | r7i.xlarge | r7i.2xlarge r7i.4xlarge | r7i.8xlarge | r7i.12xlarge | r7i.16xlarge | r7i.24xlarge | r7i.48xlarge| r7iz.large | r7iz.xlarge | |

`r7iz.2xlarge | r7iz.4xlarge | r7iz.8xlarge | r7iz.12xlarge | r7iz.16xlarge || r7iz.32xlarge | r8a.medium | r8a.large | r8a.xlarge | r8a.2xlarge | r8a.4xlarge || r8a.8xlarge | r8a.12xlarge | r8a.16xlarge | r8a.24xlarge | r8a.48xlarge || r8i.large | r8i.xlarge | r8i.2xlarge | r8i.4xlarge | r8i.8xlarge || r8i.12xlarge | r8i.16xlarge | r8i.24xlarge | r8i.32xlarge | r8i.48xlarge | r8i.96xlarge || u-3tb1.56xlarge | u-6tb1.56xlarge | u-6tb1.112xlarge | u-9tb1.112xlarge | u-12tb1.112xlarge || u-18tb1.112xlarge | u-24tb1.112xlarge | u7i-6tb.112xlarge | u7i-8tb.112xlarge| u7i-12tb.224xlarge | u7in-16tb.224xlarge | u7in-24tb.224xlarge | u7in-32tb.224xlarge | u7inh-32tb.480xlarge | x2idn.32xlarge | x2iedn.16xlarge || x2iedn.32xlarge | x2iezn.12xlarge | x8aedz.large | x8aedz.xlarge | x8aedz.3xlarge | x8aedz.6xlarge | x8aedz.12xlarge | x8aedz.24xlarge | z1d.6xlarge | z1d.12xlarge`

- Speicheroptimiert: `d3en.12xlarge dl1.24xlarge | i3en.12xlarge | i3en.24xlarge | i4i.16xlarge | i7i.large | i7i.xlarge | i7i.2xlarge | i7i.4xlarge | i7i.8xlarge i7i.12xlarge | i7i.16xlarge | i7i.24xlarge | i7i.48xlarge | i7ie.large | i7ie.xlarge | i7ie.2xlarge | i7ie.3xlarge | i7ie.6xlarge i7ie.12xlarge | i7ie.18xlarge | i7ie.24xlarge | i7ie.48xlarge | r5b.12xlarge | r5b.24xlarge`
- Beschleunigtes Rechnen: `dl1.24xlarge f2.6xlarge f2.12xlarge | f2.48xlarge | g5.24xlarge | g5.48xlarge | g6.24xlarge | g6.48xlarge | g6e.12xlarge | g6e.24xlarge | g6e.48xlarge | inf1.24xlarge | p3dn.24xlarge | p4d.24xlarge | p4de.24xlarge | p5.48xlarge | p5e.48xlarge | p5en.48xlarge | p6-b200.48xlarge | p6-b300.48xlarge | trn1.32xlarge | trn2.3xlarge | trn2.48xlarge | trn2a.3xlarge | trn2a.48xlarge | trn2n.3xlarge | trn2n.48xlarge | trn2p.48xlarge | trn2u.48xlarge | vt1.24xlarge`

Es kann ratsam sein, die Einstellungen für den C- bzw. P-Zustand zu ändern, um die Konsistenz der Prozessorleistung zu erhöhen, die Latenz zu reduzieren oder Ihre Instance für einen bestimmten Workload zu optimieren. Die Standardeinstellungen für den C- und P-Zustand sind auf maximale Performance ausgelegt. Dies ist für die meisten Workloads optimal. Erwägen Sie jedoch, mit den für diese Instances verfügbaren Einstellungen für den C- oder P-Zustand zu experimentieren, wenn Ihre Anwendung von einer verringerten Latenz auf Kosten von höheren Single- oder Dual-Core-Frequenzen oder von einer konsistenten Performance bei niedrigeren Frequenzen (im Gegensatz zu diskontinuierlichen Turbo Boost-Frequenzen) profitieren würde.

Informationen zu verschiedenen Prozessorkonfigurationen und dazu, wie Sie die Auswirkungen Ihrer Konfiguration für Amazon Linux überwachen können, finden Sie unter Processor State Control for

EC2 Amazon Linux Instance im Amazon Linux 2-Benutzerhandbuch. Diese Verfahren gelten für Amazon Linux und wurden dafür geschrieben. Sie funktionieren aber eventuell auch für andere Linux-Distributionen mit der Linux-Kernelversion 3.9 oder höher. Weitere Informationen zu anderen Linux-Distributionen und zur Steuerung des Prozessorzustands erhalten Sie jeweils in der Dokumentation Ihres Systems.

Verwaltete Amazon-EC2-Instances

Eine von Amazon-EC2 verwaltete Instance ist eine EC2-Instance, die von einem bestimmten Serviceanbieter wie Amazon EKS über EKS Auto Mode bereitgestellt und verwaltet wird. Verwaltete Instances bieten eine vereinfachte Möglichkeit, Datenverabeitungs-Workloads auf Amazon EC2 auszuführen, indem Sie die Betriebskontrolle der Instance an einen Serviceanbieter delegieren können.

Die delegierte Kontrolle ist die einzige Änderung, die für verwaltete Instances eingeführt wurde. Die technischen Spezifikationen und die Abrechnung bleiben dieselben wie bei nicht verwalteten EC2-Instances. Da Sie mit verwalteten Instances die Kontrolle an den Service Provider delegieren können, können Sie von der betrieblichen Expertise und den bewährten Methoden des Service Providers profitieren. Wenn eine Instance verwaltet wird, ist der Serviceanbieter für Aufgaben wie die Bereitstellung der Instance, die Konfiguration der Software, die Skalierung der Kapazität, die Behandlung von Instance-Ausfällen und -Ersetzungen und das Beenden der Instance verantwortlich.

Sie können die Einstellungen einer verwalteten Instance nicht direkt ändern und sie nicht beenden. Der Service und die spezifischen Abläufe werden durch die Vereinbarung zwischen Ihnen und dem Serviceanbieter festgelegt. Sie können jedoch Tags zu Ihren verwalteten Instances hinzufügen, ändern oder entfernen, sodass Sie sie innerhalb Ihrer AWS-Umgebung kategorisieren können.

Inhalt

- Abrechnung für verwaltete Instances
- Ermitteln verwalteter Instances
- Erste Schritte mit verwalteten Instances

Abrechnung für verwaltete Instances

Für eine verwaltete Amazon-EC2-Instance fällt dieselbe Grundgebühr an wie für eine nicht verwaltete Amazon-EC2-Instance, zuzüglich einer separaten Gebühr für den Serviceanbieter. Diese zusätzliche Gebühr wird von dem Serviceanbieter erhoben, der Ihre Instance verwaltet, und separat in Rechnung

gestellt. Sie deckt die Kosten der Services ab, die für den Betrieb und die Wartung Ihrer verwalteten Instance bereitgestellt werden.

Alle Kaufoptionen für Amazon-EC2-Instances sind für verwaltete Instances verfügbar, einschließlich On-Demand-Instances, Reserved Instances, Spot Instances und Savings Plans. Indem Sie Ihre Rechenleistung direkt von EC2 beziehen und sie dann Ihrem Serviceanbieter zur Verfügung stellen, profitieren Sie von allen vorhandenen Reserved Instances oder Savings Plans, die auf Ihr Konto angewendet werden, und stellen so sicher, dass Sie die kostengünstigste verfügbare Rechenkapazität nutzen.

Wenn Sie beispielsweise den Amazon EKS Auto Mode verwenden, zahlen Sie den standardmäßigen EC2-Instance-Tarif für die zugrunde liegenden Instances zuzüglich einer zusätzlichen Gebühr von Amazon EKS für die Verwaltung der Instances in Ihrem Namen. Wenn Sie sich dann für einen Savings Plan entscheiden, wird die EC2-Instance-Rate durch den Savings Plan reduziert, während die zusätzliche Gebühr von Amazon EKS unverändert bleibt.

Ermitteln verwalteter Instances

Verwaltete Instances werden durch einen wahren Wert im Feld Verwaltet identifiziert. Der Serviceanbieter wird im Feld Operator (in der Konsole) oder `Principal`-Feld (in der CLI) identifiziert.

Gehen Sie wie unten beschrieben vor, um die Verwalteten Instances zu identifizieren.

Console

So identifizieren Sie eine verwaltete Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus, die Sie überprüfen möchten.
4. Suchen Sie auf der Registerkarte Details (wenn Sie das Kontrollkästchen aktiviert haben) oder im Übersichtsbereich (wenn Sie die Instance-ID ausgewählt haben) das Feld Verwaltet.
   - Der Wert wahr steht für eine verwaltete Instance.
   - Der Wert falsch steht für eine nicht verwaltete Instance.
5. Wenn Verwaltet auf wahr gesetzt ist, zeigt das Feld Operator einen Wert an, der den Serviceanbieter angibt, der für die Verwaltung der Instance verantwortlich ist. Ein Wert von eks.amazonaws.com identifiziert beispielsweise Amazon EKS als Serviceanbieter.

AWS CLI

So identifizieren Sie eine verwaltete Instance

Führen Sie den Befehl describe-instances aus und geben Sie die Instance-ID an.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].Operator
```

Es folgt eine Beispielausgabe. Falls `Managed` den Wert `true` hat, ist die Instance eine verwaltete Instance und ein `Principal` ist enthalten. Der Prinzipal ist der Serviceanbieter, der die Instance verwaltet. Ein Wert von `eks.amazonaws.com` identifiziert beispielsweise Amazon EKS als Serviceanbieter.

```
[
    {
        "Managed": true,
        "Principal": "eks.amazonaws.com"
    }
]
```

So suchen Sie Ihre verwalteten Instances

Verwenden Sie den Befehl describe-instances und geben Sie den `operator.managed`-Filter mit einem Wert von `true` an. Die Option `--query` zeigt nur die IDs der verwalteten Instances an.

```
aws ec2 describe-instances \
    --filters "Name=operator.managed,Values=true" \
    --query Reservations[*].Instances[].InstanceId
```

PowerShell

So identifizieren Sie eine verwaltete Instance

Verwenden Sie das cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.Operator
```

Es folgt eine Beispielausgabe.

```
Managed Principal
------- ---------
True    eks.amazonaws.com
```

So suchen Sie Ihre verwalteten Instances

Verwenden Sie das cmdlet Get-EC2Instance. Dieses Beispiel zeigt nur die IDs der verwalteten Instances an.

```
(Get-EC2Instance -Filter @{Name="operator.managed";
 Values="true"}).Instances.InstanceId
```

Erste Schritte mit verwalteten Instances

Anleitungen zur Verwendung verwalteter Instances finden Sie unter Automatisieren der Cluster-Infrastruktur mit EKS Auto Mode im Amazon-EKS-Benutzerhandbuch.

EC2 Abrechnungs- und Kaufoptionen von Amazon

Sie können die folgenden Optionen verwenden, um Ihre Kosten für Amazon zu optimieren EC2:

- On-Demand-Instances – Sie bezahlen nach Sekunde für die gestarteten Instances.
- Savings Plans — Reduzieren Sie Ihre EC2 Amazon-Kosten, indem Sie sich für eine Laufzeit von 1 oder 3 Jahren zu einer gleichbleibenden Nutzungsdauer in USD pro Stunde verpflichten.
- Reserved Instances — Reduzieren Sie Ihre EC2 Amazon-Kosten, indem Sie sich für eine Laufzeit von 1 oder 3 Jahren zu einer konsistenten Instance-Konfiguration, einschließlich Instance-Typ und Region, verpflichten.
- Spot-Instances — Fordern Sie ungenutzte EC2 Instances an, wodurch Ihre EC2 Amazon-Kosten erheblich gesenkt werden können.
- Dedicated Hosts – Sie zahlen für einen physischen Host, der ausschließlich für Ihre Instances reserviert ist, und stellen Ihre eigenen vorhandenen Softwarelizenzen pro Socket, Kern oder VM bereit, um Kosten zu sparen.
- Dedicated Instances – Stundenweise Abrechnung für Instances, die auf Single-Tenant-Hardware ausgeführt werden.
- Kapazitätsreservierungen — Reservieren Sie Kapazität für Ihre EC2 Instances in einer bestimmten Availability Zone.

Wenn Sie sich nicht auf eine bestimmte Instance-Konfiguration festlegen können, sich aber auf einen Nutzungsbetrag festlegen können, erwerben Sie Savings Plans, um Ihre On-Demand-Instance-Kosten zu senken.Wenn Sie eine Kapazitätsreservierung benötigen, kaufen Sie Reserved Instances oder Kapazitätsreservierungen für eine bestimmte Availability Zone. Mithilfe von Kapazitätsblöcken kann ein Cluster von GPU-Instances reserviert werden. Spot-Instances sind eine kostengünstige Wahl, sofern Sie bei der Ausführung Ihrer Anwendungen zeitlich flexibel sind und Unterbrechungen verschmerzen können. Dedicated Hosts oder Dedicated Instances können Sie bei der Einhaltung von Compliance-Anforderungen unterstützen und Kosten senken, indem sie Ihre vorhandenen servergebundenen Software-Lizenzen verwenden.

Weitere Informationen finden Sie unter EC2 Amazon-Preise undVerwaltete Amazon-EC2-Instances.

On-Demand-Instances für Amazon EC2 kaufen

Mit On-Demand-Instances zahlen Sie für Rechenkapazität nach der Sekunde ohne langfristige Verpflichtungen. Sie haben vollständige Kontrolle über den Lebenszyklus der Instance. Sie entscheiden, wann sie aufgerufen, angehalten, in den Ruhezustand versetzt, neu gestartet oder beendet werden soll.

Mit dem Erwerb von On-Demand-Instances sind keine langfristigen Verpflichtungen verbunden. Sie bezahlen nur für die Sekunden, in denen sich Ihre On-Demand-Instances im Status `running` befinden, mit einem Minimum von 60 Sekunden. Der Preis pro Sekunde für eine laufende On-Demand-Instance ist festgelegt und auf der Seite Preise zu Amazon EC2, On-Demand-Preisseite aufgelistet.

Wir empfehlen, für Anwendungen mit kurzfristigen, unregelmäßigen Workloads, die nicht unterbrochen werden können, On-Demand-Instances zu verwenden.

Verwenden Sie für signifikante Einsparungen im Vergleich zu On-Demand-Instances AWS Savings Plans, Spot Instances oder Überblick über Reserved Instances für Amazon EC2.

Inhalt

- Kontingente für On-Demand-Instances
  - Überwachen von Kontingenten für On-Demand-Instances und der Nutzung
  - Anfordern einer Kontingenterhöhung
- Preise für On-Demand-Instances anfordern

Kontingente für On-Demand-Instances

Es gibt Kontigente für die Anzahl laufender On-Demand-Instances pro AWS-Konto und Region. Kontingente für On-Demand-Instances werden in Bezug auf die Anzahl der virtuellen Recheneinheiten (vCPUs) verwaltet, die Ihre laufenden On-Demand-Instances verwenden (unabhängig vom Instance-Typ). Jeder Kontingenttyp gibt die maximale Anzahl von vCPUs für eine oder mehrere Instance-Familien an.

Ihr Konto umfasst die folgenden Kontingente für On-Demand-Instances. Instances, die sich im Status Ausstehend, Beenden, Beenden und Ruhezustand befinden, werden nicht auf Ihre On-Demand-Instance-Kontingente angerechnet. Kapazitätsreservierungen werden auf On-Demand-Instance-Kontingente angerechnet, auch wenn sie ungenutzt sind.

Name	Standard	Anpassbar
Ausführen von On-Demand-DL-Instances	0	Ja
Ausführen von On-Demand-F-Instances	0	Ja
Ausführen von On-Demand-G- und VT-Instances	0	Ja
Ausführen von On-Demand-HPC-Instances	0	Ja
Ausführen von On-Demand-High–Memory-Instances	0	Ja
Ausführen von On-Demand-Inf-Instances	0	Ja
Ausführen von On-Demand-P-Instances	0	Ja
On-Demand-Ausführung von Standard-Instances (A, C, D, H, I, M, R, T, Z)	5	Ja
Ausführen von On-Demand-Trn-Instances	0	Ja
Ausführen von On-Demand-X-Instances	0	Ja

Weitere Informationen zu den unterschiedlichen Instance-Familien, Generationen und Größen finden Sie unter Leitfaden für Amazon-EC2-Instance-Typen.

Sie können jede Kombination von Instance-Typen starten, die Ihre jeweiligen Anwendungen erfüllen, sofern die Anzahl der vCPUs Ihr Kontokontingent nicht überschreitet. Beispiel: Bei einem Standard-Instance-Kontingent von 256 vCPUs könnten Sie 32 `m5.2xlarge`-Instances (32 x 8 vCPUs) oder 16 `c5.4xlarge`-Instances (16 x 16 vCPUs) starten. Weitere Informationen finden Sie unter EC2-On-Demand-Instance-Limits.

Aufgaben

- Überwachen von Kontingenten für On-Demand-Instances und der Nutzung
- Anfordern einer Kontingenterhöhung

Überwachen von Kontingenten für On-Demand-Instances und der Nutzung

Sie können Ihre Kontingent für On-Demand-Instances für die einzelnen Regionen mit den folgenden Methoden anzeigen und verwalten.

Anzeigen Ihrer aktuellen Kontingente mit der Service-Quotas-Konsole

1. Öffnen Sie die Service-Quotas-Konsole unter https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Wählen Sie auf der Navigationsleiste eine Region aus.
3. Geben Sie im Filterfeld den Wert **`On-Demand`** ein.
4. In der Spalte Angewandter Kontingentwert wird die maximale Anzahl der vCPUs für jeden Kontingenttyp der On-Demand-Instance für Ihr Konto angezeigt.

Anzeigen Ihrer aktuellen Kontingente mithilfe der AWS Trusted Advisor-Konsole

Öffnen Sie die Seite Service-Limits in der AWS Trusted Advisor-Konsole.

So konfigurieren Sie CloudWatch-Warnungen

Mit der Integration von Amazon-CloudWatch-Metriken können Sie Ihre EC2-Nutzung anhand Ihrer Kontingente überwachen. Sie können auch Alarme konfigurieren, um vor beinahe erreichten Kontingenten zu warnen. Weitere Informationen finden Sie unter Service Quotas and Amazon CloudWatch alarms (Service Quotas und Amazon-CloudWatch-Alarme) im Service-Quotas-Benutzerhandbuch.

Anfordern einer Kontingenterhöhung

Auch wenn Amazon EC2 Ihre Kontingente für On-Demand-Instances automatisch basierend auf Ihrer Nutzung erhöht, können Sie bei Bedarf eine Kontingenterhöhung anfordern. Wenn Sie beispielsweise mehr Instances starten möchten, als Ihr aktuelles Kontingent zulässt, können Sie mithilfe der Service-Quotas-Konsole wie in EC2 Amazon-Servicekontingente beschrieben eine Kontingenterhöhung beantragen.

Preise für On-Demand-Instances anfordern

Sie können die Price List Service API oder die AWS Price List API verwenden, um die Preise von On-Demand-Instances abzufragen. Weitere Informationen finden Sie unter Verwenden der AWS-Preislisten-API im Benutzerhandbuch für AWS Billing Billing and Cost Management.

Überblick über Reserved Instances für Amazon EC2

> **Important**
>
> Wir empfehlen Savings Plans gegenüber Reserved Instances. Sparpläne sind die einfachste und flexibelste Möglichkeit, Geld bei Ihren AWS-Datenverarbeitungskosten zu sparen und bieten niedrigere Preise (bis zu 72 % Rabatt auf On-Demand-Preise), genau wie Reserved Instances. Savings Plans unterscheiden sich jedoch von Reserved Instances. Bei Reserved Instances verpflichten Sie sich zu einer bestimmten Instance-Konfiguration. Bei Savings Plans erhalten Sie die Flexibilität, die Instance-Konfigurationen zu nutzen, die Ihren Anforderungen am besten entsprechen. Mit Savings Plans können Sie sich auf einen gleichbleibenden Nutzungsbetrag (in USD pro Stunde) festlegen. Weitere Informationen finden Sie im AWS Savings Plans User Guide.

Reserved Instances bieten Ihnen deutlich reduzierte Amazon EC2-Kosten im Vergleich zu den Preisen für On-Demand-Instances. Bei Reserved-Instances handelt es sich nicht um physische Instances, sondern um einen Fakturierungsrabatt für die Nutzung gewisser On-Demand-Instances in Ihrem Konto. Diese On-Demand-Instances müssen verschiedenen Attributen wie Instance-Typ und Region entsprechen, um vom Fakturierungsrabatt zu profitieren.

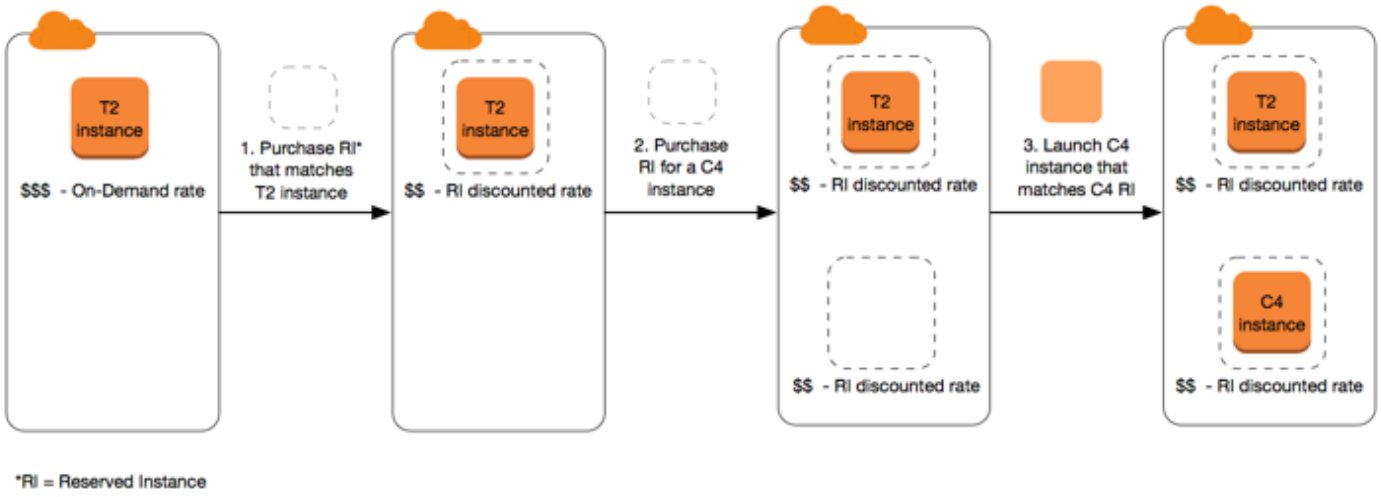
Themen für Reserved Instances

- Beispielszenario für Reserved Instances
- Schlüsselvariablen zur Bestimmung der Reserved Instance-Preise

- Regionale und zonengebundene Reserved Instances (Umfang)
- Reserved Instances-Typen (Angebotsklassen)
- Wie Reserved-Instances-Rabatte angewendet werden
- Nutzen Ihres Reserved Instances
- Wie die Abrechnung mit Reserved Instances funktioniert
- Reserved-Instances für Amazon EC2 erwerben
- Reserved Instances für Amazon EC2 auf dem Reserved Instance Marketplace verkaufen
- Ändern von Reserved Instances
- Austauschen von Convertible Reserved Instances
- Kontingente für Reserved Instances

Beispielszenario für Reserved Instances

Das folgende Diagramm zeigt ein grundlegendes Szenario zum Kauf und zur Nutzung von Reserved Instances.



In diesem Szenario verfügen Sie über eine aktive On-Demand-Instance (T2) in Ihrem Konto. Für diese zahlen Sie zurzeit die On-Demand-Tarife. Sie erwerben eine den Attributen Ihrer aktiven Instance entsprechende Reserved Instance und erhalten einen sofortigen Preisvorteil. Als Nächstes erwerben Sie eine Reserved Instance für eine C4-Instance. In Ihrem Konto sind keine aktiven Instances vorhanden, die den Attributen dieser Reserved Instance entsprechen. Als Letztes starten Sie eine Instance, die den Attributen der C4-Reserved Instance entspricht, und Sie erhalten einen sofortigen Preisvorteil.

Schlüsselvariablen zur Bestimmung der Reserved Instance-Preise

Die Reserved Instance-Preise werden anhand der folgenden Schlüsselvariablen bestimmt.

Instance-Attribute

Eine Reserved Instance hat vier Instance-Attribute, von denen ihr Preis abhängig ist.

- Instance-Typ: Beispielsweise `m4.large`. Dieser besteht aus der Instance-Familie (z. B. `m4`) und der Instance-Größe (z. B. `large`).
- Region: Die Region, in der das Reserved Instance gekauft wird.
- Tenancy: Ob die Instance auf gemeinsam genutzter Hardware (Standard) oder auf Single–Tenant-Hardware (dediziert) ausgeführt wird. Weitere Informationen finden Sie unter Amazon-EC2-Dedicated-Instances.
- Plattform: Das Betriebssystem (z. B. Windows oder Linux/Unix). Weitere Informationen finden Sie unter Wählen einer Plattform.

Dauerhafte Verpflichtung

Sie können eine Reserved Instance für eine ein- oder dreijährige Laufzeit erwerben, wobei für die dreijährige Laufzeitverpflichtung ein größerer Rabatt angeboten wird.

- Ein Jahr: Ein Jahr wird als 31536000 Sekunden (365 Tage) definiert.
- Drei Jahre: Drei Jahre werden als 94608000 Sekunden (1095 Tage) definiert.

Reserved Instances werden nicht automatisch verlängert. Wenn sie auslaufen, können Sie ohne jegliche Unterbrechung die EC2-Instance weiter nutzen. In diesem Fall werden jedoch die On-Demand-Tarife berechnet. Wenn die Reserved Instances für die T2- und C4-Instances im Beispiel oben auslaufen, zahlen Sie bis zur Beendigung der Instances oder dem Kauf neuer Reserved Instances mit den passenden Instance-Attributen wieder die On-Demand-Tarife.

> **Important**
>
> Der Kauf einer Reserved Instance kann nicht storniert werden. Sollten sich Ihre Anforderungen ändern, können Sie Ihre Reserved Instance jedoch möglicherweise ändern, austauschen oder verkaufen.

Zahlungsoptionen

Für Reserved Instances stehen folgende Zahlungsoptionen zur Verfügung:

- Komplette Vorauszahlung: Die gesamte Zahlung wird zum Anfang der Laufzeit durchgeführt. Es entstehen keine weiteren Kosten und es werden für die gesamte Laufzeit keine weiteren Stundensätze berechnet (unabhängig von den genutzten Stunden).
- Teilweise Vorauszahlung: Ein Teil der Kosten muss im Voraus bezahlt werden und die restlichen Stunden während der Laufzeit werden zu einem ermäßigten Stundensatz abgerechnet (unabhängig von der Nutzung der Reserved Instance).
- Keine Vorauszahlung: Sie zahlen einen ermäßigten Stundensatz für jede Stunde im Rahmen der Laufzeit (unabhängig davon, ob die Reserved Instance genutzt wird). Es ist keine Vorauszahlung erforderlich.

> **Note**
>
> Reserved Instances ohne Vorauszahlung arbeiten mit einer vertraglichen Verpflichtung zur monatlichen Zahlung über die gesamte Laufzeit hinweg. Aus diesem Grund benötigen Sie einen positiven Abrechnungsverlauf, bevor Sie Reserved Instances ohne Vorauszahlung erwerben können.

Im Allgemeinen sparen Sie durch eine größere Vorauszahlung für Reserved Instances mehr Geld. Im Reserved Instance Marketplace werden Reserved Instances von Drittanbietern zu günstigeren Preisen und mit kürzeren Laufzeiten angeboten. Weitere Informationen finden Sie unter Reserved Instances für Amazon EC2 auf dem Reserved Instance Marketplace verkaufen.

Angebotsklasse

Wenn sich Ihre Anforderungen ändern, können Sie Ihre Reserved Instance jedoch ändern oder austauschen (je nach Angebotsklasse).

- Standard: Diese Klasse bietet den signifikantesten Rabatt, kann aber nur geändert werden. Standard Reserved Instances kann nicht ausgetauscht werden.
- Convertible: Diese Klasse bietet einen geringeren Rabatt als Standard-Reserved Instances, kann aber gegen eine andere Convertible Reserved Instance mit anderen Instance-Attributen ausgetauscht werden. Convertible Reserved Instances können auch geändert werden.

Weitere Informationen finden Sie unter Reserved Instances-Typen (Angebotsklassen).

> **Important**
>
> Der Kauf einer Reserved Instance kann nicht storniert werden. Sollten sich Ihre Anforderungen ändern, können Sie Ihre Reserved Instance jedoch möglicherweise ändern, austauschen oder verkaufen.

Weitere Informationen finden Sie auf der Seite Preise für Amazon EC2 Reserved Instances.

Regionale und zonengebundene Reserved Instances (Umfang)

Bei dem Erwerb einer Reserved Instance legen Sie den Geltungsbereich der Reserved Instance fest. Der Umfang ist entweder regional oder zonengebunden.

- Regional: Wenn Sie eine Reserved Instance für eine Region erwerben, wird sie als regionale Reserved Instance bezeichnet.
- Zonengebunden: Wenn Sie eine Reserved Instance für eine bestimmte Availability Zone erwerben, wird sie als zonengebundene Reserved Instance bezeichnet.

Der Umfang hat keinen Einfluss auf den Preis. Sie zahlen den gleichen Preis für regionale oder zonengebundene Reserved Instance. Weitere Informationen zu Preisen Reserved Instance erhalten Sie unter Schlüsselvariablen zur Bestimmung der Reserved Instance-Preise und Preise für Amazon-EC2-Reserved-Instances.

Weitere Informationen darüber, wie Sie den Geltungsbereich einer Reserved Instance festlegen können, finden Sie unter RI-Attribute, insbesondere unter dem Aufzählungspunkt Availability Zone.

Unterschiede zwischen regionalen und zonengebundenen Reserved Instances

Die folgende Tabelle hebt einige der wichtigsten Unterschiede zwischen regionalen Reserved Instances und zonengebundenen Reserved Instances hervor:

	Regionsgebundene Reserved Instances	Zonengebundene Reserved Instances
Fähigkeit zum Reservieren von Kapazität		Ein zonaler Reserved Instance reserviert Kapazität in der

	Regionsgebundene Reserved Instances	Zonengebundene Reserved Instances
	Ein regionaler Reserved Instance reserviert keine Kapazität.	angegebenen Availability Zone.
Flexibilität bezüglich der Availability Zone	Der Reserved Instance-Rabatt gilt für die Instance-Nutzung in jeder Availability Zone in der angegebenen Region.	Keine Flexibilität bezüglich der Availability Zone – Der Reserved Instance-Rabatt gilt nur für die Instance-Nutzung in der angegebenen Availability Zone.
Flexibilität bezüglich der Instance-Größe	Der Reserved Instance-Rabatt gilt unabhängig von der Größe für die Instance-Nutzung in der Instance-Familie. Wird nur für Reserved Instances der Amazon Linux/ Unix-Plattform mit Standard-Tenancy unterstützt. Weitere Informationen finden Sie unter Flexibilität bezüglich der Instance-Größe anhängig vom Normalisierungsfaktor.	Keine Flexibilität bezüglich der Instance-Größe – Der Reserved Instance-Rabatt gilt nur für die Instance-Nutzung für die angegebene Kombinati on aus Instance-Typ und -Größe.
Einen Kauf in die Warteschl ange stellen	Sie können Käufe für regionale Reserved Instances in Warteschlange stellen	Sie können Käufe für zonengebundene Reserved Instances nicht in Warteschl ange stellen.

Weitere Informationen und Beispiele finden Sie unter Wie Reserved-Instances-Rabatte angewendet werden.

Reserved Instances-Typen (Angebotsklassen)

Die Angebotsklasse von Reserved Instance ist entweder Standard oder Convertible. Ein Standard-Reserved-Instance bietet einen größeren Rabatt als ein Convertible-Reserved-Instance, aber Sie können keinen Standard-Reserved-Instance umtauschen. Sie können Convertible-Reserved Instances wechseln. Sie können Standard- und Convertible-Reserved Instances ändern.

Die Konfiguration eines Reserved Instance umfasst einen einzelnen Instance-Typ, eine Plattform, einen Umfang und eine Tenancy über eine Laufzeit. Wenn sich Ihre Anforderungen ändern, können Sie Ihre Reserved Instance jedoch ändern oder austauschen.

Unterschiede zwischen Standard- und Convertible-Reserved Instances

Die folgenden Unterschiede gelten zwischen den Standard- und Convertible-Reserved Instances.

	Standard-Reserved Instance	Convertible Reserved Instance
Ändern von Reserved Instances	Einige Attribute können geändert werden. Weitere Informationen finden Sie unter Ändern von Reserved Instances.	Einige Attribute können geändert werden. Weitere Informationen finden Sie unter Ändern von Reserved Instances.
Reserved Instances auswechseln	Kann nicht ausgetauscht werden.	Kann während der Laufzeit gegen eine andere Convertible Reserved Instance mit neuen Attributen inkl. Instance-Familie, Instance-Typ, Plattform, Umfang und Tenancy ausgetauscht werden. Weitere Informationen finden Sie unter Austausch en von Convertible Reserved Instances.
Verkaufen im Reserved Instance Marketplace	Kann im Reserved Instance Marketplace verkauft werden.	Kann nicht im Reserved Instance Marketplace verkauft werden.

	Standard-Reserved Instance	Convertible Reserved Instance
Einkaufen im Reserved Instance Marketplace	Kann im Reserved Instance Marketplace gekauft werden.	Kann nicht im Reserved Instance Marketplace gekauft werden.

Wie Reserved-Instances-Rabatte angewendet werden

Reserved Instances sind keine physischen Instances, sondern ein Abrechnungsrabatt, der auf die laufenden On-Demand-Instances in Ihrem Konto angewendet wird. Die On-Demand-Instances müssen bestimmten Spezifikationen der Reserved Instances entsprechen, damit der Abrechnungsrabatt angewendet werden kann.

Wenn Sie eine Reserved Instance erwerben und bereits über eine laufende On-Demand-Instance verfügen, die den Spezifikationen der Reserved Instance entspricht, wird der Abrechnungsrabatt sofort und automatisch angewendet. Sie müssen Ihre Instances nicht neu starten. Wenn Sie über keine berechtigte On-Demand-Instance verfügen, starten Sie eine On-Demand-Instance mit denselben Spezifikationen wie Ihre Reserved Instance. Weitere Informationen finden Sie unter Nutzen Ihres Reserved Instances.

Die Angebotsklasse (Standard oder Convertible) der Reserved Instance hat keinen Einfluss darauf, wie der Abrechnungsrabatt angewendet wird.

Themen

- So werden zonengebundene Reserved Instances angewendet
- So werden regionale Reserved Instances angewendet
- Flexibilität bezüglich der Instance-Größe
- Beispiele zur Anwendung von Reserved Instances

So werden zonengebundene Reserved Instances angewendet

Eine Reserved Instance, die gekauft wird, um Kapazität in einer bestimmten Availability Zone zu reservieren, wird als zonengebundene Reserved Instance bezeichnet.

- Der Reserved-Instance-Rabatt gilt für die übereinstimmende Instance-Nutzung in dieser Availability Zone.

- Die Attribute (Tenancy, Plattform, Availability Zone, Instance-Typ und Instance-Größe) der aktiven Instances müssen denen der Reserved Instances entsprechen.

Wenn Sie beispielsweise zwei `c4.xlarge` Standard-Tenancy Linux/Unix Standard Reserved Instances in der Availability Zone „us-east-1a“ erwerben, kann der Reserved-Instance-Rabatt auf bis zu zwei aktive `c4.xlarge` Standard-Tenancy Linux/Unix-Instances in der Availability Zone „us-east-1a“ angewendet werden.

So werden regionale Reserved Instances angewendet

Eine für eine Region erworbene Reserved Instance wird als regionale Reserved Instance bezeichnet und bietet Flexibilität in Bezug auf die Instance-Größe und Availability Zone.

- Der Reserved Instance-Rabatt gilt für die Instance-Nutzung in jeder Availability Zone in dieser Region.
- Der Reserved-Instance-Rabatt gilt für die Instance-Nutzung innerhalb der Instance-Familie, unabhängig von der Größe – dies wird als Instance-Größenflexibilität bezeichnet.

Flexibilität bezüglich der Instance-Größe

Bei flexibler Instance-Größe gilt der Rabatt für Reserved Instances für die Nutzung von Instances, die dieselbe Familie haben. Die Reserved Instance wird basierend auf dem Normalisierungsfaktor innerhalb der Instance-Familie von der kleinsten bis hin zur größten Instance-Größe angewendet. Ein Beispiel für die Anwendung des Reserved-Instance-Rabatts finden Sie unter Szenario 2: Reserved Instances in einem einzigen Konto unter Anwendung des Normalisierungsfaktors.

Einschränkungen

- Unterstützt: Die Flexibilität der Instance-Größe wird nur für regionale Reserved Instances unterstützt.
- Nicht unterstützt: Die Flexibilität der Instance-Größe wird für die folgenden Reserved Instances nicht unterstützt:
  - Reserved Instances, die für eine bestimmte Availability Zone erworben werden (zonengebundene Reserved Instances)
  - Reserved Instances für G4ad, G4dn, G5, G5g, G6, G6e, G6f, Gr6, Gr6f, hpc7a, P5, Inf1, Inf2, u7i-6tb und u7i-8tb-Instances

- Reserved Instances für Windows Server, Windows Server mit SQL Standard, Windows Server mit SQL Server Enterprise, Windows Server mit SQL Server Web, RHEL und SUSE Linux Enterprise Server
- Reserved Instances mit Dedicated Tenancy

Flexibilität bezüglich der Instance-Größe anhängig vom Normalisierungsfaktor

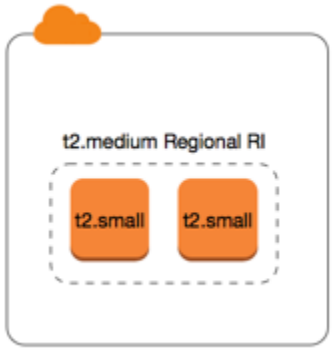
Die flexible Instance-Größe wird durch den Normalisierungsfaktor der Instance-Größe bestimmt. Der Rabatt gilt für aktive Instances derselben Instance-Familie Typs in jeder Availability Zone der Region entweder vollständig oder teilweise. Dies hängt von der Instance-Größe der Reservierung ab. Nur die Attribute Instance-Familie, Tenancy und Plattform müssen übereinstimmen.

In der folgenden Tabelle sind die unterschiedlichen Größen innerhalb einer Instance-Familie und der entsprechende Normalisierungsfaktor aufgeführt. Diese Maßeinheit wird zur Anwendung des Rabatts für Reserved Instances auf die normalisierte Nutzung des Instance-Familie genutzt.

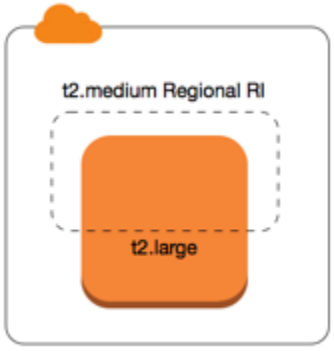
Instance-Größe	Normalisierungsfaktor
nano	0,25
micro	0.5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64

Instance-Größe	Normalisierungsfaktor
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448
112xlarge	896

Eine `t2.medium`-Instance hat beispielsweise einen Normalisierungsfaktor von 2. Wenn Sie eine `t2.medium` Standard-Tenancy Amazon Linux/Unix Reserved Instance in US East (N. Virginia) erwerben, und in der Region über zwei aktive `t2.small` Instances in Ihrem Konto verfügen, wird der Rabatt voll auf beide Instances angewendet.



Wenn Sie über eine `t2.large`-Instance in der Region USA Ost (Nord-Virginia) in Ihrem Konto verfügen, wird der Rabatt zu 50 % auf die Nutzung der Instance angewendet.



Der Normalisierungsfaktor wird auch angewendet, wenn Sie Reserved Instances ändern. Weitere Informationen finden Sie unter Ändern von Reserved Instances.

Normalisierungsfaktor für Bare Metal-Instances

Flexibilität bezüglich der Instance-Größe gilt auch für Bare Metal-Instances in der Instance-Familie. Bei regionalen Amazon Linux/Unix-Reserved Instances mit geteilter Tenancy für Bare Metal-Instances können Sie von den Reserved Instance-Einsparungen in derselben Instance-Familie profitieren. Dies gilt auch umgekehrt. Bei regionalen Amazon Linux/Unix-Reserved Instances mit geteilter Tenancy für Instances in derselben Familie wie eine Bare Metal-Instance können Sie von den Reserved Instance-Einsparungen für die Bare Metal-Instance profitieren.

Die `metal`-Instance-Größe besitzt keinen einzigen Normalisierungsfaktor. Eine Bare Metal-Instance hat den gleichen Normalisierungsfaktor wie die entsprechende virtualisierte Instance-Größe innerhalb derselben Instance-Familie. Beispielsweise hat eine `i3.metal`-Instance den gleichen Normalisierungsfaktor wie eine `i3.16xlarge`-Instance.

Instance-Größe	Normalisierungsfaktor
`a1.metal`	32
`m5zn.metal` | `x2iezn.metal` `z1d.metal`	96
`c6g.metal` | `c6gd.metal` | `i3.metal` | `m6g.metal` | `m6gd.metal` | `r6g.metal` | `r6gd.metal` | `x2gd.metal`	128
`c5n.metal`	144

Instance-Größe	Normalisierungsfaktor
c5.metal| c5d.metal | i3en.metal | m5.metal| m5d.metal | m5dn.metal | m5n.metal | r5.metal| r5b.metal | r5d.metal | r5dn.metal | r5n.metal	192
c6i.metal |c6id.metal |m6i.metal |m6id.metal |r6d.metal |r6id.metal	256
u-18tb1.metal |u-24tb1.metal	448
u-6tb1.metal |u-9tb1.metal |u-12tb1.metal	896

Beispiel: Eine `i3.metal`-Instance hat beispielsweise einen Normalisierungsfaktor von 128. Wenn Sie eine `i3.metal`-Reserved Instance der Amazon Linux/Unix-Plattform mit Standard-Tenancy in der Region US East (N. Virginia) erwerben, kann der Rabatt wie folgt angewendet werden:

- Wenn Sie in Ihrem Konto in dieser Region über eine aktive `i3.16xlarge`-Instance verfügen, wird der Rabatt voll auf die `i3.16xlarge`-Instance (`i3.16xlarge`-Normalisierungsfaktor = 128) angewendet.
- Oder wenn Sie in Ihrem Konto in dieser Region über zwei aktive `i3.8xlarge`-Instances verfügen, wird der Rabatt voll auf beide `i3.8xlarge`-Instances (`i3.8xlarge`-Normalisierungsfaktor = 64) angewendet.
- Oder wenn Sie in Ihrem Konto in dieser Region über vier aktive `i3.4xlarge`-Instances verfügen, wird der Rabatt voll auf alle vier `i3.4xlarge`-Instances (`i3.4xlarge`-Normalisierungsfaktor = 32) angewendet.

Dies gilt auch umgekehrt. Wenn Sie z. B. zwei `i3.8xlarge`-Reserved Instances auf der Amazon Linux/Unix-Plattform mit Standard-Tenancy in der Region US East (N. Virginia) erwerben und bereits über eine aktive `i3.metal`-Instance in dieser Region verfügen, wird der Rabatt voll auf die `i3.metal`-Instance angewendet.

Beispiele zur Anwendung von Reserved Instances

Die folgenden Szenarien decken die Anwendungsmöglichkeiten von Reserved Instances ab.

- Szenario 1: Reserved Instances in einem einzigen Konto

- Szenario 2: Reserved Instances in einem einzigen Konto unter Anwendung des Normalisierungsfaktors
- Szenario 3: Regionale Reserved Instances in verknüpften Konten
- Szenario 4: Zonenbasierte Reserved Instances in einem verknüpften Konto

Szenario 1: Reserved Instances in einem einzigen Konto

Sie führen die folgenden On-Demand-Instances in Konto A aus:

- 4 x `m3.large` Linux, Standard-Tenancy-Instances in Availability Zone us-east-1a
- 2 x `m4.xlarge` Amazon Linux, Standard-Tenancy-Instances in Availability Zone us-east-1b
- 1 x `c4.xlarge` Amazon Linux, Standard-Tenancy-Instances in Availability Zone us-east-1c

Sie erwerben die folgenden Reserved Instances in Konto A:

- 4 x `m3.large` Linux, Standard-Tenancy Reserved Instances in Availability Zone us-east-1a (Kapazität ist reserviert)
- 4 x `m4.large` Amazon Linux, Standard-Tenancy Reserved Instances in der Region us-east-1
- 1 x `c4.large` Amazon Linux, Standard-Tenancy Reserved Instances in der Region us-east-1

Die Reserved Instance-Rabatte werden folgendermaßen angewendet:

- Da die Attribute (Instance-Größe, Region, Plattform, Tenancy) übereinstimmen, werden der Rabatt und die Kapazitätsreservierung der vier `m3.large` Zonen-Reserved Instances für die vier `m3.large` Instances genutzt.
- Die regionalen `m4.large` Reserved Instances bieten eine Flexibilität für die Availability Zone und die Instance-Größe. Sie sind regionale Amazon Linux Reserved Instances mit Standard-Tenancy.

  Eine `m4.large` entspricht 4 normalisierten Einheiten/Stunde.

  Sie haben vier regionale `m4.large` Reserved Instances erworben. Insgesamt entsprechen diese 16 normalisierten Einheiten/Stunde (4x4). Konto A verfügt über zwei aktive `m4.xlarge` Instances. Dies entspricht 16 normalisierten Einheiten/Stunde (2x8). In diesem Fall sorgen die vier regionalen `m4.large`-Reserved-Instances für den vollständigen Rabatt für die Nutzung der zwei `m4.xlarge`-Instances.

- Die regionale `c4.large` Reserved Instance in us-east-1 bietet eine Flexibilität für die Availability Zone und die Instance-Größe, denn sie ist eine regionale Amazon Linux Reserved Instance mit Standard-Tenancy und wird auf die `c4.xlarge` Instance angewendet. Eine `c4.large` Instance entspricht 4 normalisierten Einheiten/Stunde und eine `c4.xlarge` entspricht 8 normalisierten Einheiten/Stunde.

  In diesem Fall wird die regionale `c4.large` Reserved Instance teilweise auf die `c4.xlarge`-Nutzung angewendet. Dies liegt daran, dass die `c4.large` Reserved Instance der Nutzung von 4 normalisierten Einheiten/Stunde entspricht, die `c4.xlarge` Instance jedoch 8 normalisierte Einheiten/Stunde erfordert. Aus diesem Grund wird der Rabatt durch die `c4.large` Reserved Instance nur zu 50 % auf die `c4.xlarge`-Nutzung angewendet. Die verbleibende `c4.xlarge`-Nutzung wird über den On-Demand-Tarif abgerechnet.

Szenario 2: Reserved Instances in einem einzigen Konto unter Anwendung des Normalisierungsfaktors

Sie führen die folgenden On-Demand-Instances in Konto A aus:

- 2 x `m3.xlarge` Amazon Linux, Standard-Tenancy-Instances in Availability Zone us-east-1a
- 2 x `m3.large` Amazon Linux, Standard-Tenancy-Instances in Availability Zone us-east-1b

Sie erwerben die folgende Reserved Instance in Konto A:

- 1 x `m3.2xlarge` Amazon Linux, Standard-Tenancy-Reserved-Instance in der Region us-east-1

Die Reserved Instance-Rabatte werden folgendermaßen angewendet:

- Die `m3.2xlarge` regionale Reserved Instance in us-east-1 bietet Flexibilität in Bezug auf die Availability Zone und die Instance-Größe, denn es handelt sich um eine regionale Amazon-Linux-Reserved-Instance mit Standard-Tenancy. Sie wird zunächst auf die `m3.large`-Instances und dann auf die `m3.xlarge`-Instances angewendet, da die Anwendung innerhalb der Instance-Familie basierend auf dem Normalisierungsfaktor von der kleinsten bis zur größten Instance-Größe erfolgt.

  Eine `m3.large`-Instance entspricht 4 normalisierten Einheiten/Stunde.

  Eine `m3.xlarge`-Instance entspricht 8 normalisierten Einheiten/Stunde.

Eine `m3.2xlarge`-Instance entspricht 16 normalisierten Einheiten/Stunde.

Der Rabatt wird wie folgt angewendet:

Die `m3.2xlarge` regionale Reserved Instance bietet den vollständigen Rabatt für 2 x `m3.large` Nutzung, da diese beiden Instances zusammen 8 normalisierten Einheiten/Stunde entsprechen. Damit verbleiben 8 normalisierte Einheiten/Stunde, die auf die `m3.xlarge`-Instances angewendet werden.

Mit den verbleibenden 8 normalisierten Einheiten/Stunde wendet die `m3.2xlarge` regionale Reserved Instance den vollständigen Rabatt auf 1 x `m3.xlarge` Nutzung an, da jede `m3.xlarge` Instance 8 normalisierten Einheiten/Stunde entspricht. Die verbleibende `m3.xlarge`-Nutzung wird über den On-Demand-Tarif abgerechnet.

Szenario 3: Regionale Reserved Instances in verknüpften Konten

Reserved Instances werden zuerst auf die Nutzung im erwerbenden Konto angewendet. Danach folgt die qualifizierte Nutzung in anderen Konten der Organisation. Weitere Informationen finden Sie unter Reserved Instances- und konsolidierte Fakturierung. Bei regionalen Reserved Instances, die Größenflexibilität für Instances anbieten, wird der Vorteil innerhalb der Instance-Familie von der kleinsten bis hin zur größten Instance-Größe angewendet.

Sie führen die folgenden On-Demand-Instances in Konto A (das erwerbende Konto) aus:

- 2 x `m4.xlarge` Linux, Standard-Tenancy-Instances in Availability Zone us-east-1a
- 1 x `m4.2xlarge` Linux, Standard-Tenancy-Instances in Availability Zone us-east-1b
- 2 x `c4.xlarge` Linux, Standard-Tenancy-Instances in Availability Zone us-east-1a
- 1 x `c4.2xlarge` Linux, Standard-Tenancy-Instances in Availability Zone us-east-1b

Ein weiterer Kunde führt die folgenden On-Demand-Instances in Konto B— (ein verknüpftes Konto) aus:

- 2 x `m4.xlarge` Linux, Standard-Tenancy-Instances in Availability Zone us-east-1a

Sie erwerben die folgenden regionalen Reserved Instances in Konto A:

- 4 x `m4.xlarge` Linux, Standard-Tenancy Reserved Instances in der Region us-east-1

- 2 x `c4.xlarge` Linux, Standard-Tenancy Reserved Instances in der Region us-east-1

Die regionalen Reserved Instance-Rabatte werden folgendermaßen angewendet:

- Der Rabatt der vier `m4.xlarge`-Reserved Instances wird von den beiden `m4.xlarge`-Instances und der einzelnen `m4.2xlarge`-Instance in Konto A (dem erwerbenden Konto) genutzt. Alle drei Instance entsprechen den Attributen (Instance-Familie, Region, Plattform, Tenancy). Der Rabatt wird zuerst auf die Instances im erwerbenden Konto (Konto A) angewendet, obwohl Konto B (verknüpftes Konto) über zwei `m4.xlarge` verfügt, dem den Reserved Instances ebenfalls entsprechen. Es wird keine Kapazitätsreservierung geboten, da es sich bei den Reserved Instances um regionale Reserved Instances handelt.
- Der Rabatt auf die zwei `c4.xlarge` Reserved Instances wird auf die zwei `c4.xlarge` Instances angewendet, da ihre Instance-Größe kleiner als die der `c4.2xlarge` Instance ist. Es wird keine Kapazitätsreservierung geboten, da es sich bei den Reserved Instances um regionale Reserved Instances handelt.

Szenario 4: Zonenbasierte Reserved Instances in einem verknüpften Konto

Reserved Instances im Besitz eines Kontos werden grundsätzlich erst auf die Nutzung in diesem Konto angewendet. Wenn es qualifizierende und nicht genutzte Reserved Instances für eine bestimmte Availability Zone (zonenbasierte Reserved Instances) in anderen Konten in der Organisation gibt, werden diese vor den regionalen Reserved Instances im Besitz des Kontos auf das Konto angewendet. Dies geschieht, um eine maximale Nutzung der Reserved Instances und somit eine geringere Rechnung zu gewährleisten. Zu Fakturierungszwecken werden alle Konten in der Organisation wie ein einziges Konto behandelt. Das folgende Beispiel veranschaulicht dies.

Sie führen die folgenden On-Demand-Instance in Konto A (das erwerbende Konto) aus:

- 1 x `m4.xlarge` Linux, Standard-Tenancy-Instance in Availability Zone us-east-1a

Ein Kunde führt die folgende On-Demand-Instance im verknüpften Konto B aus:

- 1 x `m4.xlarge` Linux, Standard-Tenancy-Instance in Availability Zone us-east-1b

Sie erwerben die folgenden regionalen Reserved Instances in Konto A:

- 1 x `m4.xlarge` Linux, Standard-Tenancy Reserved Instance in der Region us-east-1

Ein Kunde erwirbt die folgenden zonenbezogenen Reserved Instances im verknüpften Konto C:

- 1 x `m4.xlarge` Linux, Standard-Tenancy-Reserved Instances in Availability Zone us-east-1a

Die Reserved Instance-Rabatte werden folgendermaßen angewendet:

- Der Rabatt der zonenbezogenen `m4.xlarge` Reserved Instances im Besitz von Konto C wird auf die `m4.xlarge`-Nutzung in Konto A angewendet.
- Der Rabatt der regionalen `m4.xlarge` Reserved Instances im Besitz von Konto A wird auf die `m4.xlarge`-Nutzung in Konto B angewendet.
- Wenn die regionale Reserved Instance im Besitz von Konto A zuerst auf die Nutzung in Konto A angewendet wurde, bleibt die zonenbezogene Reserved Instance im Besitz von Konto C ungenutzt und die Nutzung in Konto B wird zum On-Demand-Tarif abgerechnet.

Weitere Informationen finden Sie unter Ihre Reservierungen verstehen im AWS Cost and Usage Report.

> **Note**
>
> Zonal Reserved Instances reservieren Kapazität nur für das Besitzerkonto und können nicht für andere AWS-Konten freigegeben werden. Wenn Sie Kapazität für andere AWS-Konten freigeben müssen, verwenden Sie Reservieren Sie Rechenkapazität mit Kapazitätsreservierungen EC2 auf Abruf.

Nutzen Ihres Reserved Instances

Reserved Instances werden bei übereinstimmenden Spezifikationen automatisch auf aktive On-Demand-Instances angewendet. Wenn Sie über keine On-Demand-Instances mit passenden Spezifikationen Ihrer Reserved Instance verfügen, bleibt die Reserved Instance bis zum Start einer Instance mit den erforderlichen Spezifikationen ungenutzt.

Wenn Sie eine On-Demand-Instance starten, um den Abrechnungsrabatt einer Reserved Instance zu nutzen, stellen Sie sicher, dass Sie bei der Konfiguration Ihrer On-Demand-Instance die folgenden Informationen angeben:

Plattform

Sie müssen ein Amazon Machine Image (AMI) angeben, das der Plattform (Produktbeschreibung) der Reserved Instance entspricht. Wenn Sie beispielsweise `Linux/UNIX` für Ihre Reserved Instance angegeben haben, können Sie eine Instance von einem Amazon Linux AMI oder einem Ubuntu AMI starten.

Instance-Typ

Wenn Sie eine zonengebundene Reserved Instance erworben haben, müssen Sie denselben Instance-Typ wie Ihre Reserved Instance angeben; zum Beispiel ., `t3.large`. Weitere Informationen finden Sie unter So werden zonengebundene Reserved Instances angewendet.

Wenn Sie eine regionale Reserved Instance erworben haben, müssen Sie einen Instance-Typ aus derselben Instance-Familie wie der Instance-Typ Ihrer Reserved Instance angeben. Wenn Sie beispielsweise `t3.xlarge` für Ihre Reserved Instance angegeben haben, müssen Sie Ihre Instance aus der T3-Familie starten, können aber eine beliebige Größe angeben, beispielsweise `t3.medium`. Weitere Informationen finden Sie unter So werden regionale Reserved Instances angewendet.

Availability Zone

Wenn Sie eine zonengebundene Reserved Instance für eine bestimmte Availability Zone erworben haben, müssen Sie die Instance in derselben Availability Zone starten.

Wenn Sie eine regionale Reserved Instance erworben haben, können Sie die Instance in jeder Availability Zone in der Region starten, die Sie für die Reserved Instance angegeben haben.

Tenancy

Die Tenancy (`dedicated` oder `shared`) der Instance muss mit der Tenancy Ihrer Reserved Instance übereinstimmen. Weitere Informationen finden Sie unter Amazon-EC2-Dedicated-Instances.

Beispiele zur Anwendung von Reserved Instances auf aktive On-Demand-Instances finden Sie unter Wie Reserved-Instances-Rabatte angewendet werden. Weitere Informationen finden Sie unter Warum werden meine Amazon EC2 Reserved Instances nicht wie erwartet auf meine AWS-Abrechnung angewendet?

Sie können verschiedene Methoden verwenden, um die On-Demand-Instances zu starten, die Ihren Reserved-Instance-Rabatt verwenden. Weitere Informationen zu den verschiedenen Startmethoden

finden Sie unter Starten Sie eine EC2 Amazon-Instance. Sie können auch Amazon EC2 Auto Scaling verwenden, um eine Instance zu starten. Weitere Informationen hierzu finden Sie im Amazon EC2 Auto Scaling-Benutzerhandbuch.

Wie die Abrechnung mit Reserved Instances funktioniert

Alle Reserved Instances bieten im Vergleich mit den Preisen für On-Demand-Instances einen Rabatt. Mit Reserved Instances zahlen Sie für die gesamte Laufzeit statt für die tatsächliche Nutzung. Je nach der für die Reserved Instance festgelegten Zahlungsoption bezahlen Sie die Reserved Instance im Voraus, teilweise im Voraus oder monatlich.

Wenn Reserved Instances ausläuft, zahlen Sie On-Demand-Tarife für eine Nutzung der EC2-Instance. Sie können eine Reserved Instance bis zu drei Jahre im Voraus für den Kauf in die Warteschlange einstellen. So können Sie sicherstellen, dass jederzeit die erforderlichen Kapazitäten verfügbar sind. Weitere Informationen finden Sie unter Einstellen des Kaufs in die Warteschlange.

Das Kostenloses AWS-Kontingent ist für AWS-Konten verfügbar. Wenn Sie das Kostenloses AWS-Kontingent zur Ausführung von Amazon-EC2-Instances nutzen und eine Reserved Instance erwerben, erfolgt die Abrechnung nach den Standard-Preisrichtlinien. Weitere Informationen finden Sie unter Kostenloses AWS-Kontingent.

Inhalt

- Nutzungsabrechnung
- Anzeigen Ihrer Rechnung
- Reserved Instances- und konsolidierte Fakturierung
- Reserved Instance-Rabatt-Preisstufen

Nutzungsabrechnung

Während der gewählten Laufzeit werden Reserved Instances jeweils zur vollen Stunde abgerechnet – unabhängig davon, ob eine Instance ausgeführt wird. Eine volle Stunde wird als vierundzwanzigster Teil des Zeitraums von Mitternacht bis Mitternacht definiert; 1:00:00 bis 1:59:59 Uhr ist beispielsweise eine volle Stunde. Weitere Informationen zum Instance-Status finden Sie unter Amazon-EC2-Instance-Statusänderungen.

Ein Reserved Instance-Abrechnungsvorteil wird auf eine laufende Instance auf Sekundenbasis angewendet. Sekundengenaue Abrechnung ist für Instances verfügbar, die eine Open-Soruce-Linux-Verteilung verwenden, wie z. B. Amazon Linux und Ubuntu. Stundengenaue Abrechnung wird für

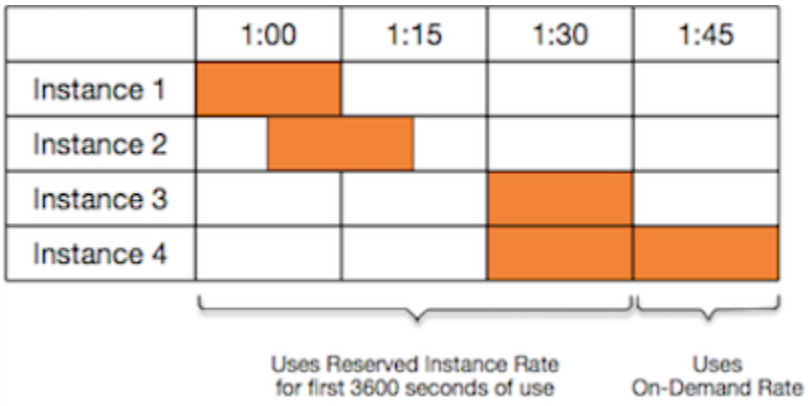
kommerzielle Linux-Verteilungen, wie z. B. Red Hat Enterprise Linux und SUSE Linux Enterprise Server, verwendet.

Ein Reserved Instance-Rabatte wird nur auf eine Instance-Stunde pro voller Stunde bis zu maximal 3600 Sekunden (eine Stunde) angewendet. Sie können mehrere Instances gleichzeitig ausführen, aber Sie können nur den Vorteil des Reserved Instance-Rabatts für insgesamt 3600 Sekunden auf Stundenbasis beanspruchen. Die Instance-Nutzung, die 3600 Sekunden auf Stundenbasis überschreitet, wird nach dem Bedarfssatz berechnet.

Wenn Sie beispielsweise eine `m4.xlarge` Reserved Instance kaufen und gleichzeitig vier `m4.xlarge`-Instances gleichzeitig eine Stunde lang ausführen, wird eine Instance pro Stunde der Reserved Instance-Nutzung und die anderen drei Instances werden für drei Stunden nach bedarfsgesteuerter Nutzung berechnet.

Wenn Sie jedoch eine `m4.xlarge` Reserved Instance kaufen und vier `m4.xlarge`-Instances 15 Minuten (900 Sekunden) lang jeweils innerhalb derselben Stunde ausführen, beträgt die gesamte Laufzeit für die Instance eine Stunde, was zu einer Stunde der Reserved Instance-Nutzung und 0 Stunden der bedarfsgesteuerten Nutzung führt.

Wenn mehrere geeignete Instances gleichzeitig laufen, wird der Rechnungsrabatt für Reserved Instance auf alle Instances gleichzeitig bis zu maximal 3600 Sekunden auf einer Stundenbasis angewendet; danach gelten bedarfsorientierte Sätze.



Cost Explorer auf der Billing and Cost Management-Konsole bietet Ihnen die Möglichkeit, die Einsparungen gegen laufende On-Demand-Instances zu analysieren. Die Reserved Instances FAQ enthält ein Beispiel zu einer Listenwertberechnung.

Wenn Sie Ihr AWS-Konto schließen, wird die On-Demand-Abrechnung für Ihre Ressourcen beendet. Wenn Sie jedoch in Ihrem Konto über Reserved Instances verfügen, erhalten Sie bis zu deren Auslaufen auch weiterhin eine Rechnung.

Anzeigen Ihrer Rechnung

Die Tarife und Gebühren für Ihr Konto können Sie über die Seite AWS Fakturierung und Kostenmanagement in der Konsole anzeigen.

- Das Dashboard zeigt eine Ausgabenzusammenfassung für Ihr Konto an.
- Erweitern Sie auf der Seite Bills (Rechnungen) unter Details den Abschnitt Elastic Compute Cloud und die Region, um Fakturierungsdaten zu Ihren Reserved Instances abzurufen.

Sie können die Gebühren online anzeigen oder eine CSV-Datei herunterladen.

Sie können außerdem Ihre Reserved-Instances-Nutzung über den AWS-Kosten- und -Nutzungsbericht nachverfolgen. Weitere Informationen finden Sie unter Ihre Reservierungen verstehen.

Reserved Instances- und konsolidierte Fakturierung

Die Preisvorteile von Reserved Instances werden geteilt, wenn das kaufende Konto Teil eines Satzes von Konten ist, die unter einem einzigen, konsolidierten Zahlerkonto abgerechnet werden. Der Instance-Nutzung für alle Mitgliedskonten wird jeden Monat im Zahlerkonto zusammengefasst. Dies ist in der Regel für Unternehmen nützlich, in denen es verschiedene Funktionsteams oder -gruppen gibt. Zur Berechnung der Abrechnung wird die normale Logik für Reserved Instances angewendet. Weitere Informationen finden Sie unter Konsolidierte Fakturierung im AWS Organizations.

Wenn Sie das Konto schließen, das die Reserved Instance erworben hat, wird das Konto des Zahlers für die Reserved Instance belastet, bis die Reserved Instance abläuft. Das geschlossene Konto wird nach 90 Tagen endgültig gelöscht, und die Mitgliedskonten profitieren nicht mehr von dem Reserved-Instance-Abrechnungsrabatt.

> **Note**
>
> Zonal Reserved Instances reservieren Kapazität nur für das Besitzerkonto und können nicht für andere AWS-Konten freigegeben werden. Wenn Sie Kapazität für andere AWS-Konten freigeben müssen, verwenden Sie Reservieren Sie Rechenkapazität mit Kapazitätsreservierungen EC2 auf Abruf.

Reserved Instance-Rabatt-Preisstufen

Wenn Ihr Konto für eine Rabattpreisstufe qualifiziert ist, erhält es beim Kauf von Reserved Instances innerhalb der Stufe ab dem Kaufzeitpunkt die Rabatte automatisch für Vorabzahlungen und Nutzungsgebühren für die Instance. Um für einen Rabatt qualifiziert zu sein, muss der Listenwert Ihrer Reserved Instances in der Region bei mindestens 500 000 USD liegen.

Es gelten die folgenden Regeln:

- Die Preisstufen und die entsprechenden Rabatte gelten nur für Käufe von Amazon EC2 Standard Reserved Instances.
- Die Preisstufen gelten nicht für Reserved Instancess für Windows mit SQL Server Standard oder SQL Server Web und SQL Server Enterprise.
- Die Preisstufen gelten nicht für Reserved Instances für Linux mit SQL Server aller Art.
- Die Preisstufenrabatte gelten nur für Käufe bei AWS. Sie gelten nicht für Käufe von Reserved Instances bei Drittanbietern.
- Die Rabattpreisstufen gelten im Moment nicht für Convertible Reserved Instance-Käufe.

Themen

- Berechnen der Reserved Instance-Preisrabatte
- Kaufen mit einer Rabattstufe
- Überschreiten von Preisstufen
- Konsolidierte Fakturierung für Preisstufen

Berechnen der Reserved Instance-Preisrabatte

Sie können die Preisstufe für Ihr Konto berechnen, indem Sie den Listenwert Ihrer gesamten Reserved Instances in einer Region berechnen. Multiplizieren Sie den stündlichen, regelmäßigen

Preis für jede Reservierung mit den gesamten Stundenzahl für die Laufzeit verbleibenden Stunden und addieren Sie dann den Vorauszahlungspreis ohne Rabatt (der sogenannte Festpreis) zum Zeitpunkt des Kaufs. Da der Listenwert auf den Preisen ohne Rabatt (öffentlich) basiert, ändert er sich durch Ihre Qualifizierung für einen Volumenrabatt oder bei einer Preissenkung nach dem Kauf Ihrer Reserved Instances nicht.

```
List value = fixed price + (undiscounted recurring hourly price * hours in term)
```

Nehmen wir beispielsweise für eine 1-jährige Teilvorauszahlung `t2.small` Reserved Instance den Anzahlungspreis von 60,00 USD und einen Stundensatz von 0,007 USD an. Dies ergibt einen Listenwert von 121,32 $.

```
121.32 = 60.00 + (0.007 * 8760)
```

So zeigen Sie die Festpreise für Reserved Instances mithilfe der Amazon EC2-Konsole an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances aus.
3. Um die Spalte Vorauszahlungspreis anzuzeigen, wählen Sie das Einstellungssymbol ( ) in der oberen rechten Ecke, schalten Sie den Vorauszahlungspreis ein und wählen Sie Bestätigen.

So zeigen Sie die Festpreise für Reserved Instances mithilfe der Befehlszeile an

- describe-reserved-instances (AWS CLI)
- Get-EC2ReservedInstance (AWS Tools for Windows PowerShell)

Kaufen mit einer Rabattstufe

Wenn Sie Reserved Instances erwerben, wendet Amazon EC2 automatisch alle Rabatte auf Ihre Käufe in einer Rabattpreisstufe an. Sie müssen nichts anders machen. Sie können die Reserved Instances ganz normal über die Amazon EC2-Tools kaufen. Weitere Informationen finden Sie unter Reserved-Instances für Amazon EC2 erwerben.

Nachdem der Listenwert Ihrer aktiven Reserved Instances in einer Region den Wert für eine Rabattpreisstufe erreicht, werden alle weiteren Käufe von Reserved Instances in dieser Region zum

Rabatttarif berechnet. Wenn Sie mit einem einzelnen Kauf von Reserved Instances in einer Region den Wert für eine Rabattpreisstufe erreichen, wird der Teil des Kaufes, der über dem Grenzwert liegt, zum Rabatttarif berechnet. Weitere Informationen über die im Rahmen des Kaufprozesses erstellten temporären Reserved Instances-IDs finden Sie unter Überschreiten von Preisstufen.

Wenn Ihr Listenwert unter den Wert für die Rabattpreisstufe fällt (beispielsweise, wenn einige Ihrer Reserved Instances auslaufen), werden alle weiteren Käufe von Reserved Instances in dieser Region nicht mehr zum Rabatttarif berechnet. Sie erhalten jedoch für alle ursprünglich zur Rabattpreisstufe erworbenen Reserved Instances weiterhin den Rabatt.

Beim Kauf von Reserved Instances gilt eines von vier möglichen Szenarien:

- Kein Rabatt – Ihr Kauf innerhalb einer Region liegt weiterhin unter dem Rabattgrenzwert.
- Teilweiser Rabatt – Ihr Kauf innerhalb einer Region überschreitet den Rabattgrenzwert für die erste Rabattstufe. Auf eine oder mehrere Reservierungen wird kein Rabatt angewendet. Auf die restlichen Reservierungen wird der Rabatt angewendet.
- Voller Rabatt – Ihr kompletter Kauf innerhalb einer Region fällt in eine Rabattstufe und der entsprechende Rabatt wird angewendet.
- Zwei Rabatttarife – Ihr Kauf innerhalb einer Region überschreitet den Rabattgrenzwert für eine höhere Rabattstufe. Ihnen werden zwei verschiedene Tarife berechnet: Auf eine oder mehrere Reservierungen wird der geringere Rabatt angewendet. Auf die restlichen Reservierungen wird der Rabatt der höheren Rabattstufe angewendet.

Überschreiten von Preisstufen

Wenn Ihr Kauf eine Rabattpreisstufe überschreitet, werden mehrere Einträge für diesen Kauf angezeigt: Ein Eintrag für den Kauf zum regulären Preis und ein weiterer für den Teil des Kaufes, der mit dem entsprechenden Rabatt berechnet wird.

Der Reserved Instance-Service generiert mehrere Reserved Instance-IDs, da Ihr Kauf auch Teile mit und ohne Rabatt umfasst. Es gibt eine ID für jeden Reservierungssatz in einer Stufe. Die vom CLI-Befehl oder durch die API-Aktion zurückgegebene ID unterscheidet sich daher von der tatsächlichen ID der neuen Reserved Instances.

Konsolidierte Fakturierung für Preisstufen

Ein Konto für die konsolidierte Fakturierung fasst den Listenwert von Mitgliedskonten innerhalb einer Region zusammen. Wenn der Listenwert aller aktiven Reserved Instances für das konsolidierte

Fakturierungskonto eine Rabattpreisstufe erreicht, werden ab diesem Zeitpunkt alle Reserved Instances-Käufe durch jedes Mitglied des konsolidierten Abrechnungskontos zum Rabatttarif berechnet (solange der Listenwert für das konsolidierte Konto über dem Rabattpreisstufengrenzwert bleibt). Weitere Informationen finden Sie unter Reserved Instances- und konsolidierte Fakturierung.

Reserved-Instances für Amazon EC2 erwerben

Um eine Reserved Instance für Amazon EC2 zu kaufen, können Sie die Amazon-EC2-Konsole, ein Befehlszeilentool oder ein SDK verwenden, um nach Angeboten für Reserved Instances von AWS und Drittanbietern zu suchen, wobei Sie Ihre Suchparameter anpassen können, bis Sie genau das finden, wonach Sie suchen.

Wenn Sie nach Angeboten für Reserved Instances suchen, erhalten Sie eine Information zu den Kosten der gefundenen Angebote. Wenn Sie mit dem Kauf fortfahren, wendet AWS automatisch einen Limitpreis für den Kaufpreis an. Die Gesamtkosten Ihrer Reserved Instances liegen auf keinen Fall über dem angebotenen Preis.

Wenn der Preis aus irgendwelchen Gründen steigt oder sich verändert, wird der Kauf nicht abgeschlossen. Wenn Sie die Reserved Instance eines Drittanbieters über den Amazon EC2 Reserved Instance Marketplace kaufen und Angebote mit Ihrer Auswahl übereinstimmen und kostengünstiger sind, verkauft AWS Ihnen die Angebote zum günstigeren Einstiegspreis.

Bevor Sie Ihren Kauf bestätigen, sollten Sie sich die Details zu der Reserved Instance ansehen. Stellen Sie sicher, dass alle Parameter korrekt sind. Nach dem Kauf einer Reserved Instance (von einem Drittanbieter im Reserved Instance Marketplace oder von AWS) kann der Kauf nicht mehr storniert werden. Sie können einen Kauf für ein zukünftiges Datum in die Warteschlange stellen und den Kauf in der Warteschlange vor dem geplanten Zeitpunkt stornieren.

Um Reserved Instances zu erwerben und zu ändern, stellen Sie sicher, dass Ihr Benutzer über die entsprechenden Berechtigungen verfügt, z. B. die Fähigkeit, Availability Zones zu beschreiben. Weitere Informationen finden Sie unter the section called “Arbeiten mit Reserved Instances” (API) oder the section called “Arbeiten mit Reserved Instances” (Konsole).

Aufgaben

- Wählen einer Plattform
- Einstellen des Kaufs in die Warteschlange
- Kaufen von Standard-Reserved Instances
- Kaufen von Convertible Reserved Instances

- Einkaufen im Reserved Instance-Marketplace
- Stornieren eines in die Warteschlange eingestellten Kaufs
- Erneuern eines Reserved Instance

Wählen einer Plattform

Amazon EC2 unterstützt die folgenden Plattformen für Reserved Instances:

- Linux/Unix
- Linux mit SQL Server-Standard
- Linux mit SQL Server Web
- Linux mit SQL Server Enterprise
- SUSE Linux
- Red Hat Enterprise Linux
- Red Hat Enterprise Linux mit HA
- Windows
- Windows mit SQL Server-Standard
- Windows mit SQL Server Web
- Windows mit SQL Server Enterprise

Überlegungen

- Wenn Sie Ihr eigenes Abonnement (BYOS) für Red Hat Enterprise Linux, SUSE Linux oder Ubuntu Pro verwenden, müssen Sie ein Angebot für die Linux/Unix-Plattform auswählen.
- Reserved Instances werden auf Instances, auf denen macOS oder Ubuntu Pro ausgeführt wird, nicht unterstützt (EC2-Abonnement enthalten, d. h. nicht BYOS). Wenn Sie mit den Preisen für On-Demand-Instances sparen möchten, empfiehlt es sich, macOS- und Ubuntu-Pro-Instances (EC2-Abonnement enthalten) mit Savings Plans zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch für Savings Plans.

Um sicherzustellen, dass eine Instance in einer bestimmten Reserved Instance ausgeführt wird, muss die Plattform der Reserved Instance mit der Plattform des AMIs übereinstimmen, das zum Starten der Instance verwendet wurde. Bei Linux-AMIs ist es wichtig zu überprüfen, ob die AMI-Plattform den allgemeinen Wert Linux/UNIX oder einen spezifischeren Wert wie SUSE Linux verwendet.

Console

So überprüfen Sie die AMI-Plattform

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie das AMI aus.
4. Notieren Sie sich auf der Registerkarte Details den Wert der Plattformdetails.

AWS CLI

So überprüfen Sie die AMI-Plattform

Verwenden Sie den Befehl describe-images und überprüfen Sie den Wert von `PlatformDetails`.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query Images[*].PlatformDetails
```

Es folgt eine Beispielausgabe.

```
[
    "Linux/UNIX"
]
```

PowerShell

So überprüfen Sie die AMI-Plattform

Verwenden Sie das cmdlet Get-EC2Image und überprüfen Sie den Wert von `PlatformDetails`.

```
Get-EC2Image `
    -ImageId ami-0abcdef1234567890 | `
    Select PlatformDetails
```

Es folgt eine Beispielausgabe.

```
PlatformDetails
```

```
---------------
Linux/UNIX
```

Einstellen des Kaufs in die Warteschlange

Wenn Sie eine Reserved Instance kaufen, wird der Kauf normalerweise sofort ausgeführt. Sie können einen Kauf aber auch für ein künftiges Ausführungsdatum (samt Zeit) in die Warteschlange einstellen. Sie können beispielsweise einen Kauf für den Zeitpunkt in die Warteschlange einstellen, an dem eine vorhandene Reserved Instance abläuft. So können Sie sicherstellen, dass jederzeit die erforderlichen Kapazitäten verfügbar sind.

Sie können Käufe regionaler Reserved Instances in die Warteschlange einstellen, nicht aber die Käufe für zonengebundene Reserved Instances oder Reserved Instances anderer Verkäufer. Sie können einen Kauf bis zu drei Jahre im Voraus in die Warteschlange einstellen. Zum geplanten Zeitpunkt wird der Kauf unter Verwendung der Standard-Zahlungsweise ausgeführt. Nachdem die Zahlung abgewickelt wurde, wird der Bonus zugewiesen.

Sie können in der Amazon-EC2-Konsole ein Datum für Ihre Einkäufe in der Warteschlange festlegen, und der Kauf wird an diesem Tag bis 00:00 Uhr UTC in die Warteschlange gestellt. Um eine andere Uhrzeit für den Kauf in der Warteschlange anzugeben, verwenden Sie ein AWS-SDK oder ein Befehlszeilentool.

Sie können in die Warteschlange eingestellte Käufe in der Amazon EC2-Konsole anzeigen. Der Status der in die Warteschlange eingestellten Käufe lautet queued (In Warteschlange). Sie können einen in die Warteschleife eingestellten Kauf jederzeit stornieren, bevor der Kaufzeitpunkt erreicht ist. Details dazu finden Sie unter Stornieren eines in die Warteschlange eingestellten Kaufs.

Kaufen von Standard-Reserved Instances

Sie können Standard-Reserved Instances in einer bestimmten Availability Zone kaufen und so eine Kapazitätsreservierung erhalten. Alternativ können Sie auf die Kapazitätsreservierung verzichten und eine regionale Standard-Reserved Instance kaufen.

Nach Abschluss des Kaufs wird der Bonus sofort zugewiesen, sofern Sie bereits eine Instance ausführen, die den Spezifikationen der Reserved Instance entspricht. Sie müssen Ihre Instances nicht neu starten. Wenn Sie über keine passende laufende Instance verfügen, starten Sie eine Instance mit exakt denselben Kriterien, die Sie für die Reserved Instance angegeben haben. Weitere Informationen finden Sie unter Nutzen Ihres Reserved Instances.

Beispiele zur Anwendung von Reserved Instances auf aktive Instances finden Sie unter Wie Reserved-Instances-Rabatte angewendet werden.

Console

So kaufen Sie Standard Reserved Instances

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances (Reservierte Instances) und dann Purchase Reserved Instances (Reserved Instances kaufen) aus.
3. Wählen Sie für Offering class (Angebotsklasse) Standard aus, um Standard-Reserved Instances anzuzeigen.
4. Aktivieren Sie auf der Kaufseite in der rechten oberen Ecke Only show offerings that reserve capacity. Wenn Sie diese Einstellung aktivieren, wird das Feld Availability Zone angezeigt.

   Um ein regionales Reserved Instance zu kaufen, deaktivieren Sie diese Einstellung. Wenn Sie diese Einstellung deaktivieren, verschwindet das Feld Availability Zone .
5. Wählen Sie bei Bedarf andere Konfigurationen aus und wählen Sie dann Search aus.
6. Geben Sie für jede Reserved Instance, die Sie kaufen möchten, die gewünschte Menge ein und wählen Sie Add to Cart (In den Einkaufswagen) aus.

   Suchen Sie in der Spalte Seller nach 3rd party, um eine Standard-Reserved-Instance im Reserved Instance Marketplace zu erwerben. Die Spalte Term zeigt Nicht-Standard-Laufzeiten an. Weitere Informationen finden Sie unter Einkaufen im Reserved Instance-Marketplace.
7. Wählen Sie Reserved InstancesView Cart (Warenkorb anzeigen) aus, um eine Zusammenfassung der ausgewählten anzuzeigen.
8. Wenn für Order On (Bestellen am) der Wert Now (Jetzt) eingestellt ist, wird der Kauf sofort ausgeführt, nachdem Sie Order all (Alle bestellen) ausgewählt haben. Um einen Kauf in die Warteschlange einzustellen, wählen Sie Now (Jetzt) und dann ein Datum aus. Sie können für jedes entsprechende Angebot im Warenkorb ein anderes Datum auswählen. Der Kauf wird am ausgewählten Datum bis 00:00 Uhr UTC in die Warteschlange gestellt.
9. Wählen Sie Order all (Alle bestellen) aus, um den Kauf abzuschließen.

   Wenn es zum Bestellzeitpunkt Angebote gibt, die mit Ihrer Auswahl übereinstimmen und kostengünstiger sind, verkauft AWS Ihnen die Angebote zum günstigeren Preis.
10. Klicken Sie auf Close.

Der Status Ihrer Bestellung wird in der Spalte State (Status) angezeigt. Wenn Ihre Bestellung abgeschlossen ist, ändert sich der State-Wert von `Payment-pending` auf `Active`. Wenn die Reserved Instance den Status `Active` hat, kann sie verwendet werden.

Wenn der Status zu `Retired` wechselt, hat AWS möglicherweise die Zahlung nicht erhalten.

AWS CLI

So kaufen Sie eine Standard Reserved Instance

1. Suchen Sie mit dem Befehl describe-reserved-instances-offerings nach verfügbaren Reserved Instances. Geben Sie für den Parameter `standard` den Wert `--offering-class` an, um nur Standard Reserved Instances zurückzugeben. Sie können zusätzliche Kriterien anwenden, um Ihre Ergebnisse einzuschränken. Verwenden Sie beispielsweise den folgenden Befehl, um eine regionale `t2.large`-Reserved-Instance mit einem Standard-Tenancy für `Linux/UNIX` und einer Laufzeit von nur einem Jahr zu kaufen:

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=duration,Values=31536000 \
              Name=scope,Values=Region
```

Um Reserved Instances nur im Reserved Instance Marketplace zu suchen, verwenden Sie den `marketplace`-Filter und geben in der Anforderung keine Laufzeit an (die Laufzeit kann kürzer als ein oder drei Jahre sein).

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=marketplace,Values=true
```

Wenn Sie eine zu Ihren Anforderungen passende Reserved Instance finden, notieren Sie sich die Angebots-ID. Beispiel:

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. Verwenden Sie den Befehl purchase-reserved-instances-offering, um die Reserved Instance zu kaufen. Sie müssen die Reserved Instance-Angebots-ID aus dem vorherigen Schritt und die Anzahl der Instances für die Reservierung angeben.

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

   Normalerweise wird der Kauf sofort ausgeführt. Sie können den Kauf auch in die Warteschlange einstellen, indem Sie dem vorherigen Aufruf die folgende Option hinzufügen.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Verwenden Sie den Befehl describe-reserved-instances, um den Status Ihrer Reserved Instance abzurufen.

```
aws ec2 describe-reserved-instances \
    --reserved-instances-ids b847fa93-e282-4f55-b59a-1342fec06327 \
    --query ReservedInstances[].State
```

PowerShell

So kaufen Sie eine Standard Reserved Instance

1. Suchen Sie mit dem cmdlet Get-EC2ReservedInstancesOffering nach verfügbaren Reserved Instances. Geben Sie für den Parameter `standard` den Wert `-OfferingClass` an, um nur Standard-Reserved Instances zurückzugeben. Sie können zusätzliche Kriterien anwenden, um Ihre Ergebnisse einzuschränken. Verwenden Sie beispielsweise den folgenden Befehl, um eine regionale `t2.large`-Reserved-Instance mit einem Standard-Tenancy für `Linux/UNIX` und einer Laufzeit von nur einem Jahr zu kaufen:

```
Get-EC2ReservedInstancesOffering `
    -InstanceType "t2.large" `
    -OfferingClass "standard" `
    -ProductDescription "Linux/UNIX" `
    -InstanceTenancy "default" `
```

```
    -Filters @{Name="duration"; Values="31536000"} `
             @{Name="scope"; Values="Region"
```

Um Reserved Instances nur im Reserved Instance Marketplace zu suchen, verwenden Sie den `marketplace`-Filter und geben in der Anforderung keine Laufzeit an (die Laufzeit kann kürzer als ein oder drei Jahre sein).

```
Get-EC2ReservedInstancesOffering `
    -InstanceType t2.large `
    -OfferingClass "standard" `
    -ProductDescription "Linux/UNIX" `
    -InstanceTenancy default `
    -Filters @{Name="marketplace"; Values="true"}
```

Wenn Sie eine zu Ihren Anforderungen passende Reserved Instance finden, notieren Sie sich die Angebots-ID. Zum Beispiel:

```
bec624df-a8cc-4aad-a72f-4f8abc34caf2
```

2. Verwenden Sie das cmdlet New-EC2ReservedInstance, um die Reserved Instance zu kaufen. Sie müssen die Reserved Instance-Angebots-ID aus dem vorherigen Schritt und die Anzahl der Instances für die Reservierung angeben.

```
New-EC2ReservedInstance `
    -ReservedInstancesOfferingId "bec624df-a8cc-4aad-a72f-4f8abc34caf2" `
    -InstanceCount 1
```

Normalerweise wird der Kauf sofort ausgeführt. Sie können den Kauf aber in die Warteschlange einstellen, indem Sie dem vorherigen Aufruf den folgenden Parameter hinzufügen.

```
-PurchaseTime "2020-12-01T00:00:00Z"
```

3. Verwenden Sie das cmdlet Get-EC2ReservedInstance, um den Status der Reserved Instance abzurufen.

```
Get-EC2ReservedInstance `
    -ReservedInstancesId b847fa93-e282-4f55-b59a-1342fec06327 | `
    Select State
```

Kaufen von Convertible Reserved Instances

Sie können Convertible Reserved Instances in einer bestimmten Availability Zone kaufen und so eine Kapazitätsreservierung erhalten. Alternativ können Sie auf die Kapazitätsreservierung verzichten und eine regionale Convertible Reserved Instance kaufen.

Wenn Sie bereits über eine aktive Instance verfügen, die mit den Spezifikationen der Reserved Instance übereinstimmt, wird der Rabatt sofort angewendet. Sie müssen Ihre Instances nicht neu starten. Wenn Sie über keine passende Instance verfügen, starten Sie eine Instance mit denselben Kriterien, die Sie für die Reserved Instance angegeben haben. Weitere Informationen finden Sie unter Nutzen Ihres Reserved Instances.

Beispiele zur Anwendung von Reserved Instances auf aktive Instances finden Sie unter Wie Reserved-Instances-Rabatte angewendet werden.

Console

So kaufen Sie Convertible Reserved Instances

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances und dann Purchase Reserved Instances (Reserved Instances kaufen) aus.
3. Wählen Sie für Offering class (Angebotsklasse) Convertible aus, um Convertible Reserved Instances anzuzeigen.
4. Aktivieren Sie auf der Kaufseite in der rechten oberen Ecke Only show offerings that reserve capacity. Wenn Sie diese Einstellung aktivieren, wird das Feld Availability Zone angezeigt.

   Um ein regionales Reserved Instance zu kaufen, deaktivieren Sie diese Einstellung. Wenn Sie diese Einstellung deaktivieren, verschwindet das Feld Availability Zone .
5. Wählen Sie bei Bedarf andere Konfigurationen aus und wählen Sie Search aus.
6. Geben Sie für jede Convertible Reserved Instance, die Sie kaufen möchten, die Menge ein und wählen Sie Add to cart (In den Einkaufswagen) aus.
7. Wählen Sie View Cart (Warenkorb anzeigen) aus, um eine Zusammenfassung der Auswahl anzuzeigen.
8. Wenn für Order On (Bestellen am) der Wert Now (Jetzt) eingestellt ist, wird der Kauf sofort ausgeführt, nachdem Sie Order all (Alle bestellen) ausgewählt haben. Um einen Kauf in die Warteschlange einzustellen, wählen Sie Now (Jetzt) und dann ein Datum aus. Sie können für

jedes entsprechende Angebot im Warenkorb ein anderes Datum auswählen. Der Kauf wird am ausgewählten Datum bis 00:00 Uhr UTC in die Warteschlange gestellt.

9. Wählen Sie Order all (Alle bestellen) aus, um den Kauf abzuschließen.

   Wenn es zum Bestellzeitpunkt Angebote gibt, die mit Ihrer Auswahl übereinstimmen und kostengünstiger sind, verkauft AWS Ihnen die Angebote zum günstigeren Preis.

10. Klicken Sie auf Close.

    Der Status Ihrer Bestellung wird in der Spalte State (Status) angezeigt. Wenn Ihre Bestellung abgeschlossen ist, ändert sich der State-Wert von `Payment-pending` auf `Active`. Wenn die Reserved Instance den Status `Active` hat, kann sie verwendet werden.

    Wenn der Status zu `Retired` wechselt, hat AWS möglicherweise die Zahlung nicht erhalten.

AWS CLI

So kaufen Sie eine Convertible Reserved Instance

1. Suchen Sie mit dem Befehl describe-reserved-instances-offerings nach verfügbaren Reserved Instances. Geben Sie für die Option `--offering-class` den Wert `convertible` an, um nur Convertible Reserved Instances zurückzugeben. Sie können zusätzliche Kriterien anwenden, um Ihre Ergebnisse einzuschränken. Verwenden Sie beispielsweise den folgenden Befehl, um eine regionale `t2.large` Reserved Instance mit einem Standard-Tenancy für `Linux/UNIX` zu kaufen.

   ```
   aws ec2 describe-reserved-instances-offerings \
       --instance-type t2.large \
       --offering-class convertible \
       --product-description "Linux/UNIX" \
       --instance-tenancy default \
       --filters Name=scope,Values=Region
   ```

   Wenn Sie eine zu Ihren Anforderungen passende Reserved Instance finden, notieren Sie sich die Angebots-ID. Beispiel:

   ```
   "ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
   ```

2. Verwenden Sie den Befehl purchase-reserved-instances-offering, um die Reserved Instance zu kaufen. Sie müssen die Reserved Instance-Angebots-ID aus dem vorherigen Schritt und die Anzahl der Instances für die Reservierung angeben.

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

Normalerweise wird der Kauf sofort ausgeführt. Sie können den Kauf auch in die Warteschlange einstellen, indem Sie dem vorherigen Aufruf die folgende Option hinzufügen.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Verwenden Sie den Befehl describe-reserved-instances, um den Status Ihrer Reserved Instance abzurufen.

```
aws ec2 describe-reserved-instances \
    --reserved-instances-ids b847fa93-e282-4f55-b59a-1342fec06327 \
    --query ReservedInstances[].State
```

PowerShell

So kaufen Sie eine Convertible Reserved Instance

1. Suchen Sie mit dem cmdlet Get-EC2ReservedInstancesOffering nach verfügbaren Reserved Instances. Geben Sie für den Parameter `convertible` den Wert `-OfferingClass` an, um nur Convertible Reserved Instances zurückzugeben. Sie können zusätzliche Kriterien anwenden, um Ihre Ergebnisse einzuschränken. Verwenden Sie beispielsweise den folgenden Befehl, um eine regionale `t2.large` Reserved Instance mit einem Standard-Tenancy für `Linux/UNIX` zu kaufen.

```
Get-EC2ReservedInstancesOffering `
    -InstanceType "t2.large" `
    -OfferingClass "convertible" `
    -ProductDescription "Linux/UNIX" `
    -InstanceTenancy "default" `
    -Filters @{Name="scope"; Values="Region"
```

Wenn Sie eine zu Ihren Anforderungen passende Reserved Instance finden, notieren Sie sich die Angebots-ID. Zum Beispiel:

```
bec624df-a8cc-4aad-a72f-4f8abc34caf2
```

2. Verwenden Sie das cmdlet New-EC2ReservedInstance, um die Reserved Instance zu kaufen. Sie müssen die Angebots-ID der Reserved Instance aus dem vorherigen Schritt und die Anzahl der Instances für die Reservierung angeben.

```
New-EC2ReservedInstance `
    -ReservedInstancesOfferingId "bec624df-a8cc-4aad-a72f-4f8abc34caf2" `
    -InstanceCount 1
```

Normalerweise wird der Kauf sofort ausgeführt. Sie können den Kauf aber in die Warteschlange einstellen, indem Sie dem vorherigen Aufruf den folgenden Parameter hinzufügen.

```
-PurchaseTime "2020-12-01T00:00:00Z"
```

3. Verwenden Sie das cmdlet Get-EC2ReservedInstance, um den Status der Reserved Instance abzurufen.

```
Get-EC2ReservedInstance `
    -ReservedInstancesId b847fa93-e282-4f55-b59a-1342fec06327 | `
    Select State
```

Einkaufen im Reserved Instance-Marketplace

Sie können Reserved Instances von Drittanbietern kaufen, die über Reserved Instances vom Reserved Instance Marketplace verfügen, die sie nicht mehr brauchen. Sie können mithilfe der Amazon EC2-Konsole oder einem Befehlszeilen-Tool kaufen. Der Vorgang entspricht dem Kauf von Reserved Instances bei AWS. Weitere Informationen finden Sie unter Kaufen von Standard-Reserved Instances.

Es gibt ein paar Unterschiede zwischen Reserved Instances, die im Reserved Instance Marketplace gekauft werden, und Reserved Instances, die direkt bei erworben werden AWS:

- Laufzeit: Von Drittanbietern erworbene Reserved Instances bieten nicht mehr die volle Standardlaufzeit. Die Standardlaufzeit der von AWS erworbenen Reserved Instances beträgt ein Jahr oder drei Jahre.
- Vorauszahlungspreis: Reserved Instances von Drittanbietern können zu abweichenden Vorauszahlungspreisen verkauft werden. Die nutzungsabhängigen oder regelmäßigen Gebühren bleiben unverändert, da diese bereits beim ursprünglichen Kauf der Reserved Instances bei festgesetzt wurden AWS.
- Typen von Reserved Instances: Nur Amazon EC2 Standard-Reserved-Instances können über den Reserved Instance Marketplace erworben werden. Convertible Reserved Instances, Amazon RDS und Amazon ElastiCache Reserved Instances sind auf dem Reserved Instance Marketplace nicht zum Kauf verfügbar.

Dem Verkäufer werden grundlegende Informationen zu Ihnen mitgeteilt (z. B. die Postleitzahl und das Land).

Mit diesen Informationen kann der Verkäufer möglicherweise anfallenden Transaktionssteuern (z. B. Mehrwertsteuer) bestimmen. Sie werden als Auszahlungsbericht bereitgestellt. In seltenen Fällen muss AWS möglicherweise Ihre E-Mail-Adresse an den Verkäufer weitergeben, damit dieser Sie bei Fragen zum Verkauf kontaktieren kann (z. B. bei steuerlichen Fragen).

Aus denselben Gründen teilt AWS auf dem Kaufbeleg des Käufers den Namen der juristischen Person des Verkäufers mit. Wenn Sie aus steuerlichen oder anderen Gründen weitere Informationen zum Verkäufer benötigen, kontaktieren Sie bitte den Support.

Stornieren eines in die Warteschlange eingestellten Kaufs

Sie können einen Kauf bis zu drei Jahre im Voraus in die Warteschlange einstellen. Sie können einen in die Warteschleife eingestellten Kauf jederzeit stornieren, bevor der Kaufzeitpunkt erreicht ist.

Console

So stornieren Sie einen in die Warteschlange eingestellten Kauf

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances aus.
3. Wählen Sie mindestens eine Reserved Instances aus.
4. Wählen Sie Actions (Aktionen), Delete Queued Reserved Instances (In die Warteschlange eingestellte reservierte Instances löschen).

5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen) und dann Close (Schließen) aus.

AWS CLI

So stornieren Sie einen in die Warteschlange eingestellten Kauf

Verwenden Sie den Befehl delete-queued-reserved-instances.

```
aws ec2 delete-queued-reserved-instances \
    --reserved-instances-ids b847fa93-e282-4f55-b59a-1342fec06327
```

PowerShell

So stornieren Sie einen in die Warteschlange eingestellten Kauf

Verwenden Sie das cmdlet Remove-EC2QueuedReservedInstance.

```
Remove-EC2QueuedReservedInstance `
    -ReservedInstancesId b847fa93-e282-4f55-b59a-1342fec06327
```

Erneuern eines Reserved Instance

Sie können einen Reserved Instance verlängern, bevor er abläuft. Beim Erneuern einesReserved Instance wird der Kauf eines Reserved Instance mit der gleichen Konfiguration in die Warteschlange gesetzt, bis der aktuelle Reserved Instance abläuft.

Sie müssen eine Reserved Instance über die Amazon-EC2-Konsole verlängern.

So verlängern Sie einen Reserved Instance mit einem in die Warteschlange gesetzten Einkauf

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances aus.
3. Wählen Sie die zu erneuernde Reserved Instance aus.
4. Wählen Sie Actions (Aktionen), Renew Reserved Instances (Reserved Instances erneuern).
5. Um die Bestellung abzuschließen, wählen Sie Order all (Alle bestellen) und dann Close (Schließen) aus.

Reserved Instances für Amazon EC2 auf dem Reserved Instance Marketplace verkaufen

Der Amazon EC2 Reserved Instance Marketplace ist eine Plattform, über die AWS-Kunden und Drittanbieter ungenutzte Standard Reserved Instances verkaufen können. Diese Reserved Instances können in Bezug auf Laufzeit und Preisoptionen variieren. Möglicherweise möchten Sie Ihre Reserved Instances verkaufen, wenn Sie sie nicht mehr benötigen, z. B. wenn Sie Ihre Instances in eine neue AWS-Region verschieben, zu einem anderen Instance-Typ wechseln, Projekte abschließen, bevor die Laufzeit der Reserved Instance abläuft, sich Ihre Geschäftsanforderungen ändern oder Sie über Überkapazitäten verfügen.

Sobald Sie Ihre Reserved Instances im Reserved Instances Marketplace anbieten, sind diese für mögliche Kunden sichtbar. Alle Reserved Instances werden nach deren verbleibender Laufzeit und dem Stundenpreis gruppiert.

Bei der Anfrage eines Käufers, die Reserved Instance eines Drittanbieters über Reserved Instance Marketplace zu erwerben, verkauft AWS zuerst die Reserved Instance mit dem günstigsten Einstiegspreis in der entsprechenden Gruppe. Danach verkauft AWS die Reserved Instance mit dem nächstniedrigeren Preis. Dies wird so lange wiederholt, bis die Anforderung des Kunden erfüllt ist. AWS verarbeitet dann die Transaktionen und überträgt den Besitz der Reserved Instances an den Käufer.

Die Reserved Instance bleibt bis zum Verkauf in Ihrem Besitz. Nach dem Verkauf geben Sie die Kapazitätsreservierungen und die regelmäßigen Rabatte ab. Wenn Sie Ihre Instance weiterhin nutzen, berechnet AWS Ihnen ab dem Zeitpunkt des Verkaufs Ihrer Reserved Instance den On-Demand-Preis.

Wenn Sie nicht genutzte Reserved Instances im Reserved Instance Marketplace verkaufen möchten, müssen Sie bestimmte Kriterien erfüllen.

Weitere Informationen zum Kauf von Reserved Instances im Reserved Instance Marketplace finden Sie im Einkaufen im Reserved Instance-Marketplace.

Inhalt

- Beschränkungen und Einschränkungen
- Registrieren als Verkäufer
- Bankkonto für Auszahlung
- Steuerinformationen

- Preis festsetzen von Reserved Instances
- Auflisten Ihrer Reserved Instances
- Reserved Instance-Angebotsstatus
- Lebenszyklus eines Angebots
- Nach dem Verkauf Ihrer Reserved Instance
- Auszahlung
- Weitergabe von Informationen an den Käufer

Beschränkungen und Einschränkungen

Bevor Sie Ihre nicht genutzten Reservierungen verkaufen können, müssen sich als Verkäufer im Reserved Instance Marketplace registrieren. Weitere Informationen finden Sie unter Registrieren als Verkäufer.

Beim Verkauf von Reserved Instances gelten die folgenden Begrenzungen und Einschränkungen:

- Es können nur regionale und zonale Amazon EC2 Standard Reserved Instances über den Reserved-Instance-Marketplace verkauft werden.
- Amazon EC2 Convertible Reserved Instances können nicht über den Reserved Instance Marketplace verkauft werden.
- Reserved Instances für andere AWS-Services wie Amazon RDS und Amazon ElastiCache können nicht über den Reserved-Instance-Marketplace verkauft werden.
- Die verbleibende Laufzeit der Standard-Reserved Instance muss mindestens einen Monat betragen.
- Sie können keine Standard-Reserved Instance in einer Region verkaufen, die standardmäßig deaktiviert ist.
- Der Mindestpreis im Reserved Instance Marketplace beträgt 0,00 USD.
- Sie können Reserved Instances vom Typ „No Upfront“ (Keine Vorauszahlung), „Partial Upfront“ (Teilweise Vorauszahlung) oder „All Upfront“ (Komplette Vorauszahlung) im Reserved Instance Marketplace verkaufen, sofern sie seit mindestens 30 Tagen in Ihrem Konto aktiv sind. Wenn es eine Vorauszahlung für eine Reserved Instance gibt, kann diese erst dann verkauft werden, wenn AWS die Vorauszahlung erhalten hat.
- Sie können eine Reserved Instance im Reserved Instance Marketplace nicht verkaufen, wenn Sie sie mit einem Mengenrabatt gekauft haben.

- Sie können Ihr Angebot im Reserved Instance Marketplace nicht direkt bearbeiten. Sie können jedoch das Angebot stornieren und dann ein neues Angebot mit neuen Parametern erstellen. Weitere Informationen finden Sie unter Preis festsetzen von Reserved Instances. Sie können Ihre Reserved Instances außerdem vor dem Verkaufsangebot ändern. Weitere Informationen finden Sie unter Ändern von Reserved Instances.
- AWS berechnet eine Servicegebühr von 12 Prozent des Gesamtvorauszahlungspreises für jede im Reserved Instance Marketplace zu verkaufende Standard-Reserved-Instance. Der Vorauszahlungspreis ist der Preis, der dem Verkäufer für die Standard-Reserved Instance berechnet wird.
- Wenn Sie sich als Verkäufer registrieren, muss die von Ihnen angegebene Bank eine US-Adresse aufweisen. Weitere Informationen finden Sie unter Zusätzliche Anforderungen für Verkäufer für kostenpflichtige Produkte im AWS Marketplace-Verkäuferhandbuch.
- Amazon Web Services India Private Limited (AWS India)-Kunden können sich nicht als Verkäufer auf dem EC2 Reserved Instances Marketplace registrieren und können nicht Reserved Instances auf dem EC2 Reserved Instance Marketplace verkaufen, selbst wenn sie über ein US-Bankkonto verfügen. Weitere Informationen finden Sie unter Was sind die Unterschiede zwischen AWS-Konten und AWS-Indien-Konten?
- Wenn Sie Ihren Datensatz-Verkäufer zu Amazon Web Services India Private Limited (AWS India) ändern, werden Sie als Verkäufer vom EC2 Reserved Instance Marketplace abgemeldet und alle Ihre bestehenden aktiven Angebote auf dem EC2 Reserved Instance Marketplace werden entfernt. Um Ihren Verkäuferstatus wiederherzustellen, müssen Sie den Standort Ihres Kontos in ein anderes Land als Indien ändern und die Verkäuferregistrierung erneut abschließen.

Registrieren als Verkäufer

> **Note**
>
> Nur der Root-Benutzer des AWS-Kontos kann ein Konto als Verkäufer registrieren.

Für den Verkauf auf dem Reserved Instance Marketplace müssen Sie sich zuerst als Verkäufer registrieren. Während der Registrierung müssen Sie folgende Informationen angeben:

- Bankdaten: AWS benötigt Ihre Bankdaten, um Auszahlungen für den Verkauf von Reservierungen vornehmen zu können. Die angegebene Bank muss über eine US-Anschrift verfügen. Weitere Informationen finden Sie unter Bankkonto für Auszahlung.

- Tax information (Steuerinformationen) — Alle Verkäufer sind verpflichtet, ein Interview zu den Steuerinformationen durchzuführen, um die erforderlichen steuerlichen Meldepflichten zu ermitteln. Weitere Informationen finden Sie unter Steuerinformationen.

Nach dem Eingang Ihrer ausgefüllten Verkäuferregistrierung bei AWS erhalten Sie eine E-Mail mit einer Bestätigung Ihrer Registrierung. Die E-Mail informiert Sie darüber, dass Sie mit dem Verkauf im Reserved Instance Marketplace beginnen können.

Bankkonto für Auszahlung

AWS benötigt Ihre Bankdaten, um Auszahlungen für den Verkauf von Reserved Instance vornehmen zu können. Die angegebene Bank muss über eine US-Anschrift verfügen. Weitere Informationen finden Sie unter Zusätzliche Anforderungen für Verkäufer für kostenpflichtige Produkte im AWS Marketplace-Verkäuferhandbuch.

So registrieren Sie ein Standardbankkonto für Auszahlungen

1. Öffnen Sie die Seite Reserved Instance Marketplace Seller Registration und melden Sie sich mit Ihren AWS-Anmeldeinformationen an.
2. Geben Sie auf der Seite Manage Bank Account die folgenden Informationen zur Bank an:
   - Name des Bankkontoinhabers
   - Bankleitzahl
   - Kontonummer
   - Kontotyp

> **Note**
>
> Wenn Sie ein Unternehmenskonto verwenden, müssen Sie die Informationen zum Bankkonto per Fax senden(+1 206-765-3424).

Nach der Registrierung wird das angegebene Bankkonto als Standardkonto mit ausstehender Verifizierung durch die Bank eingerichtet. Die Verifizierung eines neuen Bankkontos kann bis zu zwei Wochen dauern. Während dieser Zeit können Sie keine Auszahlungen erhalten. Bei einem bereits etablierten Konto dauert es normalerweise ca. zwei Tage, bis die Auszahlung abgeschlossen ist.

So ändern Sie das Standardbankkonto für Auszahlungen

1. Öffnen Sie die Seite Reserved Instance Marketplace Seller Registration und melden Sie sich mit dem Konto an, das Sie bei der Registrierung verwendet haben.
2. Fügen Sie auf der Seite Manage Bank Account ein neues Bankkonto hinzu oder bearbeiten Sie das Standardbankkonto.

Steuerinformationen

Ihr Verkauf von Reserved Instances kann transaktionsbasierten Steuern unterliegen (z. B. Mehrwertsteuer). Sie sollten gemeinsam mit der Steuer-, Rechts-, Buchhaltungs- oder Finanzabteilung Ihres Unternehmens prüfen, ob Transaktionssteuern anfallen. Sie sind für die Erfassung und die Zahlung von entsprechenden Steuern an die jeweilige Behörde verantwortlich.

Im Rahmen des Registrierungsprozesses für Verkäufer müssen Sie im Seller Registration Portal ein Steuer-Interview durchführen. In dem Interview werden Ihre Steuerinformationen erfasst und ein IRS-Formular W-9, W-8BEN oder W-8BEN-E ausgefüllt, das verwendet wird, um alle erforderlichen steuerlichen Meldepflichten zu ermitteln.

Die im Rahmen des Steuer-Interviews anzugebenden Steuerinformationen hängen ggf. davon ab, ob Sie als Privatperson oder als Unternehmen tätig sind und ob Sie oder Ihr Unternehmen eine US-amerikanische oder nicht-amerikanische natürliche oder juristische Person sind. Berücksichtigen Sie beim Ausfüllen des Steuer-Interviews Folgendes:

- Die von AWS bereitgestellten Informationen (inkl. der Informationen in diesem Thema) stellen keine Steuer-, Rechts- oder Expertenberatung dar. Um die möglicherweise für Ihr Unternehmen geltenden Anforderungen für das IRS-Reporting zu ermitteln und bei weiteren Fragen, sprechen Sie bitte Ihren Steuerberater, Rechtsberater oder Unternehmensberater an.
- Beantworten Sie alle Fragen und geben Sie alle angeforderten Informationen ein, um die IRS-Reporting-Anforderungen möglichst vollständig zu erfüllen.
- Überprüfen Sie Ihre Antworten. Vermeiden Sie Tippfehler oder fehlerhafte Steueridentifikationsnummern. Diese können dazu führen, dass das Steuerformular ungültig ist.

Basierend auf Ihren Antworten auf Steuerbenachrichtigungen und IRS-Meldeschwellen reicht Amazon ggf. das Formular 1099-K ein. Amazon sendet eine Kopie Ihres 1099-K-Formulars am oder vor dem 31. Januar des Jahres, das auf das Jahr folgt, in dem Ihr Steuerkonto die

Schwellenwerte erreicht. Wenn Ihr Konto den Grenzwert im Jahr 2018 erreicht, wird Ihr Formular 1099-K beispielsweise am oder vor dem 31. Januar 2019 verschickt.

Weitere Informationen zu den IRS-Anforderungen und dem Formular 1099-K finden Sie unter Häufig gestellte Fragen zum Formular 1099-K auf der IRS-Website.

Preis festsetzen von Reserved Instances

Wenn Sie die Gebühr für Ihre Reserved Instances festlegen, beachten Sie Folgendes:

- Vorabgebühr – Die Vorabgebühr ist die einzige Gebühr, die Sie für von Ihnen verkaufte Reserved Instances festlegen können. Die Vorabgebühr ist die einmalige Gebühr, die der Käufer beim Kauf der jeweiligen Reserved Instance bezahlt.

  Da sich der Wert der Reserved Instances im Laufe der Zeit verringert, kann AWS standardmäßig eine monatliche Preisreduzierung festlegen (mit einem identischen Wert für jeden Monat). Sie können jedoch entsprechend dem Verkaufszeitpunkt Ihrer Reservierung abweichende Preise im Voraus festlegen. Wenn Ihre Reserved Instance beispielsweise noch über eine verbleibende Laufzeit von neun Monaten verfügt, können Sie den akzeptablen Betrag für einen Kauf dieser Reserved Instance innerhalb der verbleibenden neun Monate festlegen. Sie können einen anderen Preis für fünf verbleibende Monate und einen weiteren Preis für einen verbleibenden Monat festlegen.

  Der Mindestpreis im Reserved Instance Marketplace beträgt 0,00 USD.
- Limits – Die folgenden Limits für den Verkauf von Reserved Instances gelten für die Lebensdauer Ihres AWS-Konto. Diese sind keine jährlichen Limits und sie können nicht erhöht werden.
  - Sie können bis zu 50 000 USD in Reserved Instances verkaufen.
  - Sie können bis zu 5 000 Reserved Instances verkaufen.
- Kann nicht bearbeitet werden – Sie können Ihr Angebot nicht direkt bearbeiten. Sie können jedoch das Angebot stornieren und dann ein neues Angebot mit neuen Parametern erstellen.
- Kann storniert werden – Sie können ein Angebot jederzeit stornieren (solange es den Status `active` aufweist). Sie können das Angebot nicht stornieren, wenn es bereits einem Verkauf zugeordnet oder für diesen verarbeitet wird. Wenn einige Instances aus Ihrem Angebot zugeordnet sind, und Sie das Angebot stornieren, werden nur die noch nicht zugeordneten Instances aus dem Angebot entfernt.

Auflisten Ihrer Reserved Instances

Als registrierter Verkäufer können Sie eine oder mehrere Reserved Instances. Sie können entweder alle über ein Angebot verkaufen oder diese in Teilen verkaufen. Des Weiteren können Sie Reserved Instances in jeder Konfiguration aus Instance-Typ, Plattform und Umfang anbieten.

Die Konsole ermittelt einen vorgeschlagenen Preis. Sie überprüft, ob Angebote entsprechend Ihrer Reserved Instance vorliegen, und gibt das Angebot mit dem niedrigsten Preis zurück. Andernfalls berechnet sie einen vorgeschlagenen Preis anhand der Kosten der Reserved Instance für die verbleibende Zeit. Wenn der berechnete Preis unter 1,01 USD liegt, beträgt der vorgeschlagene Preis 1,01 USD.

Sie können Ihr Angebot stornieren. Wurde ein Angebot bereits verkauft, so gilt die Stornierung nicht für den bereits verkauften Teil. Nur noch nicht verkaufte Teile des Angebotes werden aus dem Reserved Instance Marketplace entfernt.

Console

So können Sie eine Reserved Instance im Reserved Instance Marketplace auflisten

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances aus.
3. Wählen Sie das aufzulistende Reserved Instances aus, und wählen Sie Actions (Aktionen), Sell Reserved Instances (Verkaufen).
4. Wählen Sie auf der Seite Configure Your Reserved Instances Listing in den entsprechenden Spalten die Anzahl der zu verkaufenden Instances sowie den Vorauszahlungspreis für die verbleibende Laufzeit aus. Sehen Sie sich über den Pfeil neben der Spalte Months Remaining die Wertveränderung Ihrer Reservierung an.
5. Wenn Sie ein fortgeschrittener Benutzer sind und die Preisgestaltung anpassen möchten, können Sie unterschiedliche Werte für die nachfolgenden Monate eingeben. Wählen Sie Reset aus, um die standardmäßige, lineare Preisreduzierung wiederherzustellen.
6. Wählen Sie Continue aus, sobald Sie mit der Konfiguration fertig sind.
7. Bestätigen Sie die Details Ihres Angebotes auf der Seite Confirm Your Reserved Instances Listing. Wählen Sie List Reserved Instance aus, sobald alles korrekt ist.

So zeigen Sie Ihre Angebote in der Amazon-EC2-Konsole an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Reserved Instances aus.
3. Wählen Sie das Reserved Instance aus, das Sie aufgelistet haben, und wählen Sie die Registerkarte My Listings (Meine Auflistungen) am unteren Rand der Seite.

AWS CLI

So verwalten Sie Reserved Instances im Reserved Instance Marketplace

1. Rufen Sie über den Befehl Reserved Instancesdescribe-reserved-instances eine Liste Ihrer ab. Notieren Sie sich die ID der Reserved Instance, die Sie auflisten möchten.
2. Verwenden Sie den Befehl create-reserved-instances-listing. Sie müssen die ID der Reserved Instance, die Anzahl der Instances und den Preisplan angeben.
3. Verwenden Sie den Befehl describe-reserved-instances-listings, um Ihr Angebot anzuzeigen.
4. Verwenden Sie den Befehl cancel-reserved-instances-listings, um Ihr Angebot zu stornieren.

PowerShell

So verwalten Sie Reserved Instances im Reserved Instance Marketplace

1. Rufen Sie mit dem cmdlet Get-EC2ReservedInstance eine Liste Ihrer Reserved Instances ab. Notieren Sie sich die ID der Reserved Instance, die Sie auflisten möchten.
2. Verwenden Sie das cmdlet New-EC2ReservedInstancesListing. Sie müssen die ID der Reserved Instance, die Anzahl der Instances und den Preisplan angeben.
3. Verwenden Sie das cmdlet Get-EC2ReservedInstancesListing, um Ihr Angebot anzuzeigen.
4. Verwenden Sie das cmdlet Stop-EC2ReservedInstancesListing, um Ihr Angebot zu stornieren.

Reserved Instance-Angebotsstatus

Listing State (Angebotsstatus) auf der Registerkarte My Listings (Meine Angebote) der Reserved Instances-Seite zeigt den Status Ihrer aktuellen Angebote an:

Die in Listing State angezeigten Informationen stellen den Status Ihres Angebots im Reserved Instance Marketplace dar. Er unterscheidet sich im Status in der Spalte State auf der Seite Reserved Instances. Diese State-Information bezieht sich auf Ihre Reservierung.

- Active — Das Angebot steht zum Kauf zur Verfügung.

- Cancelled: Das Angebot wurde storniert und steht nicht im Reserved Instance Marketplace zum Kauf zur Verfügung.
- Closed — Die Reserved Instance wird nicht angeboten. Eine Reserved Instance kann `closed` sein, da der Verkauf des Angebots abgeschlossen ist.

Lebenszyklus eines Angebots

Wenn alle Instances in Ihrem Angebot zugeordnet und verkauft sind, zeigt die Registerkarte My Listings in Total instance count die gleiche Anzahl wie in Sold an. Es sind keine Instances mit dem Status Available mehr für Ihr Angebot vorhanden. Sein Status lautet `closed`.

Wenn nur ein Teil Ihres Angebots verkauft wird, zieht AWS die Reserved Instances im Angebot zurück und erstellt die Anzahl von Instances, die den verbleibenden Reserved Instances entspricht. Die Angebots-ID und das entsprechende Angebot bleiben mit weniger zu verkaufenden Reservierungen weiterhin aktiv.

Alle weiteren Verkäufe von Reserved Instances in diesem Angebot werden genauso verarbeitet. Wenn alle Reserved Instances in einem Angebot verkauft werden, markiert AWS das Angebot als `closed`.

Sie erstellen beispielsweise ein Angebot wie Reserved Instances listing ID 5ec28771-05ff-4b9b-aa31-9e57dexample mit einer Angebotsmenge von 5.

Die Registerkarte My Listings auf der Konsolenseite Reserved Instance zeigt das Angebot folgendermaßen an:

Reserved Instance listing ID 5ec28771-05ff-4b9b-aa31-9e57dexample

- Total reservation count = 5
- Sold = 0
- Available = 5
- Status = active

Ein Käufer kauft zwei der Reservierungen. Es verbleiben also drei zu verkaufende Reservierungen. Da es sich um einen teilweisen Verkauf handelt, erstellt AWS eine neue Reservierung mit der Anzahl drei für die verbleibenden Reservierungen.

So sieht Ihr Angebot auf der Registerkarte My Listings aus:

Reserved Instance listing ID 5ec28771-05ff-4b9b-aa31-9e57dexample

- Total reservation count = 5
- Sold = 2
- Available = 3
- Status = active

Sie können Ihr Angebot stornieren. Wurde ein Angebot bereits verkauft, so gilt die Stornierung nicht für den bereits verkauften Teil. Nur noch nicht verkaufte Teile des Angebotes werden aus dem Reserved Instance Marketplace entfernt.

Nach dem Verkauf Ihrer Reserved Instance

Wenn Ihre Reserved Instance verkauft wird, sendet AWS Ihnen eine E-Mail-Benachrichtigung. Sie erhalten für jeden Tag mit einer beliebigen Aktivität eine E-Mail-Benachrichtigung zu allen Aktivitäten des Tages. Zu den Aktivitäten kann gehören, dass Sie eine Auflistung erstellen oder verkaufen oder dass AWS Guthaben auf Ihr Konto sendet.

Console

So verfolgen Sie den Status eines Reserved-Instance-Angebots in der Konsole:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Navigationsseite Reserved Instances aus.
3. Suchen Sie auf der Registerkarte Meine Angebote den Wert von Angebots-Status. Die Registerkarte enthält außerdem Informationen zur Laufzeit, zum Angebotspreis und eine Aufschlüsselung, wie viele Instances im Angebot verfügbar, ausstehend, verkauft und storniert sind.

AWS CLI

So verfolgen Sie den Status eines Reserved-Instance-Angebots in der Konsole:

Verwenden Sie den Befehl describe-reserved-instances-listings mit dem passenden Filter, um Informationen zu Ihren Angeboten abzurufen.

```
aws ec2 describe-reserved-instances-listings
```

PowerShell

So verfolgen Sie den Status eines Reserved-Instance-Angebots in der Konsole:

Verwenden Sie das cmdlet Get-EC2ReservedInstancesListing.

```
Get-EC2ReservedInstancesListing
```

Auszahlung

Sobald AWS die Geldmittel vom Käufer erhält, wird eine E-Mail zum Verkauf der Reserved Instance an das registrierte E-Mail-Konto des Besitzers gesendet.

AWS sendet eine ACH-Überweisung (Automated Clearing House) an Ihr angegebenes Bankkonto. Dieser Transfer findet normalerweise zwischen einem und drei Tagen nach dem Verkauf Ihrer Reserved Instance statt. Die Auszahlung findet einmal pro Tag statt. Sie erhalten eine E-Mail mit einem Auszahlungsbericht, nachdem die Mittel freigegeben wurden. Berücksichtigen Sie, dass Sie erst dann eine Auszahlung erhalten können, wenn AWS eine Verifizierung von Ihrer Bank erhalten hat. Dieser Vorgang kann bis zu zwei Wochen dauern.

Die verkaufte Reserved Instance wird auch weiterhin in der Beschreibung Ihrer Reserved Instances angezeigt.

Sie erhalten eine Barauszahlung für Ihre Reserved Instances über eine Überweisung direkt auf Ihr Bankkonto. AWS erhebt eine Servicegebühr von 12 Prozent der gesamten Vorauszahlung jeder Reserved Instance, die Sie im Reserved Instance Marketplace verkaufen.

Weitergabe von Informationen an den Käufer

Wenn Sie im Reserved Instance Marketplace verkaufen, teilt AWS den juristischen Namen Ihres Unternehmens auf dem Beleg des Käufers entsprechend der US-Vorschriften mit. Wenn der Käufer den Support anruft, da er Sie zur Anforderung einer Rechnung oder aus einem anderen Grund kontaktieren möchte, muss AWS dem Käufer möglicherweise Ihre E-Mail-Adresse für einen direkten Kontakt bereitstellen.

Aus denselben Gründen erhalten die Verkäufer über den Auszahlungsbericht die Postleitzahl und das Land des Käufers. Als Verkäufer benötigen Sie diese Informationen möglicherweise für die anfallenden Transaktionssteuern (z. B. Mehrwertsteuer).

AWS bietet keine steuerliche Beratung. Wenn Ihr Steuerexperte jedoch feststellt, dass Sie bestimmte zusätzliche Informationen benötigen, können Sie den Support kontaktieren.

Ändern von Reserved Instances

Wenn sich Ihre Anforderungen ändern, können Sie Ihre Standard- oder Convertible Reserved Instances ändern. So profitieren Sie auch weiterhin von den Rabatten. Sie können Attribute wie die Availability Zone, die Instance-Größe (innerhalb derselben Instance-Familie und -Generation) und den Umfang Ihrer Reserved Instance ändern.

> **Note**
>
> Sie können auch eine Convertible Reserved Instance gegen eine andere Convertible Reserved Instance mit einer anderen Konfiguration austauschen. Weitere Informationen finden Sie unter Austauschen von Convertible Reserved Instances.

Sie können Ihre kompletten Reserved Instances oder einen Teil ändern. Sie können Ihre ursprünglichen Reserved Instances in zwei oder mehr neue Reserved Instances aufteilen. Wenn Sie beispielsweise über eine Reservierung für 10 Instances in `us-east-1a` verfügen und Sie 5 Instances in `us-east-1b` verschieben möchten, führt die Änderungsanforderung zu zwei neuen Reservierungen: Eine für 5 Instances in `us-east-1a`, und eine für 5 Instances in `us-east-1b`.

Sie können außerdem zwei oder mehr Reserved Instances in einer einzige Reserved Instance zusammenführen. Wenn Sie beispielsweise vier `t2.small` Reserved Instances mit jeweils einer Instance haben, können Sie diese in einer `t2.large` Reserved Instance zusammenführen. Weitere Informationen finden Sie unter Support für das Ändern von Instance-Größen.

Nach der Änderung wird der Rabatt für die Reserved Instances nur auf Instances mit den neuen Parametern angewendet. Wenn Sie beispielsweise die Availability Zone einer Reservierung ändern, werden die Kapazitätsreservierung und die Preisvorteile automatisch auf die Instance-Nutzung in der neuen Availability Zone angewendet. Solange keine anderen gültigen Reservierungen in Ihrem Konto vorhanden sind, werden Instances, die nicht mehr mit den neuen Parametern übereinstimmen, über den On-Demand-Tarif abgerechnet.

Wenn Ihre Änderungsanforderung erfolgreich ist:

- Die geänderte Reservierung gilt sofort. Die Preisvorteile werden eine Stunde nach Ihrer Änderungsanforderungen auf die neuen Instances angewendet. Wenn Sie beispielsweise Ihre Reservierung um 21:15 Uhr erfolgreich ändern, wird der Preisvorteil um 21:00 Uhr auf Ihre neue Instance übertragen. Sie können das Datum des Inkrafttretens der abgeänderten Reserved Instances mithilfe des Befehls describe-reserved-instances abrufen.

- Die ursprüngliche Reservierung wird zurückgezogen. Ihr Enddatum entspricht dem Startdatum der neuen Reservierung. Das Enddatum der neuen Reservierung entspricht dem Enddatum der ursprünglichen Reserved Instance. Wenn Sie eine dreijährige Reservierung mit einer verbleibenden Laufzeit von 16 Monaten ändern, hat die resultierende, geänderte Reservierung eine Laufzeit von 16 Monaten. Das Enddatum entspricht dem der ursprünglichen Reservierung.
- Die geänderte Reservierung zeigt einen Festpreis von 0 USD statt des Festpreises der ursprünglichen Reservierung an.
- Der Festpreis der geänderten Reservierung wirkt sich nicht auf die Rabattstufenpreisberechnungen für Ihr Konto aus. Diese basieren auf dem Festpreis der ursprünglichen Reservierung.

Wenn Ihre Änderungsanforderung fehlschlägt, verbleiben Ihre Reserved Instances in der ursprünglichen Konfiguration. Sie stehen direkt für eine weitere Änderungsanforderung zur Verfügung.

Es gibt keine Gebühr für die Änderung. Sie erhalten keine neuen Rechnungen.

Sie können Ihre Reservierungen beliebig oft ändern. Sie können jedoch nach der Übermittlung keine ausstehenden Änderungsanforderungen ändern oder diese stornieren. Nach der erfolgreichen Durchführung der Änderungen. So können sie die Änderungen bei Bedarf rückgängig machen.

Inhalt

- Anforderungen und Einschränkungen für Änderungen
- Support für das Ändern von Instance-Größen
- Senden von Änderungsanforderungen
- Fehlerbehebung bei Änderungsanforderungen

Anforderungen und Einschränkungen für Änderungen

Sie können diese Attribute wie folgt ändern.

Änderbares Attribut	Unterstützte Plattformen	Einschränkungen und Überlegungen
Ändern der Availability Zones innerhalb einer Region	Linux und Windows	-

Änderbares Attribut	Unterstützte Plattformen	Einschränkungen und Überlegungen
Ändern des Umfangs von einer Availability Zone auf eine Region und entgegengesetzt	Linux und Windows	Eine zonale Reserved Instance ist auf eine Availability Zone ausgerichtet und reserviert die Kapazität in dieser Availability Zone. Wenn Sie den Umfang von einer Availability Zone auf eine Region ändern (mit anderen Worten, von zonal zu regional), verlieren Sie den Vorteil der Kapazitätsreservierung. Eine regionale Reserved Instance ist auf eine Region ausgerichtet. Der Reserved-Instance-Rabatt gilt für die Instance-Nutzung in jeder Availability Zone in dieser Region. Darüber hinaus gilt der Reserved-Instance-Rabatt auf die Instance-Nutzung in allen Größen in der ausgewählten Instance-Familie. Wenn Sie den Umfang von einer Region auf eine Availability Zone ändern (mit anderen Worten, von regional zu zonal), verlieren Sie die Flexibilität für die Availability Zone und die Instance-Größe (falls zutreffend). Weitere Informationen finden Sie unter Wie Reserved-

Änderbares Attribut	Unterstützte Plattformen	Einschränkungen und Überlegungen
		Instances-Rabatte angewendet werden.
Ändern der Instance-Größe innerhalb desselben Instance-Familie und -Generation	Nur Linux/UNIX Die Flexibilität der Instance-Größe ist für Reserved Instances auf den anderen Plattformen nicht verfügbar, darunter fallen Linux mit SQL Server Standard, Linux mit SQL Server Web, Linux mit SQL Server Enterprise, Red Hat Enterprise Linux, SUSE Linux, Windows, Windows mit SQL Standard, Windows mit SQL Server Enterprise und Windows mit SQL Server Web.	Die Reservierung muss die Standard-Tenancy verwenden. Einige Instance-Familien werden nicht unterstützt, da keine anderen Größen verfügbar sind. Weitere Informationen finden Sie unter . Support für das Ändern von Instance-Größen

Voraussetzungen

Amazon EC2 verarbeitet Ihre Änderungsanforderungen, sofern eine ausreichende Kapazität für Ihre neue Konfiguration zur Verfügung steht (falls zutreffend). Außerdem müssen die folgenden Bedingungen zutreffen:

- Die Reserved Instance kann nicht vor dem Kauf oder beim Kauf geändert werden.
- Die Reserved Instance muss aktiv sein.
- Es dürfen keine Änderungsanforderungen ausstehen.
- Die Reserved Instance ist nicht im Reserved Instance Marketplace aufgelistet.
- Der Ressourcenbedarf der Instance-Größe der Origianlreservierung und der neuen Konfiguration müssen übereinstimmen. Weitere Informationen finden Sie unter Support für das Ändern von Instance-Größen.

- Die Original-Reserved Instances müssen entweder Standard-Reserved Instances oder Convertible Reserved Instances, aber nicht eine Kombination aus beiden sein.
- Die Original-Reserved Instances müssen in derselben Stunde ablaufen, wenn es sich um Standard-Reserved Instances handelt.
- Um die Instance-Größe zu ändern, muss die Reserved Instance die Flexibilität der Instance-Größe unterstützen. Eine Liste der Reserved Instances, die die Flexibilität der Instance-Größe nicht unterstützen, finden Sie unter Flexibilität bezüglich der Instance-Größe.

Support für das Ändern von Instance-Größen

Sie können die Instance-Größe einer Reserved Instance ändern, wenn die folgenden Anforderungen erfüllt sind.

Voraussetzungen

- Die Plattform ist Linux/UNIX.
- Sie müssen eine andere Instance-Größe in derselben Instance-Familie (gekennzeichnet durch einen Buchstaben, z. B. T) und Generation (gekennzeichnet durch eine Zahl, z. B. 2) auswählen.

  Sie können beispielsweise eine Reserved Instance von `t2.small` auf `t2.large` ändern, da beide zur gleichen T2-Familie und -Generation gehören. Sie können eine Reserved Instance jedoch nicht von T2 auf M2 oder von T2 auf T3 ändern, da in diesen beiden Beispielen die Ziel-Instance-Familie und -Generation nicht mit der ursprünglichen Reserved Instance identisch sind.
- Sie können die Instance-Größe einer Reserved Instance nur ändern, wenn sie die Instance-Größenflexibilität unterstützt. Eine Liste der Reserved Instances, die die Flexibilität der Instance-Größe nicht unterstützen, finden Sie unter Flexibilität bezüglich der Instance-Größe.
- Sie können die Instance Größe von Reserved Instances für `t1.micro`-Instances nicht ändern, da `t1.micro` nur über eine Größe verfügt.
- Das Original und die neue Reserved Instance müssen denselben Ressourcenbedarf für die Instance-Größe aufweisen.

Inhalt

- Ressourcenbedarf für die Instance-Größe
- Normalisierungsfaktoren für Bare Metal-Instances

Ressourcenbedarf für die Instance-Größe

Jede Reserved Instance hat einen Ressourcenbedarf für die Instance-Größe. Dieser wird über den Normalisierungsfaktor der Instance-Größe und die Anzahl der Instances in der Reservierung bestimmt. Wenn Sie die Instance-Größen in einer Reserved Instance ändern, muss der Ressourcenbedarf der neuen Konfiguration mit dem der ursprünglichen Konfiguration übereinstimmen. Andernfalls wird die Änderungsanforderung nicht verarbeitet.

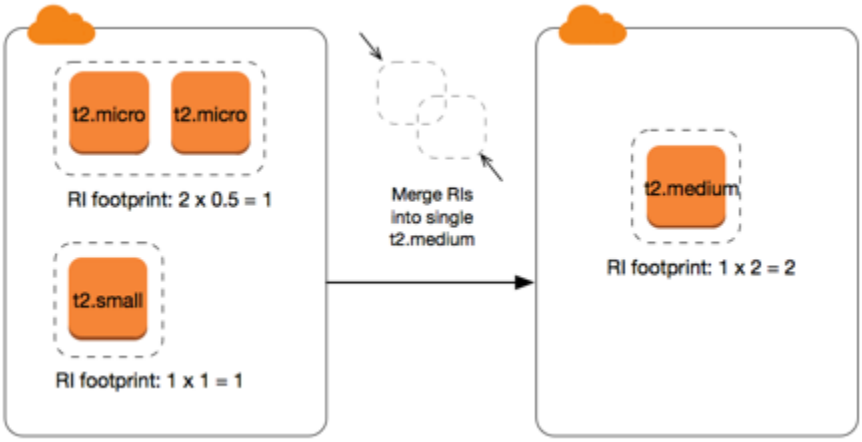
Um den Ressourcenbedarf für die Instance-Größe einer Reserved Instance zu berechnen, multiplizieren Sie die Anzahl der Instances mit dem Normalisierungsfaktor. In der Amazon EC2-Konsole wird der Normalisierungsfaktor in Einheiten gemessen. In der folgenden Tabelle wird der Normalisierungsfaktor für die Instance-Größen in einer Instance-Familie beschrieben. `t2.medium` hat beispielsweise einen Normalisierungsfaktor von 2. Daher hat eine Reservierung für vier `t2.medium`-Instances einen Ressourcenbedarf von 8 Einheiten.

Instance-Größe	Normalisierungsfaktor
nano	0,25
micro	0.5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72

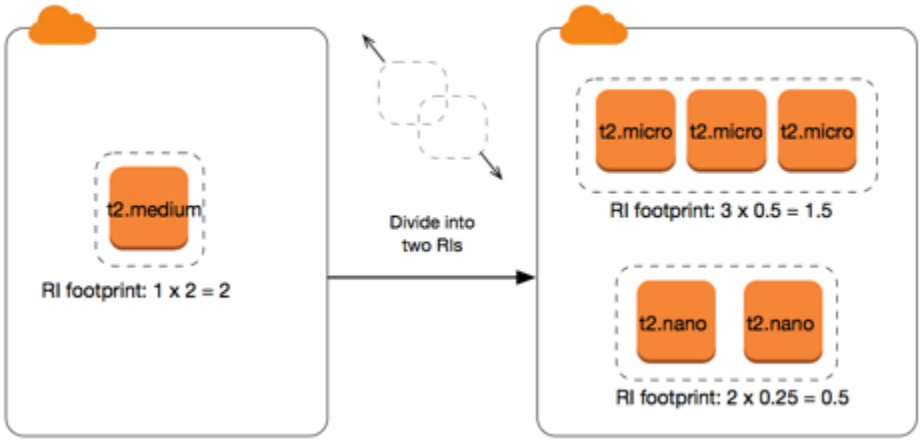
Instance-Größe	Normalisierungsfaktor
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448
112xlarge	896

Sie können Ihre Reservierungen unterschiedlichen Instance-Größen in derselben Instance-Familie zuweisen, sofern der Ressourcenbedarf für die Instance-Größe Ihrer Reservierung gleichbleibt. Beispielsweise können Sie eine Reservierung für eine `t2.large`-Instance (1 @ 4 Einheiten) in vier `t2.small`-Instances (4 @ 1 Einheit) unterteilen. Ebenso können Sie eine Reservierung für vier `t2.small`-Instances in einer `t2.large`-Instance kombinieren. Sie können Ihre Reservierung für zwei `t2.small`-Instances jedoch nicht in eine `t2.large`-Instance ändern, da der Ressourcenbedarf der neuen Reservierung (4 Einheiten) größer ist als der Ressourcenbedarf der Originalreservierung (2 Einheiten).

Im folgenden Beispiel haben Sie eine Reservierung mit zwei `t2.micro`-Instances (1 Einheit) und eine Reservierung mit einer `t2.small`-Instance (1 Einheit). Wenn Sie beide Reservierungen mit einer einzigen Reservierung mit einer `t2.medium`-Instance (2 Einheiten) zusammenführen, entspricht der Ressourcenbedarf der neuen Reservierung dem Ressourcenbedarf der kombinierten Reservierungen.



Sie können außerdem eine Reservierung in zwei oder mehr Reservierungen aufteilen. Im folgenden Beispiel haben Sie eine Reservierung mit einer `t2.medium`-Instance (2 Einheiten). Sie können die Reservierung in zwei Reservierungen unterteilen, eine mit zwei `t2.nano`-Instances (0,5 Einheiten) und die andere mit drei `t2.micro`-Instances (1,5 Einheiten).



Normalisierungsfaktoren für Bare Metal-Instances

Sie können eine Reservierung mit `metal`-Instances ändern, die andere Größen innerhalb derselben Instance-Familie verwenden. Ebenso können Sie eine Reservierung mit anderen Instances als Bare Metal-Instances ändern, indem Sie die `metal`-Größe innerhalb derselben Instance-Familie verwenden. Im Allgemeinen hat eine Bare Metal-Instance dieselbe Größe wie die größte verfügbare Instance-Größe innerhalb derselben Instance-Familie. Beispielsweise hat eine `i3.metal`-Instance die gleiche Größe wie eine `i3.16xlarge`-Instance, sodass sie denselben Normalisierungsfaktor haben.

In der folgenden Tabelle wird der Normalisierungsfaktor für die Bare Metal-Instance-Größen in den Instance-Familien mit Bare Metal-Instances beschrieben. Der Normalisierungsfaktor für `metal`-Instances hängt im Gegensatz zu den anderen Instance-Größen von der Instance-Familie ab.

Instance-Größe	Normalisierungsfaktor
a1.metal	32
m5zn.metal | x2iezn.metal z1d.metal	96
c6g.metal | c6gd.metal | i3.metal | m6g.metal | m6gd.metal | r6g.metal | r6gd.metal | x2gd.metal	128
c5n.metal	144
c5.metal | c5d.metal | i3en.metal | m5.metal | m5d.metal | m5dn.metal | m5n.metal | r5.metal | r5b.metal | r5d.metal | r5dn.metal | r5n.metal	192
c6i.metal | c6id.metal | m6i.metal | m6id.metal | r6d.metal | r6id.metal	256
u-18tb1.metal | u-24tb1.metal	448
u-6tb1.metal | u-9tb1.metal | u-12tb1.metal	896

Beispiel: Eine `i3.metal`-Instance hat beispielsweise einen Normalisierungsfaktor von 128. Wenn Sie eine `i3.metal`-Reserved Instance der Amazon Linux/Unix-Plattform mit Standard-Tenancy erwerben, können Sie die Reservierung wie folgt aufteilen:

- Da eine `i3.16xlarge`-Instance dieselbe Größe wie eine `i3.metal`-Instance hat, ist ihr Normalisierungsfaktor 128 (128/1). Die Reservierung für eine `i3.metal`-Instance kann in eine `i3.16xlarge`-Instance geändert werden.
- Da eine `i3.8xlarge`-Instance halb so groß wie eine `i3.metal`-Instance ist, ist ihr Normalisierungsfaktor 64 (128/2). Die Reservierung für eine `i3.metal`-Instance kann in zwei `i3.8xlarge`-Instances aufgeteilt werden.

- Da eine `i3.4xlarge`-Instance ein Viertel der Größe einer `i3.metal`-Instance ist, ist ihr Normalisierungsfaktor 32 (128/4). Die Reservierung für eine `i3.metal`-Instance kann in vier `i3.4xlarge`-Instances aufgeteilt werden.

Senden von Änderungsanforderungen

Bevor Sie Ihre Reserved Instances ändern, sollten Sie die geltenden Einschränkungen lesen. Bevor Sie die Instance-Größe ändern, berechnen Sie den Gesamtumfang der Instance-Größe der ursprünglichen Reservierungen, die Sie ändern möchten, und stellen Sie sicher, dass er mit dem Gesamtumfang der Instance-Größe Ihrer neuen Konfigurationen übereinstimmt.

Console

So ändern Sie Reserved Instances

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Seite Reserved Instances eine oder mehrere zu ändernde Reserved Instances aus und wählen Sie dann Actions (Aktionen), Modify Reserved Instances (Reserved Instances ändern) aus.

   Wenn Ihre Reserved Instances nicht im aktiven Status sind oder nicht geändert werden können, ist Modify Reserved Instances (&ris; ändern) deaktiviert.
3. Der erste Eintrag in der Änderungstabelle zeigt die Attribute der gewählten Reserved Instances sowie mindestens eine Zielkonfiguration an. Die Spalte Units zeigt den Gesamtressourcenbedarf für die Instance-Größe an. Wählen Sie Add für jede neue Konfiguration aus. Ändern Sie die Attribute der einzelnen Konfigurationen nach Ihren Anforderungen.

   - Scope (Bereich): Wählen Sie aus, ob die Konfiguration für eine Availability Zone oder die gesamte Region angewendet wird.
   - Availability Zone: Wählen Sie die erforderliche Availability Zone aus. Nicht für regionale Reserved Instances anwendbar.
   - Instance Type: Wählen Sie den erforderlichen Instance-Typ aus. Die kombinierten Konfigurationen müssen dem Ressourcenbedarf für die Instance-Größe Ihrer ursprünglichen Konfigurationen entsprechen.
   - Count (Anzahl): Geben Sie die Anzahl der Instances an. Um die Reserved Instances in mehrere Konfigurationen aufzuteilen, reduzieren Sie die Anzahl, wählen Sie Add

(Hinzufügen) aus und geben Sie eine Anzahl für die zusätzliche Konfiguration an. Wenn Sie beispielsweise über eine einzelne Konfiguration mit einer Anzahl von 10 verfügen, können Sie deren Anzahl auf 6 ändern und eine Konfiguration mit einer Anzahl von 4 hinzufügen. Durch diesen Vorgang wird die ursprüngliche Reserved Instance zurückgezogen, nachdem die neuen Reserved Instances aktiviert wurden.

4. Klicken Sie auf Continue.
5. Um Ihre Änderung zu bestätigen, wenn Sie die Angabe Ihrer Zielkonfigurationen abgeschlossen haben, wählen Sie Submit Modifications aus.
6. Sie können den Status Ihrer Änderungsanforderung über die Spalte State (Status) auf der Reserved Instances-Seite ablesen. Die folgenden Zustände sind möglich.

   - active (Aktiv) (ausstehende Änderung) – Übergangsstatus für Original-Reserved Instances
   - retired (Veraltet) (ausstehende Änderung) – Übergangsstatus für Original-Reserved Instances, während neue Reserved Instances erstellt werden.
   - veraltet: Reserved Instances erfolgreich geändert und ersetzt
   - aktiv — Einer der Folgenden:
     - Neue Reserved Instances durch eine erfolgreiche Änderungsanforderung erstellt.
     - Ursprüngliche Reserved Instances nach einer fehlgeschlagenen Änderungsanforderung

AWS CLI

So ändern Sie Reserved Instances

Verwenden Sie den Befehl modify-reserved-instances. Sie können die Konfigurationsdetails in einer JSON-Datei angeben.

```
aws ec2 modify-reserved-instances \
    --reserved-instances-ids b847fa93-e282-4f55-b59a-1342f5bd7c02 \
    --target-configurations file://configuration.json
```

So können Sie den Status Ihrer Änderungsanfrage abrufen

Verwenden Sie den Befehl describe-reserved-instances-modifications. Der Status ist `processing`, `fulfilled` oder `failed`.

```
aws ec2 describe-reserved-instances-modifications \
```

```
    --reserved-instances-modification-ids rimod-d3ed4335-b1d3-4de6-ab31-0f13aaf46687
\
    --query ReservedInstancesModifications[].Status
```

PowerShell

So ändern Sie Reserved Instances

Verwenden Sie das cmdlet Edit-EC2ReservedInstance. Sie können die Konfigurationsdetails in einem Objekt des Typs `Amazon.EC2.Model.ReservedInstancesConfiguration` angeben.

```
Edit-EC2ReservedInstance `
    -ReservedInstancesId b847fa93-e282-4f55-b59a-1342f5bd7c02 `
    -TargetConfiguration $configuration
```

So können Sie den Status Ihrer Änderungsanfrage abrufen

Verwenden Sie das cmdlet Get-EC2ReservedInstancesModification. Der Status ist `processing`, `fulfilled` oder `failed`.

```
Get-EC2ReservedInstancesModification `
    -ReservedInstancesModificationId rimod-d3ed4335-b1d3-4de6-ab31-0f13aaf46687 | `
    Select Status
```

Fehlerbehebung bei Änderungsanforderungen

Wenn die angeforderten Zielkonfigurationseinstellungen eindeutig waren, erhalten Sie eine Nachricht zur Verarbeitung Ihrer Anforderung. Zu diesem Zeitpunkt hat Amazon EC2 nur festgestellt, dass die Parameter Ihrer Änderungsanforderung gültig sind. Ihre Änderungsanforderung kann trotzdem während der Verarbeitung aufgrund einer unzureichenden Kapazität fehlschlagen.

In einigen Situationen erhalten Sie möglicherweise eine Nachricht, die eine unvollständige oder fehlgeschlagene Änderungsanforderung anzeigt. Nutzen Sie die Informationen aus diesen Nachrichten als Startpunkt für eine neue Änderungsanforderung. Stellen Sie vor dem Senden der Anforderung sicher, dass Sie die anwendbaren Einschränkungen gelesen haben.

Nicht alle ausgewählten Reserved Instances können für die Änderung verarbeitet werden

Amazon EC2 ermittelt die nicht änderbaren Reserved Instances und führt diese auf. Wenn Sie eine entsprechende Nachricht erhalten, wechseln Sie zur Seite Reserved Instances in der Amazon EC2-Konsole und überprüfen Sie die Informationen für die Reserved Instances.

Fehler bei der Verarbeitung Ihrer Änderungsanforderung

Sie haben eine oder mehrere Reserved Instances für eine Änderung gesendet. Es konnten jedoch nicht alle Anforderungen verarbeitet werden. Abhängig von der Anzahl der zu ändernden Reservierungen können Sie unterschiedliche Versionen der entsprechenden Nachricht erhalten.

Amazon EC2 zeigt die Gründe für die Nicht-Verarbeitung Ihrer Anforderung an. Sie können beispielsweise die gleiche Zielkonfiguration —(eine Kombination aus Availability Zone und Plattform) — für eine oder mehrere Untergruppen der zu ändernden Reserved Instances angegeben haben. Versuchen Sie, die Änderungsanforderung erneut zu senden. Stellen Sie jedoch sicher, dass die Instance-Details der Reservierung übereinstimmen. Stellen Sie außerdem sicher, dass die Zielkonfigurationen für alle zu ändernden Untergruppen einheitlich sind.

Austauschen von Convertible Reserved Instances

Sie können auch eine oder mehrere Convertible Reserved Instances gegen eine andere Convertible Reserved Instance mit einer anderen Konfiguration (einschließlich Instance-Familie, Betriebssystem und Tenancy) austauschen. Es gibt keine Begrenzungen für die Anzahl der Austauschvorgänge. Die neue Convertible Reserved Instance muss jedoch einen identischen oder höheren Wert als die auszutauschenden originalen Convertible Reserved Instances haben.

Wenn Sie Ihre Convertible Reserved Instance austauschen, wird die Anzahl der Instances für Ihre aktuelle Reservierung gegen die Anzahl der Instances ausgetauscht, die einen identischen oder höheren Wert für die Konfiguration der neuen Convertible Reserved Instance abdeckt. Amazon EC2 berechnet die Anzahl der Reserved Instances, die Sie als Ergebnis des Austauschs erhalten können.

Sie können Standard-Reserved Instances nicht austauschen, aber Sie können sie ändern. Weitere Informationen finden Sie unter Ändern von Reserved Instances .

Inhalt

- Anforderungen für den Austausch von Convertible Reserved Instances
- Berechnen der Convertible Reserved Instances-Austausche
- Mischen von Convertible Reserved Instances
- Austauschen eines Teils einer Convertible Reserved Instance
- Senden von Austauschanforderungen

Anforderungen für den Austausch von Convertible Reserved Instances

Amazon EC2 verarbeitet Ihre Austauschanforderung, sofern die folgenden Bedingungen erfüllt sind. Ihr Convertible Reserved Instance muss folgende Eigenschaften erfüllen:

- Aktiv
- Keine ausstehende vorherige Änderungsanforderung
- Es müssen noch mindestens 24 Stunden bis zum Ablauf verbleiben.

Die folgenden Regeln gelten:

- Convertible Reserved Instances müssen gegen andere Convertible Reserved Instances ausgetauscht werden, die derzeit von AWS angeboten werden.
- Convertible Reserved Instances sind einer bestimmten Region zugeordnet, die für die Dauer der Reservierung festgelegt ist. Sie können eine Convertible Reserved Instance nicht gegen eine Convertible Reserved Instance in einer anderen Region eintauschen.
- Um eine zonale Convertible Reserved Instance auszutauschen, muss AWS über genügend Kapazität für den neuen Instance-Typ in der Region verfügen.
- Sie können eine oder mehrere Convertible Reserved Instances jeweils nur durch eine neue Convertible Reserved Instance ersetzen.
- Um einen Teil einer Convertible Reserved Instance auszutauschen, können Sie sie in zwei oder mehrere Reservierungen ändern und dann eine oder mehrere der Reservierungen gegen eine neue Convertible Reserved Instance tauschen. Weitere Informationen finden Sie unter Austauschen eines Teils einer Convertible Reserved Instance. Weitere Informationen zum Anpassen Ihrer Reserved Instances finden Sie unter Ändern von Reserved Instances.
- Alle Convertible Reserved Instances mit Vorauszahlung können gegen Convertible Reserved Instances mit teilweiser Vorauszahlung getauscht werden und umgekehrt.

> **Note**
>
> Liegt der für den Austausch erforderliche Gesamtvorauszahlungsbetrag (Anpassungskosten) unter 0,00 USD, stellt Ihnen AWS automatisch eine Anzahl von Instances in der Convertible Reserved Instance zur Verfügung. Dadurch wird sichergestellt, dass die Anpassungskosten 0,00 USD oder mehr betragen.

> **Note**
>
> Wenn der Gesamtwert (Vorauszahlungspreis + Stundenpreis * Anzahl der verbleibenden Stunden) der neuen Convertible Reserved Instance kleiner ist als der Gesamtwert der ausgetauschten Convertible Reserved Instance, stellt Ihnen AWS automatisch eine Anzahl von Instances in der Convertible Reserved Instance zur Verfügung. Damit wird sichergestellt, dass der Gesamtwert gleich oder höher als der Gesamtwert der ausgetauschten Convertible Reserved Instance ist.

- Um von besseren Preisen zu profitieren, können Sie eine Convertible Reserved Instance ohne Vorauszahlung gegen eine Convertible Reserved Instance mit vollständiger Vorauszahlung oder eine &cri; mit teilweiser Vorauszahlung tauschen.
- Sie können keine Convertible Reserved Instances mit vollständiger Vorauszahlung oder mit teilweiser Vorauszahlung gegen Convertible Reserved Instances ohne Vorauszahlung austauschen.
- Sie können eine Convertible Reserved Instance ohne Vorauszahlung gegen eine andere Convertible Reserved Instance ohne Vorauszahlung nur dann eintauschen, wenn der Stundenpreis der neuen Convertible Reserved Instance gleich oder höher liegt als der Stundenpreis der getauschten Convertible Reserved Instance.

> **Note**
>
> Wenn der Gesamtwert (Stundenpreis * Anzahl der verbleibenden Stunden) der neuen Convertible Reserved Instance kleiner ist als der Gesamtwert der ausgetauschten Convertible Reserved Instance, stellt Ihnen AWS automatisch eine Anzahl von Instances in der Convertible Reserved Instance zur Verfügung. Damit wird sichergestellt, dass der Gesamtwert gleich oder höher als der Gesamtwert der ausgetauschten Convertible Reserved Instance ist.

- Wenn Sie mehrere Convertible Reserved Instances mit verschiedenen Ablaufdaten austauschen, entspricht das Ablaufdatum der neuen Convertible Reserved Instance dem Datum, das am weitesten in der Zukunft liegt.
- Wenn Sie eine einzelne Convertible Reserved Instance austauschen, muss sie dieselbe Laufzeit (1 oder 3 Jahre) wie die neue Convertible Reserved Instance. Wenn Sie mehrere Convertible Reserved Instances mit verschiedenen Laufzeiten mischen, hat die neue Convertible Reserved

Instance eine Laufzeit von 3 Jahren. Weitere Informationen finden Sie unter Mischen von Convertible Reserved Instances.

- Wenn Amazon EC2 eine Convertible Reserved Instance austauscht, wird die zugehörige Reservierung zurückgezogen und das Enddatum der neuen Reservierung übertragen. Nach dem Umtausch legt Amazon EC2 sowohl das Enddatum für die alte Reservierung als auch das Startdatum für die neue Reservierung fest, das dem Datum des Umtausches entspricht. Wenn Sie beispielsweise eine dreijährige Reservierung austauschen, deren Laufzeit noch 16 Monate beträgt, ist die Reservierung eine 16-monatige Reservierung mit demselben Enddatum wie die Reservierung der von Ihnen ausgetauschten Convertible Reserved Instance.

Berechnen der Convertible Reserved Instances-Austausche

Das Wechseln von Convertible Reserved Instances ist kostenfrei. Es fallen jedoch möglicherweise Anpassungskosten an. Hierbei handelt es sich um anteilige Kosten für den Unterschied zwischen den vorher vorhandenen Convertible Reserved Instances und den neuen Convertible Reserved Instances, die Sie im Zuge des Austauschs erhalten.

Jede Convertible Reserved Instance hat eine Liste mit Werten. Der Listenwert wird mit dem Listenwert der Convertible Reserved Instances vergleichen, die Sie anfordern. So wird festgestellt, wie viele Instance-Reservierungen Sie aus dem Austausch erhalten können.

Beispiel: Sie haben eine Convertible Reserved Instance mit einem Listenwert von 1 x 35 USD, die Sie gegen einen neuen Instance-Typ mit einem Listenwert von 10 USD austauschen möchten.

```
$35/$10 = 3.5
```

Sie können Ihre Convertible Reserved Instance gegen eine 10-USD-Convertible Reserved Instances tauschen. Sie können keine halben Reservierungen erwerben. Daher müssen Sie für den restlichen Teil eine zusätzliche Convertible Reserved Instance erwerben:

```
3.5 = 3 whole Convertible Reserved Instances + 1 additional Convertible Reserved
 Instance
```

Die vierte Convertible Reserved Instance hat dasselbe Enddatum wie die anderen drei. Wenn Sie Convertible Reserved Instances mit teilweiser oder vollständiger Vorauszahlung austauschen, zahlen Sie die Anpassungskosten für die vierte Reservierung. Die verbleibenden Vorauszahlungskosten Ihrer Convertible Reserved Instances betragen 500 USD. Die neue Reservierung würde normalerweise auf Umlagebasis 600 USD kosten. Ihnen werden 100 USD berechnet.

```
$600 prorated upfront cost of new reservations - $500 remaining upfront cost of old
 reservations = $100 difference
```

Mischen von Convertible Reserved Instances

Wenn Sie zwei oder mehr Convertible Reserved Instances zusammenführen, muss die Laufzeit der neuen Convertible Reserved Instance mit der Laufzeit der alten Convertible Reserved Instances oder mit der längsten Laufzeit der Convertible Reserved Instances übereinstimmen. Das Ablaufdatum der neuen Convertible Reserved Instance entspricht dem Ablaufdatum, das am weitesten in der Zukunft liegt.

Angenommen, es gibt die folgenden Convertible Reserved Instances in Ihrem Konto:

Reserved Instance ID	Begriff	Ablaufdatum
aaaa1111	1 Jahr	31.12.2018
bbbb2222	1 Jahr	31.07.2018
cccc3333	3 Jahre	30.06.2018
dddd4444	3 Jahre	31.12.2019

- Sie können `aaaa1111` und `bbbb2222` mischen und sie gegen eine neue 1-Jahres-Convertible Reserved Instance tauschen. Sie können sie nicht gegen eine 3-Jahres-Convertible Reserved Instance tauschen. Das Ablaufdatum der neuen Convertible Reserved Instance ist der 31.12.2018.
- Sie können `bbbb2222` und `cccc3333` mischen und sie gegen eine neue 3-Jahres-Convertible Reserved Instance tauschen. Sie können sie nicht gegen eine 1-Jahres-Convertible Reserved Instance tauschen. Das Ablaufdatum der neuen Convertible Reserved Instance ist der 31.07.2018.
- Sie können `cccc3333` und `dddd4444` mischen und sie gegen eine neue 3-Jahres-Convertible Reserved Instance tauschen. Sie können sie nicht gegen eine 1-Jahres-Convertible Reserved Instance tauschen. Das Ablaufdatum der neuen Convertible Reserved Instance ist der 31.12.2019.

Austauschen eines Teils einer Convertible Reserved Instance

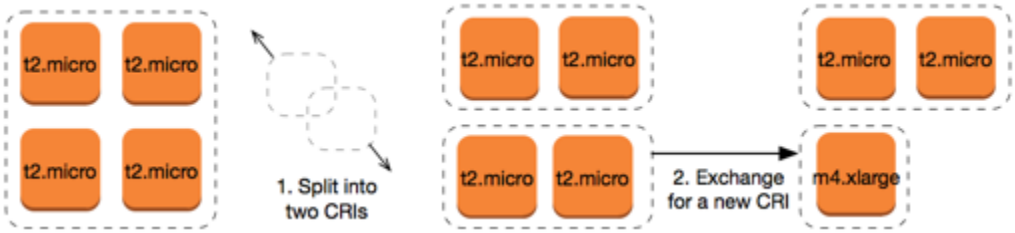
Sie können den Änderungsprozess zum Aufteilen Ihrer Convertible Reserved Instance in kleinere Reservierungen nutzen und dann eine oder mehrere Reservierungen gegen eine neue Convertible

Reserved Instance tauschen. Die folgenden Beispiele veranschaulichen die entsprechende Vorgehensweise.

Example Beispiel: Convertible Reserved Instance mit mehreren Instances

In diesem Beispiel haben Sie eine `t2.micro` Convertible Reserved Instance mit vier Instances in der Reservierung. So wechseln Sie zwei `t2.micro` Instances gegen eine `m4.xlarge` Instance:

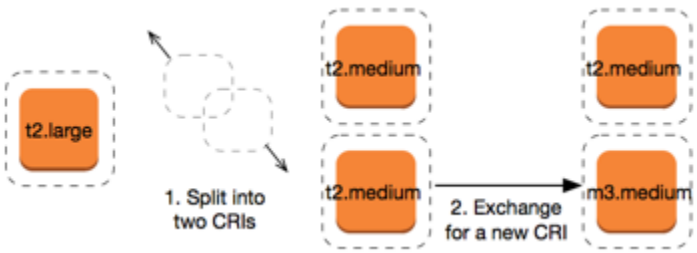
1. Ändern Sie die `t2.micro` Convertible Reserved Instance, indem Sie sie in zwei `t2.micro` Convertible Reserved Instances mit jeweils zwei Instances aufteilen.
2. Wechseln Sie eine der neuen `t2.micro` Convertible Reserved Instances gegen eine `m4.xlarge` Convertible Reserved Instance.



Example Beispiel: Convertible Reserved Instance mit einer einigen Instance

In diesem Beispiel haben Sie eine `t2.large` Convertible Reserved Instance. So ändern Sie sie in eine kleinere `t2.medium` Instance und eine `m3.medium` Instance:

1. Ändern Sie die `t2.large` Convertible Reserved Instance, indem Sie sie in zwei `t2.medium` Convertible Reserved Instances aufteilen. Eine einzelne `t2.large` Instance hat einen genau so großen Instance-Footprint wie zwei `t2.medium` Instances.
2. Wechseln Sie eine der neuen `t2.medium` Convertible Reserved Instances gegen eine `m3.medium` Convertible Reserved Instance.



Weitere Informationen finden Sie unter Support für das Ändern von Instance-Größen und Senden von Austauschanforderungen.

Senden von Austauschanforderungen

Sie können Ihre Convertible Reserved Instances austauschen. Reserved Instances, die ausgetauscht werden, werden außer Betrieb genommen.

Console

So tauschen Sie Convertible Reserved Instances aus

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Reserved Instances aus, wählen Sie die Convertible Reserved Instances für den Austausch aus und wählen Sie Actions (Aktionen), Exchange Reserved Instance (&ri; tauschen) aus.
3. Wählen Sie die Attribute für die gewünschte Konfiguration aus und wählen Sie Find offering (Angebot finden) aus.
4. Wählen Sie ein neues Convertible Reserved Instance aus. Am unteren Bildschirmrand können Sie die Anzahl von Reserved Instances anzeigen, die Sie für den Austausch erhalten, sowie alle zusätzlichen Kosten.
5. Wenn Sie eine zu Ihren Anforderungen passende Convertible Reserved Instance ausgewählt haben, wählen Sie Review (Überprüfen) aus.
6. Wählen Sie Exchange (Austauschen) und dann Close (Beenden).

AWS CLI

So tauschen Sie eine Convertible Reserved Instance aus

1. Suchen Sie mithilfe des Befehls describe-reserved-instances-offerings eine neue Convertible Reserved Instance, die Ihren Anforderungen entspricht.
2. Holen Sie mit dem Befehl get-reserved-instances-exchange-quote ein Angebot für den Austausch ein. Dieses enthält die Anzahl der Reserved Instances, die Sie aus dem Austausch erhalten, und die Anpassungskosten für den Austausch:
3. Führen Sie den Austausch mit dem Befehl accept-reserved-instances-exchange-quote durch.

PowerShell

So tauschen Sie eine Convertible Reserved Instance aus

1. Suchen Sie mithilfe des cmdlets Get-EC2ReservedInstancesOffering nach einer neuen Convertible Reserved Instance, die Ihren Anforderungen entspricht.
2. Holen Sie sich mit dem cmdlet GetEC2-ReservedInstancesExchangeQuote ein Angebot für den Austausch ein. Dieses enthält die Anzahl der Reserved Instances, die Sie aus dem Austausch erhalten, und die Anpassungskosten für den Austausch:
3. Führen Sie den Austausch mit dem cmdlet Approve-EC2ReservedInstancesExchangeQuote durch.

Kontingente für Reserved Instances

Sie können jeden Monat neue Reserved Instances erwerben. Die Anzahl der neuen Reserved Instances, die Sie jeden Monat erwerben können, richtet sich nach Ihrem monatlichen Kontingent. Es lautet wie folgt:

Quota-Beschreibung	Standardkontingent
Neue regionsgebundene Reserved Instances	20 pro Region und Monat
Neue zonengebundene Reserved Instances	20 pro Availability Zone und Monat

In einer Region mit drei Availability Zones beträgt das Standardkontingent beispielsweise 80 neue Reserved Instances pro Monat. Es wird wie folgt berechnet:

- 20 regionsgebundene Reserved Instances für die Region
- Plus 60 zonengebundene Reserved Instances (20 für jede der drei Availability Zones)

Instances im `running`-Status werden auf Ihr Kontingent angerechnet. Instances im Status `pending`, `stopping`, `stopped` und `hibernated` werden nicht auf Ihr Kontingent angerechnet.

Gesamtzahl der erworbenen Reserved Instances anzeigen

Die Anzahl der Reserved Instances, die Sie erwerben, wird durch das Konsolenfeld Instance count (Instance-Anzahl) oder den `InstanceCount`-Parameter (AWS CLI) angezeigt. Wenn Sie neue

Reserved Instances erwerben, wird das Kontingent an der Gesamtzahl der Instances gemessen. Wenn Sie z. B. eine einzelne Reserved-Instance-Konfiguration mit einer Instance-Anzahl von 10 erwerben, wird der Kauf als 10 und nicht als 1 auf Ihr Kontingent angerechnet.

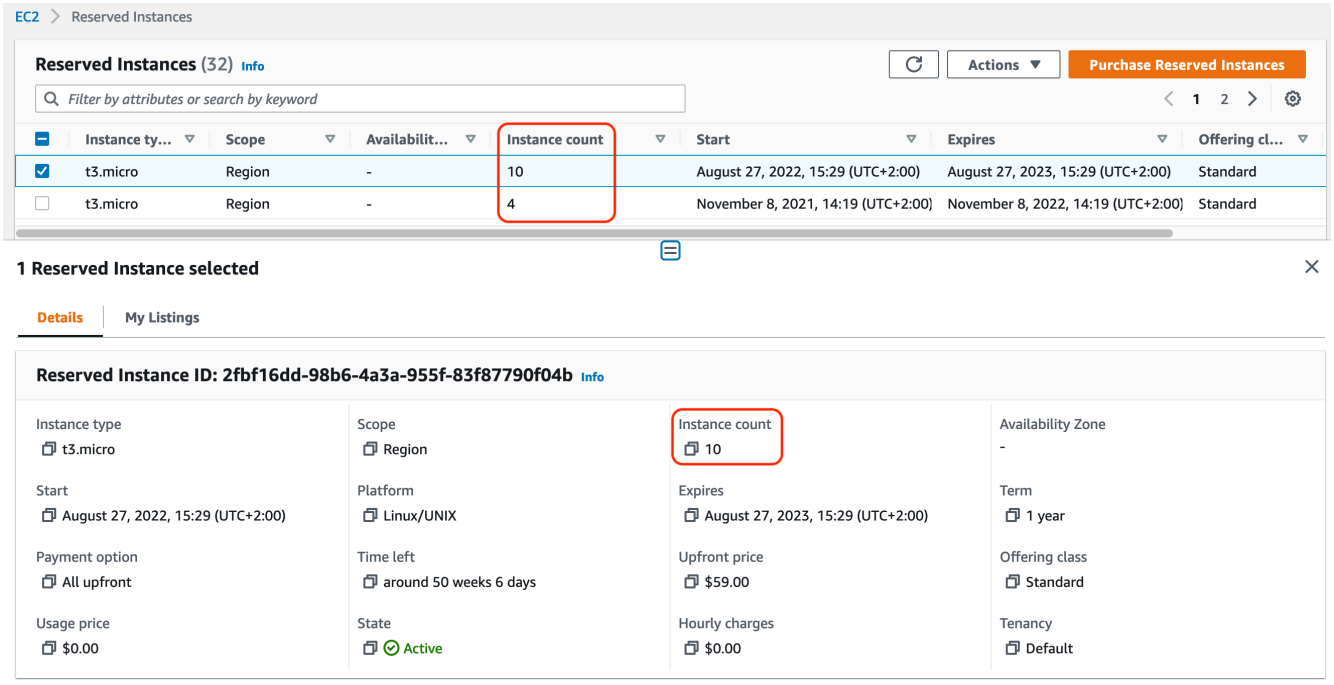
Sie können anzeigen, wie viele Reserved Instances Sie erworben haben, indem Sie Amazon EC2 oder die AWS CLI verwenden.

Console

So zeigen Sie die Gesamtzahl der erworbenen Reserved Instances an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances aus.
3. Wählen Sie eine Reserved-Instance-Konfiguration aus der Tabelle aus und markieren Sie das Feld Instance count (Instance-Anzahl).

   Im folgenden Screenshot stellt die ausgewählte Zeile eine einzelne Reserved-Instance-Konfiguration für einen `t3.micro`-Instance-Typ dar. Die Spalte Instance count (Instance-Anzahl) in der Tabellenansicht und das Feld Instance count (Instance-Anzahl) in der Detailansicht (im Screenshot dargestellt) zeigen an, dass es 10 Reserved Instances für diese Konfiguration gibt.



AWS CLI

So zeigen Sie die Gesamtzahl der erworbenen Reserved Instances an

Verwenden Sie den Befehl describe-reserved-instances und geben Sie die ID der Reserved-Instance-Konfiguration an.

```
aws ec2 describe-reserved-instances \
    --reserved-instances-ids a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
    --output table
```

Es folgt eine Beispielausgabe. Das Feld `InstanceCount` zeigt an, dass es 10 Reserved Instances für diese Konfiguration gibt.

```
-------------------------------------------------------------------
|                    DescribeReservedInstances                    |
+-----------------------------------------------------------------+
||                       ReservedInstances                       ||
|+----------------------+----------------------------------------+|
||  CurrencyCode        |  USD                                   ||
||  Duration            |  31536000                              ||
||  End                 |  2023-08-27T13:29:44+00:00             ||
||  FixedPrice          |  59.0                                  ||
||  InstanceCount       |  10                                    ||
||  InstanceTenancy     |  default                               ||
||  InstanceType        |  t3.micro                              ||
||  OfferingClass       |  standard                              ||
||  OfferingType        |  All Upfront                           ||
||  ProductDescription  |  Linux/UNIX                            ||
||  ReservedInstancesId |  a1b2c3d4-5678-90ab-cdef-EXAMPLE11111  ||
||  Scope               |  Region                                ||
||  Start               |  2022-08-27T13:29:45.938000+00:00      ||
||  State               |  active                                ||
||  UsagePrice          |  0.0                                   ||
|+----------------------+----------------------------------------+|
|||                     RecurringCharges                        |||
||+---------------------------------+--------------------------+||
|||  Amount                         |  0.0                     |||
|||  Frequency                      |  Hourly                  |||
||+---------------------------------+--------------------------+||
```

PowerShell

So zeigen Sie die Gesamtzahl der erworbenen Reserved Instances an

Verwenden Sie das Cmdlet Get-EC2ReservedInstance und geben Sie die ID der Reserved-Instance-Konfiguration an.

```
Get-EC2ReservedInstance -ReservedInstancesId a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Es folgt eine Beispielausgabe. Das Feld `InstanceCount` zeigt an, dass es 10 Reserved Instances für diese Konfiguration gibt.

```
AvailabilityZone    :
CurrencyCode        : USD
Duration            : 31536000
End                 : 1/12/2017 8:57:08 PM
FixedPrice          : 0
InstanceCount       : 10
InstanceTenancy     : default
InstanceType        : t3.medium
OfferingClass       : standard
OfferingType        : All Upfront
ProductDescription  : Windows
RecurringCharges    : {}
ReservedInstancesId : a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
Scope               : Region
Start               : 10/12/2016 4:00:00 PM
State               : active
Tags                : {}
UsagePrice          : 0
```

Überlegungen

Eine regionale Reserved Instance gewährt einen Rabatt auf eine laufende On-Demand-Instance. Das Standard-On-Demand-Instance-Limit ist 20. Sie können Ihr laufendes On-Demand-Instance-Limit nicht überschreiten, indem Sie die regionale Reserved Instances kaufen. Wenn Sie beispielsweise bereits 20 laufende On-Demand-Instances haben und 20 regionale Reserved Instances kaufen, werden die 20 regionalen Reserved Instances verwendet, um einen Rabatt auf die 20 laufenden On-Demand-Instances anzuwenden. Wenn Sie mehr regionale Reserved Instances kaufen, können Sie nicht mehr Instances starten, weil Sie Ihr On-Demand-Instance-Limit erreicht haben.

Bevor Sie Reserved Instances regional kaufen, stellen Sie sicher, dass Ihr On-Demand-Instance-Limit der Anzahl der regionalen Reserved Instances entspricht oder diese überschreitet, die Sie nutzen möchten. Stellen Sie bei Bedarf sicher, dass Sie eine Erhöhung Ihres On-Demand-Instance-Limits beantragen, bevor Sie mehr regionale Reserved Instances kaufen.

Eine zonengebundene Reserved Instance – eine Reserved Instance, die für eine bestimmte Availability Zone gekauft wird – bietet sowohl eine Kapazitätsreservierung als auch einen Rabatt. Sie können Ihr laufendes On-Demand-Instance-Limit um überschreiten, indem Sie Zone Reserved Instances kaufen. Wenn Sie zum Beispiel bereits 20 laufende On-Demand-Instances haben und 20 Zonen Reserved Instances kaufen, können Sie weitere 20 On-Demand-Instances starten, die den Spezifikationen Ihrer Zonen Reserved Instances entsprechen, was Ihnen insgesamt 40 laufende Instances gibt.

Anzeigen Ihrer Reserved-Instance-Kontingente und Anfordern einer Kontingenterhöhung

Die Amazon-EC2-Konsole stellt Informationen zum Kontingent bereit. Sie können auch eine Kontingenterhöhung anfordern. Weitere Informationen finden Sie unter Anzeigen Ihrer aktuellen Kontingente und Beantragen einer Erhöhung.

Spot Instances

Eine Spot-Instance ist eine Instance, die freie EC2 Kapazität nutzt, die für weniger als den On-Demand-Preis verfügbar ist. Da Sie mit Spot-Instances ungenutzte EC2 Instances mit hohen Rabatten anfordern können, können Sie Ihre EC2 Amazon-Kosten erheblich senken. Der Stundenpreis für eine Spot-Instance wird als Spot-Preis bezeichnet. Der Spot-Preis für jeden Instance-Typ in jeder Availability Zone wird von Amazon EC2 festgelegt und schrittweise auf der Grundlage des langfristigen Angebots an und der Nachfrage nach Spot-Instances angepasst. Ihre Spot Instance läuft, wann immer Kapazität verfügbar ist.

Spot Instances sind eine kostengünstige Wahl, sofern Sie bei der Ausführung Ihrer Anwendungen zeitlich flexibel sind und Unterbrechungen verschmerzen können. Spot Instances sind z. B. für Datenanalysen, Batch-Verarbeitungsaufträge, die Hintergrundverarbeitung und optionale Aufgaben geeignet. Weitere Informationen finden Sie unter Amazon EC2 Spot-Instances.

Einen Vergleich der verschiedenen Kaufoptionen für EC2 Instances finden Sie unter EC2 Abrechnungs- und Kaufoptionen von Amazon.

Konzepte

Bevor Sie mit Spot Instances arbeiten, sollten Sie mit den folgenden Konzepten vertraut sein:

- Spot-Kapazitätspool — Eine Gruppe ungenutzter EC2 Instances mit demselben Instance-Typ (z. B. `m5.large`) und derselben Availability Zone.
- Spot-Preis: Der aktuelle Preis einer Spot-Instance pro Stunde.
- Spot-Instance-Anforderung: Fordert eine Spot-Instance an. Wenn Kapazität verfügbar ist, EC2 erfüllt Amazon Ihre Anfrage. Eine Spot-Instance-Anforderung erfolgt entweder einmalig oder persistent. Amazon übermittelt EC2 automatisch erneut eine persistente Spot-Instance-Anfrage, nachdem die mit der Anfrage verknüpfte Spot-Instance unterbrochen wurde.
- EC2 Empfehlung zur Instance-Neuverteilung — Amazon EC2 sendet ein Empfehlungssignal zur Instance-Neuverteilung aus, um Sie darüber zu informieren, dass für eine Spot-Instance ein erhöhtes Ausfallrisiko besteht. Dieses Signal bietet Ihnen die Möglichkeit, Ihre Workloads proaktiv auf bestehende oder neue Spot Instances zu verteilen, ohne auf die zweiminütige Ankündigung einer Spot-Instance-Unterbrechung warten zu müssen.
- Spot-Instance-Unterbrechung — Amazon EC2 beendet, stoppt oder versetzt Ihre Spot-Instance in den Ruhezustand, wenn Amazon die Kapazität wieder EC2 benötigt. Amazon EC2 stellt eine Benachrichtigung zur Unterbrechung der Spot-Instance bereit, sodass die Instance zwei Minuten lang gewarnt wird, bevor sie unterbrochen wird.

Unterschiede zwischen Spot Instances und On-Demand-Instances

In der folgenden Tabelle sind die wichtigsten Unterschiede zwischen Spot Instances und On-Demand-Instances aufgeführt.

	Spot Instances	On-Demand Instances
Startzeit	Kann nur dann sofort gestartet werden, wenn die Spot-Instance-Anforderung aktiv ist und Kapazität vorhanden ist.	Kann nur dann sofort gestartet werden, wenn Sie eine manuelle Startanfo rderung stellen und Kapazität zur Verfügung steht.
Verfügbare Kapazität	Wenn keine Kapazität verfügbar ist, löst die Spot-Instance-Anforderung automatisch die Startanforderung aus, bis die Kapazität verfügbar ist.	Wenn bei einer Startanforderung keine Kapazität verfügbar ist, erhalten Sie einen Fehler wegen unzureichender Kapazität (ICE).

	Spot Instances	On-Demand Instances
Stundenpreis	Der stündliche Preis für Spot Instances variiert je nach langfristigem Angebot und Nachfrage.	Der Stundenpreis für On-Demand-Instances ist statisch.
Neuausgleichsempfehlung	Das Signal, das Amazon für eine laufende Spot-Instance EC2 ausgibt, wenn für die Instance ein erhöhtes Risiko einer Unterbrechung besteht.	Sie bestimmen, wann ein On-Demand-Instance unterbrochen (gestoppt, in den Ruhezustand versetzt oder beendet) wird.
Instance-Unterbrechung	Sie können eine Amazon EBS-gestützte Spot-Instance beenden und starten. Darüber hinaus EC2 kann Amazon eine einzelne Spot-Instance unterbrechen, wenn keine Kapazität mehr verfügbar ist.	Sie bestimmen, wann ein On-Demand-Instance unterbrochen (gestoppt, in den Ruhezustand versetzt oder beendet) wird.

Preise und Einsparungen

Sie zahlen den Spot-Preis für Spot-Instances, der von Amazon festgelegt EC2 und auf der Grundlage des langfristigen Angebots an und der Nachfrage nach Spot-Instances schrittweise angepasst wird. Ihre Spot-Instances laufen, bis Sie sie beenden, keine Kapazität mehr verfügbar ist oder Ihre Amazon EC2 Amazon EC2 Auto Scaling Scaling-Gruppe sie während des Scale-In beendet.

Wenn Sie oder Amazon eine laufende Spot-Instance EC2 unterbrechen, werden Ihnen die genutzten Sekunden oder die volle Stunde in Rechnung gestellt, oder Sie erhalten keine Gebühren, je nachdem, welches Betriebssystem verwendet wurde und wer die Spot-Instance unterbrochen hat. Weitere Informationen finden Sie unter Fakturierung für unterbrochene Spot-Instances.

Spot Instances sind nicht durch Savings Plans abgedeckt. Wenn Sie einen Savings Plan haben, bietet dieser keine zusätzlichen Einsparungen zu den Einsparungen, die Sie bereits durch die Nutzung von Spot Instances erhalten. Darüber hinaus gelten für Ihre Ausgaben für Spot Instances nicht für die Verpflichtungen in Ihren Compute Savings Plans.

Anzeigen von Preisen

Den aktuellen (alle fünf Minuten aktualisierten) niedrigsten Spot-Preis pro AWS-Region Instance-Typ finden Sie auf der Preisseite für Amazon EC2 Spot-Instances.

Verwenden Sie die EC2 Amazon-Konsole oder den describe-spot-price-historyBefehl, um den Spot-Preisverlauf der letzten drei Monate anzuzeigen. Weitere Informationen finden Sie unter Spot-Instance-Preisverlauf anzeigen.

Wir ordnen die Availability Zones unabhängig voneinander den jeweiligen Codes zu AWS-Konto. Aus diesem Grund können Sie für denselben Availability-Zone-Code (beispielsweise `us-west-2a`) für verschiedene Konten verschiedene Ergebnisse erhalten.

Anzeigen der Einsparungen

Sie können die Einsparungen anzeigen, die durch die Verwendung von Spot-Instances für eine einzelne Spot-Flotte oder für alle Spot Instances erzielt wurden. Sie können die Einsparungen der letzten Stunde oder der letzten drei Tag)e sowie die durchschnittlichen Kosten pro vCPU-Stunde und pro Speicher(GiB)-Stunde einsehen. Die Einsparungen werden geschätzt und können von den tatsächlichen Einsparungen abweichen, da sie die Abrechnungsanpassungen für Ihre Nutzung nicht enthalten. Weitere Informationen zur Anzeige von Einsparungsinformationen finden Sie unter Einsparungen durch den Spot-Instances-Einkauf.

Anzeigen der Abrechnung

Ihre Rechnung enthält Einzelheiten zu Ihrer Servicenutzung. Weitere Informationen finden Sie unter Anzeigen Ihrer Rechnung im AWS Billing -Benutzerhandbuch.

Bewährte Methoden für Amazon EC2 Spot

Amazon EC2 bietet AWS Cloud über Spot-Instances Zugriff auf freie EC2 Rechenkapazität mit Einsparungen von bis zu 90% im Vergleich zu On-Demand-Preisen. Der einzige Unterschied zwischen On-Demand-Instances und Spot-Instances besteht darin EC2, dass Spot-Instances von Amazon mit einer Frist von zwei Minuten unterbrochen werden können, wenn Amazon die Kapazität zurückfordern EC2 muss. Um die beste Erfahrung mit Spot Instances zu gewährleisten, ist es wichtig, die bewährten Methoden für deren Verwendung zu verstehen und anzuwenden.

Spot Instances werden für zustandslose, fehlertolerante, flexible Anwendungen empfohlen. Spot Instances eignen sich beispielsweise gut für Big Data, containerisierte Workloads, CI/CD, zustandslose Webserver, High Performance Computing (HPC) und Rendering-Workloads.

Während des Ausführens sind Spot Instances genau gleich wie On-Demand-Instances. Spot garantiert jedoch nicht, dass Sie Ihre ausgeführten Instances lange genug halten können, um Ihre Workloads abzuschließen. Spot garantiert auch nicht, dass Sie die sofortige Verfügbarkeit der von Ihnen gesuchten Instances erhalten können oder dass Sie immer die von Ihnen angeforderte Gesamtkapazität erhalten können. Darüber hinaus können sich Spot-Instance-Unterbrechungen und Spot-Instance-Kapazitäten im Laufe der Zeit ändern, da die Spot-Instance-Verfügbarkeit je nach Angebot und Nachfrage variiert und die Performance in der Vergangenheit keine Garantie für zukünftige Ergebnisse darstellt.

Spot Instances sind nicht für Workloads geeignet, die unflexibel, statusbehaftet, fehlerintolerant oder eng zwischen Instance-Knoten verbunden sind. Wir empfehlen Spot Instances nicht für Workloads, die nicht tolerieren, dass gelegentlich die gesamte Zielkapazität nicht vollständig verfügbar ist. Die Einhaltung der bewährten Methoden von Spot, um flexibel in Bezug auf Instance-Typen und Availability Zones zu sein, bietet zwar die beste Chance auf Hochverfügbarkeit, es gibt jedoch keine Garantie dafür, dass Kapazität verfügbar ist, da eine steigende Nachfrage nach On-Demand-Instances die Workloads auf Spot Instances stören kann.

Wir warnen dringend davor, Spot Instances für diese Workloads zu verwenden oder ein Failover auf On-Demand-Instances zu versuchen, um Unterbrechungen zu handhaben. Ein Failover auf On-Demand-Instances kann versehentlich zu Unterbrechungen Ihrer anderen Spot Instances führen. Wenn Spot Instances für eine Kombination aus Instance-Typ und Availability Zone unterbrochen werden, kann es für Sie außerdem schwierig werden, On-Demand-Instances mit derselben Kombination zu erhalten.

Unabhängig davon, ob Sie ein erfahrener Spot-Benutzer oder neu bei Spot Instances sind: Wenn Sie derzeit Probleme mit Spot-Instance-Unterbrechungen oder Spot-Instance-Verfügbarkeit haben, empfehlen wir Ihnen, diese bewährten Methoden zu befolgen, um die beste Erfahrung mit dem Spot-Service zu erzielen.

Bewährte Methoden für Spot

- Vorbereiten einzelner Instances auf Unterbrechungen
- Flexibel sein bei Instance-Typen und Availability Zones
- Attributbasierte Auswahl des Instance-Typs verwenden
- Verwenden Sie Spot-Platzierungswerte, um optimale Regionen und Availability Zones zu identifizieren
- Verwenden Sie EC2 Amazon EC2 Auto Scaling Scaling-Gruppen oder EC2 Fleet, um Ihre Gesamtkapazität zu verwalten

- Nutzen der preis- und kapazitätsoptimierten Zuweisungsstrategie
- Verwenden Sie integrierte AWS Dienste, um Ihre Spot-Instances zu verwalten
- Was ist die beste Spot-Request-Methode?

Vorbereiten einzelner Instances auf Unterbrechungen

Der beste Weg, um Spot-Instance-Unterbrechungen ordnungsgemäß zu handhaben, besteht darin, Ihre Anwendung so zu konzipieren, dass sie eine Fehlertoleranz aufweist. Um dies zu erreichen, können Sie Empfehlungen zur Neuverteilung von EC2 Instances und Hinweise zur Unterbrechung von Spot-Instances nutzen.

Eine Empfehlung zur Neuverteilung einer EC2 Instance ist ein Signal, das Sie darüber informiert, wenn bei einer Spot-Instance ein erhöhtes Ausfallrisiko besteht. Das Signal gibt Ihnen die Möglichkeit, die Spot-Instance vor der zweiminütigen Spot-Instance-Unterbrechungsbenachrichtigung proaktiv zu verwalten. Sie können entscheiden, Ihr Workload auf neue oder bestehende Spot Instances auszugleichen, die nicht einem erhöhten Risiko einer Unterbrechung ausgesetzt sind. Wir haben es Ihnen leicht gemacht, dieses Signal zu verwenden, indem wir die Funktion Capacity Rebalancing in Auto Scaling Scaling-Gruppen und EC2 Fleet verwenden.

Eine Benachrichtigung zur Unterbrechung einer Spot-Instance ist eine Warnung, die zwei Minuten vor der EC2 Unterbrechung einer Spot-Instance durch Amazon ausgegeben wird. Wenn Ihre Workload „zeitlich flexibel“ ist, können Sie Ihre Spot Instances so konfigurieren, dass sie bei einer Unterbrechung angehalten oder in den Ruhezustand versetzt werden, anstatt beendet zu werden. Amazon stoppt Ihre Spot-Instances bei einer Unterbrechung EC2 automatisch oder versetzt sie in den Ruhezustand und nimmt die Instances automatisch wieder auf, wenn wir über verfügbare Kapazitäten verfügen.

Wir empfehlen Ihnen, in Amazon eine Regel zu erstellen EventBridge, die die Empfehlungen zur Neuverteilung und die Unterbrechungsbenachrichtigungen erfasst und dann einen Checkpoint für den Fortschritt Ihrer Arbeitslast auslöst oder die Unterbrechung ordnungsgemäß behandelt. Weitere Informationen finden Sie unter Überwachen von Signalen für Neuausgleichsempfehlungen. Ein ausführliches Beispiel, das Sie Schritt für Schritt durch die Erstellung und Verwendung von Ereignisregeln führt, finden Sie unter Die Vorteile von Amazon EC2 Spot-Instance Interruption Notices nutzen.

Weitere Informationen erhalten Sie unter EC2 Empfehlungen zur Neugewichtung von Instanzen und Spot-Instance-Unterbrechungen.

Flexibel sein bei Instance-Typen und Availability Zones

Ein Spot-Kapazitätspool besteht aus einer Reihe ungenutzter EC2 Instances mit demselben Instance-Typ (zum Beispiel`m5.large`) und derselben Availability Zone (zum Beispiel us-east-1a). Sie sollten flexibel darin sein, welche Instance-Typen Sie anfordern und in welchen Availability Zones Sie Ihren Workload bereitstellen können. Dies gibt Spot eine bessere Chance, die erforderliche Menge an Rechenkapazität zu finden und zuzuweisen. Fragen Sie zum Beispiel nicht nur nach `c5.large`, wenn Sie bereit wären, Larges aus den Familien c4, m5 und m4 zu verwenden.

Je nach Ihren spezifischen Anforderungen können Sie auswerten, über welche Instance-Typen hinweg Sie flexibel sein können, um Ihre Computing-Anforderungen zu erfüllen. Wenn ein Workload vertikal skaliert werden kann, sollten Sie größere Instance-Typen (mehr V CPUs und Arbeitsspeicher) in Ihre Anfragen aufnehmen. Wenn Sie nur horizontal skalieren können, sollten Sie Instance-Typen älterer Generation einbeziehen, da sie von On-Demand-Kunden weniger gefragt sind.

Eine gute Faustregel besteht darin, für jeden Workload über mindestens 10 Instance-Typen hinweg flexibel zu sein. Stellen Sie außerdem sicher, dass alle Availability Zones für die Verwendung in Ihrer VPC konfiguriert und für Ihren Workload ausgewählt sind.

Attributbasierte Auswahl des Instance-Typs verwenden

Bei der attributbasierten Auswahl des Instance-Typs können Sie Instanzattribute wie v, memory und storage für den Workload angebenCPUs, den Sie ausführen möchten. EC2 Amazon EC2 Auto Scaling oder EC2 Fleet identifiziert und startet dann automatisch Instances, die Ihren angegebenen Attributen entsprechen. Dadurch entfällt der Aufwand für die manuelle Auswahl bestimmter Instance-Typen, was ein tiefes Verständnis des Angebots der einzelnen Instance-Typen voraussetzt.

Darüber hinaus ermöglicht Ihnen die attributbasierte Auswahl des Instance-Typs, neu veröffentlichte Instance-Typen automatisch zu verwenden, sobald sie verfügbar sind. Dies gewährleistet einen nahtlosen Zugriff auf ein immer breiteres Spektrum an Spot-Instance-Kapazität.

Die attributbasierte Auswahl von Instance-Typen ist ideal für Workloads und Frameworks, die hinsichtlich der Instance-Typen flexibel sein können, wie High Performance Computing (HPC) und Big-Data-Workloads.

Weitere Informationen finden Sie unter Erstellen einer gemischten Instance-Gruppe mithilfe der attributbasierten Instance-Typauswahl im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch und Geben Sie Attribute für die Auswahl von Instance-Typen für EC2-Flotte oder Spot-Flotte an in diesem Handbuch.

Verwenden Sie Spot-Platzierungswerte, um optimale Regionen und Availability Zones zu identifizieren

Spot-Instances sind ungenutzte EC2 Kapazität, und diese Kapazität schwankt je nach Angebot und Nachfrage. EC2 Daher erhalten Sie möglicherweise nicht immer genau die Spot-Kapazität, die Sie an einem bestimmten Standort zu einem bestimmten Zeitpunkt benötigen. Um diese Unvorhersehbarkeit zu mindern, können Sie das Feature der Spot-Platzierungsbewertung verwenden. Dieses Feature bietet Empfehlungen für Regionen oder Availability Zones, in denen die Wahrscheinlichkeit höher ist, dass sie über ausreichend Kapazität verfügen, um Ihren Spot-Kapazitätsbedarf zu decken, ohne dass Sie zuerst Spot Instances an diesen Standorten starten müssen.

Die Spot-Platzierungsbewertung eignet sich am besten für Workloads, die hinsichtlich der Instance-Typen und der Region oder Availability Zone, die sie verwenden können, flexibel sein können. Sie müssen lediglich die Spot-Kapazität angeben, die Sie benötigen, Ihre Anforderungen an den Instance-Typ und ob Sie Empfehlungen für Regionen oder Availability Zones wünschen. Im Gegenzug erhalten Sie für jede Region oder Availability Zone eine Punktzahl zwischen 1 und 10, die die Wahrscheinlichkeit angibt, dass Ihre angeforderte Spot-Kapazität an diesem Standort erfolgreich bereitgestellt wird. Ein Ergebnis von 10 zeigt an, dass Ihre Spot-Anforderung sehr wahrscheinlich erfolgreich sein wird.

Es ist wichtig zu beachten, dass es sich bei der Bewertung von Spot-Platzierungen um eine point-in-time Empfehlung handelt, da die Kapazität im Laufe der Zeit variieren kann. Sie garantiert nicht die verfügbare Kapazität und sagt auch nicht das Risiko einer Unterbrechung voraus.

Sie können die Spot Placement Score-Funktion in der EC2 Amazon-Konsole oder in einem SDK verwenden. AWS CLI Weitere Informationen finden Sie unter Spot-Platzierungsbewertung.

Verwenden Sie EC2 Amazon EC2 Auto Scaling Scaling-Gruppen oder EC2 Fleet, um Ihre Gesamtkapazität zu verwalten

Mit Spot können Sie in Bezug auf die Gesamtkapazität denken — in Einheiten, die VCPUs, Arbeitsspeicher, Speicher oder Netzwerkdurchsatz beinhalten —, anstatt in Bezug auf einzelne Instances zu denken. Amazon EC2 Auto Scaling Scaling-Gruppen und EC2 Fleet ermöglichen es Ihnen, eine Zielkapazität zu starten und aufrechtzuerhalten und automatisch Ressourcen anzufordern, um alle zu ersetzen, die unterbrochen oder manuell beendet wurden. Wenn Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe oder eine EC2 Flotte konfigurieren, müssen Sie nur die Instance-Typen und die Zielkapazität auf der Grundlage Ihrer Anwendungsanforderungen angeben. Weitere Informationen finden Sie unter Amazon EC2 Auto Scaling Scaling-Gruppen im

Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch und Erstellen Sie eine EC2 Flotte in diesem Benutzerhandbuch.

Nutzen der preis- und kapazitätsoptimierten Zuweisungsstrategie

Zuweisungsstrategien in Amazon EC2 Auto Scaling Scaling-Gruppen helfen Ihnen dabei, Ihre Zielkapazität bereitzustellen, ohne manuell nach Spot-Kapazitätspools mit freier Kapazität suchen zu müssen. Es wird empfohlen, die `price-capacity-optimized`-Strategie zu verwenden, da diese Strategie automatisch Instances aus den am häufigsten verfügbaren Spot-Kapazitätspools bereitstellt, die außerdem den niedrigstmöglichen Preis bieten. Sie können auch die `price-capacity-optimized` Zuweisungsstrategie in EC2 Fleet nutzen. Da Ihre Spot-Instance-Kapazität aus Pools mit optimaler Kapazität bezogen wird, verringert dies die Möglichkeit, dass Ihre Spot Instances zurückgewonnen werden. Weitere Informationen finden Sie unter Zuweisungsstrategien für mehrere Instance-Typen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch und Wenn Workloads mit hohen Unterbrechungskosten verbunden sind in diesem Benutzerhandbuch.

Verwenden Sie integrierte AWS Dienste, um Ihre Spot-Instances zu verwalten

Andere AWS Dienste lassen sich in Spot integrieren, um die gesamten Rechenkosten zu senken, ohne dass die einzelnen Instances oder Flotten verwaltet werden müssen. Wir empfehlen Ihnen, die folgenden Lösungen für Ihre jeweiligen Workloads in Betracht zu ziehen: Amazon EMR, Amazon Elastic Container Service AWS Batch, Amazon Elastic Kubernetes Service, Amazon SageMaker AI und Amazon Servers AWS Elastic Beanstalk. GameLift Weitere Informationen zu den Best Practices von Spot mit diesen Services finden Sie auf der Amazon EC2 Spot Instances Workshop-Website.

Was ist die beste Spot-Request-Methode?

Bestimmen Sie anhand der folgenden Tabelle, welche API für die Anforderung von Spot Instances verwendet werden soll.

API	Wann sollte dies verwendet werden?	Anwendungsfall	Soll ich diese API verwenden?
CreateAutoScalingGroup	• Sie benötigen mehrere Instances mit einer einzigen Konfiguration oder	Erstellen Sie eine Auto-Scaling-Gruppe, die den Lebenszyklus Ihrer Instances verwaltet	Ja

API	Wann sollte dies verwendet werden?	Anwendungsfall	Soll ich diese API verwenden?
	einer gemischten Konfiguration. • Sie möchten das Lebenszyklusmanagement mit einer konfigurierbaren API automatisieren.	und gleichzeitig die gewünschte Anzahl von Instances beibehält. Unterstützt die horizontale Skalierung (Hinzufügen weiterer Instances) zwischen festgelegten Mindest- und Maximalgrenzen.	

API	Wann sollte dies verwendet werden?	Anwendungsfall	Soll ich diese API verwenden?
CreateFleet	• Sie benötigen mehrere Instances mit einer einzigen Konfiguration oder einer gemischten Konfiguration. • Sie möchten Ihren Instance-Lebenszyklus selbst verwalten. • Wenn Sie kein Auto Scaling benötigen, empfehlen wir eine Flotte des Typs `instant`.	Erstellen Sie eine Flotte von On-Demand-Instances und Spot Instances in einer einzigen Anforderung mit mehreren Startspezifikationen, die sich in Bezug auf Instance-Typ, AMIdie Availability Zone oder Subnetz unterscheiden. Die Spot-Instance-Zuweisungsstrategie ist standardmäßig auf `lowest-price` pro Einheit eingestellt, aber Sie können die Einstellung auf `price-capacity-optimized` , `capacity-optimized` oder `diversified` ändern.	Ja – im `instant`-Modus, wenn Sie das Auto Scaling nicht benötigen

API	Wann sollte dies verwendet werden?	Anwendungsfall	Soll ich diese API verwenden?
RunInstances	• Sie verwenden die RunInstances API bereits, um On-Demand-Instances zu starten, und möchten einfach zum Starten von Spot-Instances wechseln, indem Sie einen einzigen Parameter ändern. • Sie benötigen nicht mehrere Instances mit verschiedenen Instance-Typen.	Starten Sie eine bestimmte Anzahl von Instances mit einem AMI- und einem Instance-Typ.	Nein — weil gemischte Instance-Typen in einer einzigen Anfrage RunInstances nicht zulässig sind

API	Wann sollte dies verwendet werden?	Anwendungsfall	Soll ich diese API verwenden?
RequestSpotFleet	• Wir raten dringend davon ab, die RequestSpotFleet API zu verwenden, da es sich um eine veraltete API handelt, für die keine geplanten Investitionen erforderlich sind. • Wenn Sie den Lebenszyklus Ihrer Instance verwalten möchten, verwenden Sie die CreateFleet API. • Wenn Sie Ihren Instanzlebenszyklus nicht verwalten möchten, verwenden Sie die CreateAutoScalingGroup API.	NICHT VERWENDEN. RequestSpotFleet ist eine veraltete API ohne geplante Investitionen.	Nein

API	Wann sollte dies verwendet werden?	Anwendungsfall	Soll ich diese API verwenden?
RequestSpotInstances	• Wir raten dringend davon ab, die RequestSpotInstances API zu verwenden, da es sich um eine veraltete API ohne geplante Investitionen handelt.	NICHT VERWENDEN. RequestSpotInstances ist eine veraltete API ohne geplante Investitionen.	Nein

Funktionsweise von Spot Instances

Um eine Spot-Instance zu starten, erstellen Sie entweder eine Spot-Instance-Anfrage, oder Amazon EC2 erstellt in Ihrem Namen eine Spot-Instance-Anfrage. Die Spot-Instance wird gestartet, wenn die Spot-Instance-Anforderung erfüllt ist.

Sie können eine Spot-Instance mit mehreren verschiedenen Services starten. Weitere Informationen finden Sie unter Erste Schritte mit Amazon EC2 Spot-Instances. In diesem Benutzerhandbuch beschreiben wir die folgenden Möglichkeiten, eine Spot-Instance zu starten mit EC2:

- Sie können eine Spot-Instance-Anfrage erstellen, indem Sie den Launch-Instance-Assistenten in der EC2 Amazon-Konsole oder den Befehl run-instances verwenden. Weitere Informationen finden Sie unter Ihre Spot Instances verwalten.
- Sie können eine EC2 Flotte erstellen, in der Sie die gewünschte Anzahl von Spot-Instances angeben. Amazon EC2 erstellt in Ihrem Namen eine Spot-Instance-Anfrage für jede Spot-Instance, die in der EC2 Flotte angegeben ist. Weitere Informationen finden Sie unter Erstellen Sie eine EC2 Flotte.
- Sie können eine Spot-Flotten-Anforderung erstellen, in der Sie die gewünschte Anzahl von Spot Instances angeben. Amazon EC2 erstellt in Ihrem Namen eine Spot-Instance-Anfrage für jede Spot-Instance, die in der Spot-Flotte-Anfrage angegeben ist. Weitere Informationen finden Sie unter Erstellen einer Spot-Flotte.

Ihre Spot Instance wird gestartet, wenn Kapazität verfügbar ist. Ihre Spot-Instance läuft, bis Sie sie stoppen oder beenden oder bis Amazon sie EC2 unterbricht (bekannt als Spot-Instance-Unterbrechung). Amazon EC2 kann eine Spot-Instance stoppen, beenden oder in den Ruhezustand versetzen, wenn sie unterbrochen wird.

Wenn Sie Spot Instances verwenden, müssen Sie auf Unterbrechungen vorbereitet sein. Amazon EC2 kann Ihre Spot-Instance unterbrechen, wenn die Nachfrage nach Spot-Instances steigt oder wenn das Angebot an Spot-Instances sinkt. Wenn Amazon eine Spot-Instance EC2 unterbricht, wird eine Benachrichtigung zur Unterbrechung der Spot-Instance angezeigt, sodass die Instance zwei Minuten lang gewarnt wird, bevor Amazon sie EC2 unterbricht. Sie können für Spot Instances keinen Beendigungsschutz aktivieren. Weitere Informationen finden Sie unter Spot-Instance-Unterbrechungen.

Inhalt

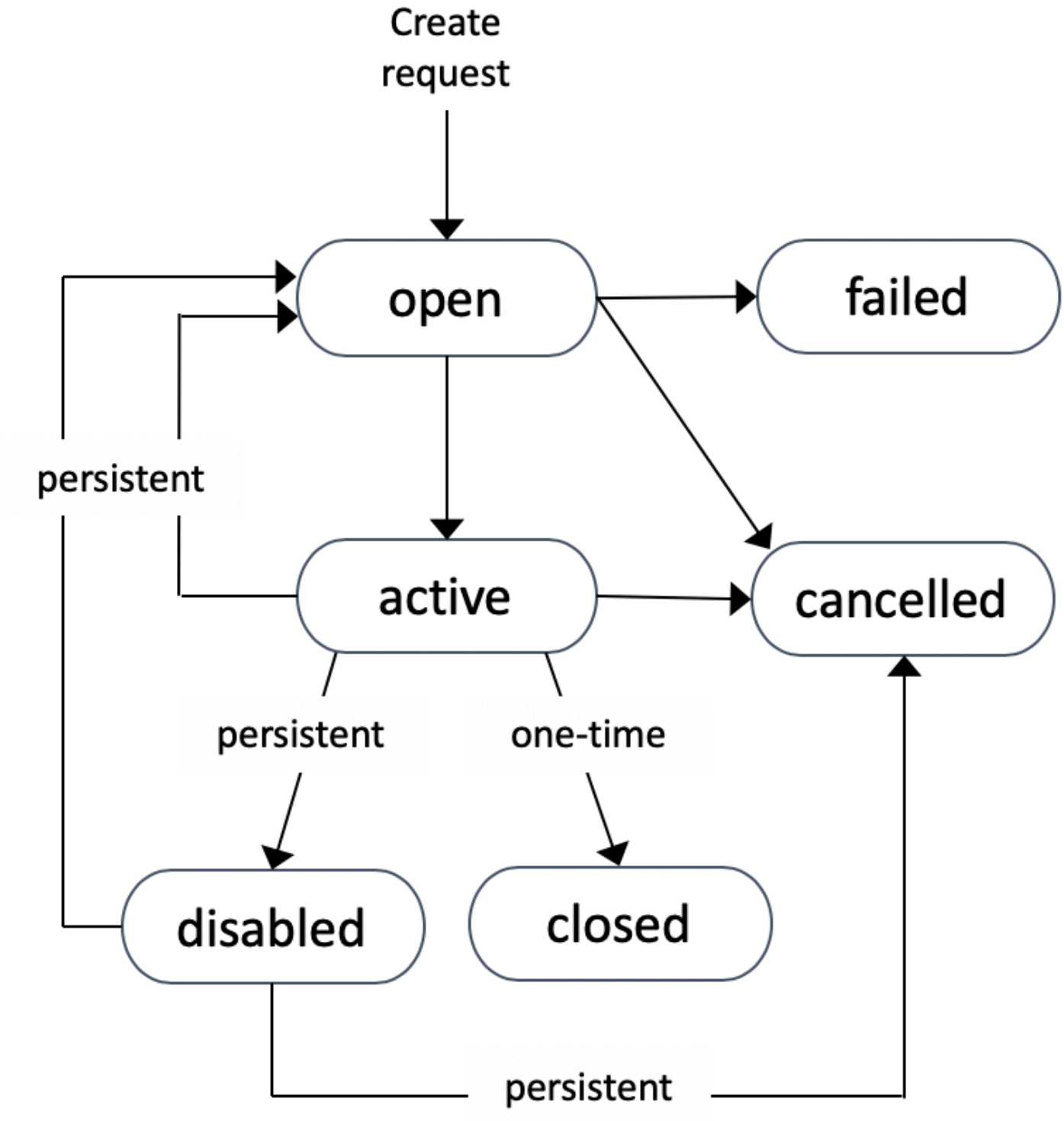
- Zustand von Spot-Instance-Anforderungen
- Starten Sie Spot Instances in einer Startgruppe
- Starten von Spot Instances in einer Availability-Zone-Gruppe
- Starten von Spot Instances in einer VPC
- Instances mit Spitzenlastleistung starten
- Auf Einzel-Tenant-Hardware starten

Zustand von Spot-Instance-Anforderungen

Eine Spot-Instance-Anforderung kann die folgenden Zustände aufweisen:

- `open`: Die Anforderung wartet darauf, erfüllt zu werden.
- `active`: Die Anforderung wurde erfüllt und ist mit einer Spot-Instance verknüpft.
- `failed`: Die Anforderung weist einen oder mehrere fehlerhafte Parameter auf.
- `closed`: Die Spot-Instance wurde unterbrochen oder beendet.
- `disabled`: Sie haben die Spot-Instance gestoppt.
- `cancelled`: Sie haben die Anforderung storniert oder die Anforderung ist abgelaufen.

Die folgende Abbildung stellt die Übergänge zwischen den Anforderungszuständen dar. Beachten Sie, dass die Übergänge vom Anforderungstyp (einmalig oder persistent) abhängen.



Eine einmalige Spot-Instance-Anfrage bleibt aktiv, bis Amazon die Spot-Instance EC2 startet, die Anfrage abläuft oder Sie die Anfrage stornieren. Wenn keine Kapazität verfügbar ist, wird Ihre Spot Instance beendet und die Spot-Instance-Anforderung geschlossen.

Eine persistente Spot-Instance-Anforderung bleibt so lange aktiv, bis sie abläuft oder abgebrochen wird, selbst wenn die Anforderung erfüllt wird. Wenn keine Kapazität verfügbar ist, wird Ihre Spot Instance unterbrochen. Nach einer Unterbrechung Ihrer Instance wird die Spot Instance gestartet, wenn sie angehalten wurde oder wieder aufgenommen, wenn sie sich im Ruhezustand befindet. Sie können eine Spot Instance anhalten und erneut starten, wenn die Kapazität verfügbar ist. Wenn die Spot-Instance beendet wird (unabhängig davon, ob die Spot-Instance gestoppt oder ausgeführt wird), wird die Spot-Instance-Anfrage erneut geöffnet und Amazon EC2 startet eine neue Spot-Instance. Weitere Informationen finden Sie unter Anhalten einer Spot-Instance, Starten einer Spot-Instance und Beenden einer Spot-Instance.

Sie können den Status Ihrer Spot-Instance-Anforderungen sowie den Status der gestarteten Spot Instances über den Status nachverfolgen. Weitere Informationen finden Sie unter Den Status einer Spot-Instance-Anfrage abrufen.

Starten Sie Spot Instances in einer Startgruppe

Geben Sie in Ihrer Spot-Instance-Anfrage eine Startgruppe an, um Amazon EC2 anzuweisen, nur dann eine Reihe von Spot-Instances zu starten, wenn es alle starten kann. Wenn der Spot-Service eine der Instances einer Startgruppe beenden muss, muss er sie alle beenden. Wenn Sie jedoch eine oder mehrere Instances in einer Startgruppe beenden, beendet Amazon die verbleibenden Instances in der Startgruppe EC2 nicht.

Auch wenn diese Option nützlich sein kann, kann sich durch das Hinzufügen dieser Bedingung die Chance verringern, dass Ihre Spot-Instance-Anforderung erfüllt wird, und die Chance erhöhen, dass Ihre Spot Instances beendet werden. Ihre Startgruppe umfasst beispielsweise Instances in mehreren Availability Zones. Wenn die Kapazität in einer dieser Availability Zones abnimmt und nicht mehr verfügbar ist, EC2 beendet Amazon alle Instances für die Startgruppe.

Wenn Sie eine weitere erfolgreiche Spot-Instance-Anforderung erstellen, die dieselbe (vorhandene) Startgruppe wie eine zuvor erfolgreiche Anforderung festlegt, werden die neuen Instances zu der Startgruppe hinzugefügt. Wenn eine Instance in dieser Startgruppe beendet wird, werden folglich alle Instances in der Startgruppe beendet; dies umfasst alle Instances, die durch die erste und zweite Anforderung gestartet wurden.

Starten von Spot Instances in einer Availability-Zone-Gruppe

Geben Sie in Ihrer Spot-Instance-Anfrage eine Availability Zone-Gruppe an, EC2 um Amazon anzuweisen, eine Reihe von Spot-Instances in derselben Availability Zone zu starten. Amazon EC2 muss nicht alle Instances in einer Availability Zone-Gruppe gleichzeitig unterbrechen. Wenn Amazon

eine der Instances in einer Availability Zone-Gruppe unterbrechen EC2 muss, laufen die anderen weiter.

Auch wenn diese Option sehr nützlich sein kann, können durch das Hinzufügen dieser Bedingung die Chancen sinken, dass Ihre Spot-Instance-Anforderung erfüllt wird.

Wenn Sie eine Gruppe von Availability Zones angeben, in der Spot-Instance-Anforderung jedoch keine Availability Zone angeben, hängt das Ergebnis vom angegebenen Netzwerk ab.

Standard-VPC

Amazon EC2 verwendet die Availability Zone für das angegebene Subnetz. Wenn Sie kein Subnetz angeben, wählt es eine Availability Zone und sein Standard-Subnetz aus – dies ist jedoch nicht unbedingt die günstigste Zone. Wenn Sie das Standard-Subnetz für eine Availability Zone gelöscht haben, müssen Sie ein anderes Subnetz angeben.

Nicht standardmäßige VPC

Amazon EC2 verwendet die Availability Zone für das angegebene Subnetz.

Starten von Spot Instances in einer VPC

Sie geben ein Subnetz für Ihre Spot Instances genau so an, wie Sie ein Subnetz für Ihre On-Demand-Instances angeben.

- [Standard-VPC] Wenn Ihre Spot-Instance in einer bestimmten kostengünstigen Availability Zone gestartet werden soll, müssen Sie das entsprechende Subnetz in Ihrer Spot-Instance-Anforderung angeben. Wenn Sie kein Subnetz angeben, EC2 wählt Amazon eines für Sie aus, und die Availability Zone für dieses Subnetz hat möglicherweise nicht den niedrigsten Spot-Preis.
- [Nicht standardmäßige VPC] Sie müssen das Subnetz für Ihre Spot-Instance angeben.

Instances mit Spitzenlastleistung starten

Bei den T-Instance-Typen handelt es sich um Instances mit Spitzenleistung. Wenn Sie Ihre Spot Instances mit einem Burstable-Performance-Instance-Typ starten, und wenn Sie planen, Ihre Spot Instances mit Spitzenlastleistung sofort und für eine kurze Dauer zu verwenden, ohne Leerlaufzeit für die Anrechnung von CPU-Guthaben, empfiehlt sich, diese im Standardmodus zu starten, um höhere Kosten zu vermeiden. Wenn Sie die Spot Instances mit Spitzenlastleistung im Unlimited mode (Unbegrenzten Modus) starten und die Spitzenlastleistung der CPU sofort nutzen, geben Sie

überschüssiges Guthaben für Spitzen aus. Wenn Sie die Instance für eine kurze Zeit nutzen, hat die Instance keine Zeit, CPU-Guthaben zu sammeln, um das überschüssige Guthaben zu bezahlen. Das überschüssige Guthaben wir beim Beenden der Instance abgerechnet.

Der unbegrenzte Modus für Spot Instances mit Spitzenlastleistung ist nur dann geeignet, wenn die Instance lange genug läuft, um CPU-Guthaben für Spitzen zu erhalten. Andernfalls macht das Bezahlen für überzähliges Guthaben die Spot Instances mit Spitzenlastleistung teurer als die Verwendung anderer Instances. Weitere Informationen finden Sie unter Verwendung des unbegrenzten Modus im Vergleich zu einer festen CPU.

T2-Instances erhalten bei Konfiguration im Standardmodus Startguthaben. T2-Instances sind die einzigen Instances mit Spitzenleistung, die Startguthaben erhalten. Startguthaben sollen eine produktive erste Starterfahrung für T2-Instances bieten, indem sie ausreichende Rechenressourcen zur Verfügung gestellt werden, um die Instance zu konfigurieren. Wiederholte Starts von T2-Instances, um neue Startguthaben zu erhalten, sind nicht zulässig. Wenn Sie dauerhaft eine CPU benötigen, können Sie Guthaben verdienen (durch Leerlauf über einen gewissen Zeitraum), Unbegrenzten Modus für T2 Spot Instances verwenden oder einen Instance-Typ mit dedizierter CPU verwenden.

Auf Einzel-Tenant-Hardware starten

Spot-Instances können auf Single-Tenant-Hardware ausgeführt werden. Dedizierte Spot-Instances sind physisch von Instances isoliert, die zu anderen AWS Konten gehören. Weitere Informationen finden Sie unter Amazon-EC2-Dedicated-Instances Amazon EC2 Dedicated Instances.

Führen Sie einen der folgenden Schritte aus, um eine Dedicated-Spot-Instance auszuführen:

- Geben Sie beim Erstellen der Spot-Instance-Anforderung eine `dedicated`-Tenancy an. Weitere Informationen finden Sie unter Ihre Spot Instances verwalten.
- Fordern Sie eine Spot-Instance in einer VPC mit einer `dedicated`-Instance-Tenancy an. Weitere Informationen finden Sie unter Dedicated Instances in eine VPC mit Standard-Tenancy starten. Sie können keine Spot Instance mit der Tenancy `default` anfordern, wenn Sie diese in einer VPC mit Instance-Tenancy von `dedicated` anfordern.

Alle Instance-Familien unterstützen Dedicated Spot Instances außer T-Instances. Für jede unterstützte Instance-Familie unterstützt nur die größte Instance-Größe oder Metallgröße Dedicated Spot Instances.

Spot-Instance-Preisverlauf anzeigen

Die Spot-Instance-Preise werden von Amazon festgelegt EC2 und je nach langfristigen Trends bei Angebot und Nachfrage nach Spot-Instance-Kapazität schrittweise angepasst.

Wenn Ihre Spot-Anforderung erfüllt ist, starten Ihre Spot Instances zum aktuellen Spot-Preis, der den On-Demand-Preis nicht übersteigt. Sie können den Spot-Preisverlauf für die letzten 90 Tage gefiltert nach Instance-Typ, Betriebssystem und Availability Zone anzeigen.

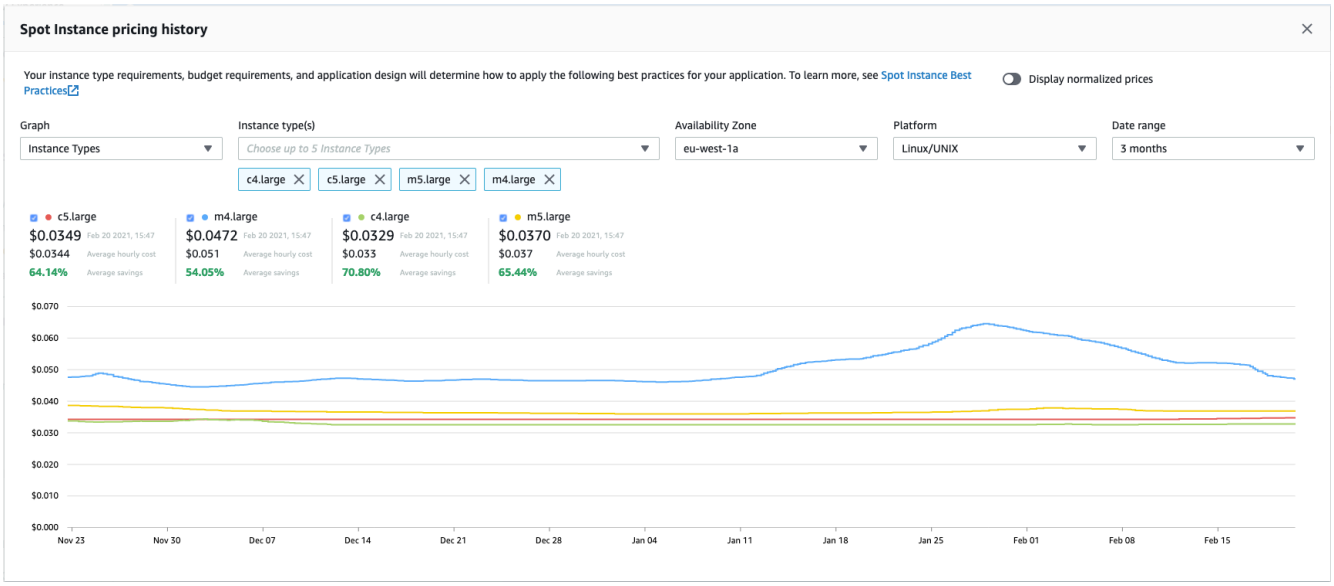
Die aktuellen Spot-Instance-Preise finden Sie unter Amazon EC2 Spot-Instance-Preise.

Console

So zeigen Sie den Spot-Preisverlauf an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Pricing History (Preisverlauf) aus.
4. Vergleichen Sie für Graph (Diagramm) den Preisverlauf nach Availability Zones oder nach Instance-Typen.
   - Wenn Sie Availability Zones auswählen, wählen Sie Instance-Typ, Betriebssystem (Plattform) und Datumsbereich, für die Sie den Preisverlauf anzeigen möchten.
   - Wenn Sie Instance-Typen auswählen, wählen Sie bis zu fünf Instance-Typen, Availability Zone, Betriebssystem (Plattform) und Datumsbereich, für die Sie den Preisverlauf anzeigen möchten.

   Der folgende Screenshot zeigt einen Preisvergleich für verschiedene Instance-Typen.



5. Bewegen Sie den Mauszeiger über das Diagramm, um die Preise zu bestimmten Zeiten im ausgewählten Datumsbereich anzuzeigen. Die Preise werden in den Informationsblöcken über dem Diagramm angezeigt. Der in der obersten Reihe angezeigte Preis zeigt den Preis an einem bestimmten Datum an. Der in der zweiten Zeile angezeigte Preis zeigt den Durchschnittspreis für den ausgewählten Datumsbereich.
6. Um den Preis pro vCPU anzuzeigen, schalten Sie Normalisierte Preise anzeigen ein. Um den Preis für den Instance-Typ anzuzeigen, deaktivieren Sie Normalisierte Preise anzeigen.

AWS CLI

So zeigen Sie den Spot-Preisverlauf an

Verwenden Sie den folgenden describe-spot-price-history-Befehl.

```
aws ec2 describe-spot-price-history \
    --instance-types c6i.xlarge \
    --product-descriptions "Linux/UNIX" \
    --start-time 2025-04-01T00:00:00 \
    --end-time 2025-04-02T00:00:0
```

PowerShell

So zeigen Sie den Spot-Preisverlauf an

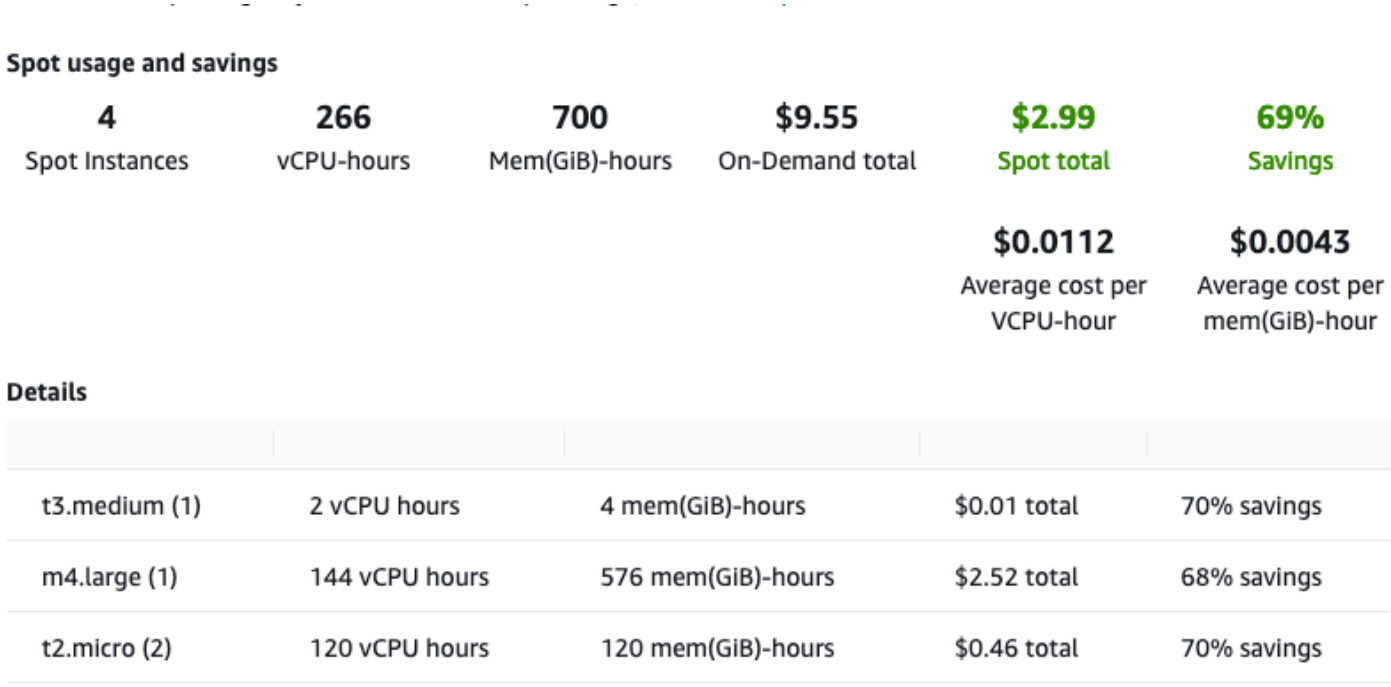
Verwenden Sie das cmdlet Get-EC2SpotPriceHistory.

```
Get-EC2SpotPriceHistory `
    -InstanceType c6i.xlarge `
    -ProductDescription "Linux/UNIX" `
    -UtcStartTime 2025-04-01T00:00:00 `
    -UtcEndTime 2025-04-02T00:00:0
```

Einsparungen durch den Spot-Instances-Einkauf

Sie können die Nutzungs- und Einsparinformationen für Spot Instances auf Flottenebene oder für alle laufenden Spot Instances anzeigen. Auf der Ebene der einzelnen Flotten umfassen die Nutzungs- und Einsparungsinformationen alle Instances, die von der Flotte gestartet und beendet werden. Sie können diese Informationen aus der letzten Stunde oder den letzten drei Tagen anzeigen.

Der folgende Screenshot aus dem Abschnitt Einsparungen zeigt die Spot-Nutzungs- und Einsparungsinformationen für eine Spot-Flotte.



Sie können die folgenden Nutzungs- und Einsparungsinformationen anzeigen:

- Spot Instances: Die Anzahl der Spot Instances, die von der Spot-Flotte gestartet und beendet wurden. Wenn Sie die Einsparungsübersicht anzeigen, stellt die Zahl alle Ihre laufenden Spot Instances dar.

- vCPU-hours (vCPU-Stunden) – Die Anzahl der vCPU-Stunden, die über alle Spot Instances für den ausgewählten Zeitraum hinweg verbraucht werden.
- Mem(GiB)-hours (Mem(GiB)-Stunden) – Die Anzahl der GiB-Stunden, die über alle Spot Instances für den ausgewählten Zeitraum hinweg verbraucht werden.
- On-Demand total (On-Demand gesamt) – Der Gesamtbetrag, den Sie für den ausgewählten Zeitraum bezahlt hätten, wenn Sie diese Instances mit On-Demand-Instances gestartet hätten.
- Spot total (Spot gesamt) – Der zu zahlende Gesamtbetrag für den gewählten Zeitraum.
- Savings (Einsparungen) – Der Prozentsatz, den Sie sparen, indem Sie den On-Demand-Preis nicht zahlen.
- Durchschnittliche Kosten pro vCPU-Stunde — Die durchschnittlichen stündlichen Kosten für die Nutzung von v CPUs für alle Spot-Instances im ausgewählten Zeitraum, berechnet wie folgt: Durchschnittliche Kosten pro vCPU-Stunde = Spot-Gesamt/vCPU-Stunden.
- Durchschnittliche Kosten pro Mem-Stunde (GiB) — Die durchschnittlichen stündlichen Kosten für die GiBs Nutzung aller Spot-Instances für den ausgewählten Zeitraum, berechnet wie folgt: Durchschnittliche Kosten pro Mem-Stunde (GiB) = Spot-Gesamtwert/Mem (GiB) -Stunden.
- Details-Tabelle: Die verschiedenen Instance-Typen (die Anzahl der Instances pro Instance-Typ steht in Klammern), die die Spot-Flotte bilden. Wenn Sie die Einsparungsübersicht anzeigen, umfassen diese Ihre gesamten laufenden Spot Instances.

Sparinformationen können nur über die EC2 Amazon-Konsole eingesehen werden.

So zeigen Sie Informationen zu den Einsparungen für eine Spot-Flotte an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie die ID einer Spot-Flotten-Anfrage aus und scrollen Sie zum Abschnitt Einsparungen.

   Aktivieren Sie alternativ das Kontrollkästchen neben der Spot-Flotten-Anforderungs-ID und wählen Sie die Registerkarte Einsparungen.
4. Standardmäßig werden auf der Seite Nutzungs- und Einsparungsinformationen für die letzten drei Tage angezeigt. Sie können last hour (letzte Stunde) oder last three days (letzten drei Tage) auswählen. Für Spot-Flotten, die vor weniger als einer Stunde gestartet wurden, zeigt die Seite die geschätzten Einsparungen für diese Stunde an.

So zeigen Sie Informationen zu den Einsparungen für alle laufenden Spot Instances an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Savings Summary (Einsparungsübersicht) aus.

Erstellt eine Spot-Instance-Anforderung

Um Spot Instances zu verwenden, erstellen Sie eine Spot-Instance-Anforderung, die die gewünschte Anzahl von Instances, den Instance-Typ und die Availability Zone enthält. Wenn Kapazität verfügbar ist, EC2 erfüllt Amazon Ihre Anfrage sofort. Andernfalls EC2 wartet Amazon, bis Ihre Anfrage erfüllt werden kann oder bis Sie die Anfrage stornieren.

Sie können den Launch-Instance-Assistenten in der EC2 Amazon-Konsole oder den Befehl run-instances verwenden, um eine Spot-Instance genauso anzufordern, wie Sie eine On-Demand-Instance starten können. Diese Methode wird nur aus folgenden Gründen empfohlen:

- Sie verwenden bereits den Launch Instance Wizard oder den run-instances-Befehl, um On-Demand-Instances zu launchen, und Sie möchten einfach zum Launchen von Spot Instances wechseln, indem Sie einen einzelnen Parameter ändern.
- Sie benötigen nicht mehrere Instances mit verschiedenen Instance-Typen.

Diese Methode wird im Allgemeinen nicht zum Launchen von Spot Instances empfohlen, da Sie nicht mehrere Instance-Typen angeben können und Spot Instances und On-Demand-Instances nicht in derselben Anforderung launchen können. Für die bevorzugten Methoden zum Starten von Spot Instances, darunter das Starten einer Flotte einschließlich Spot Instances und On-Demand-Instances mit mehreren Instance-Typen finden Sie unter Was ist die beste Spot-Request-Methode?

Wenn Sie mehrere Spot-Instances gleichzeitig anfordern, EC2 erstellt Amazon separate Spot-Instance-Anfragen, sodass Sie den Status jeder Anfrage separat verfolgen können. Weitere Informationen zum Nachverfolgen von Spot-Instance-Anforderungen finden Sie unter Den Status einer Spot-Instance-Anfrage abrufen.

Console

So erstellen Sie eine Spot-Instance-Anforderung

Die Schritte 1 bis 9 sind die gleichen Schritte, die Sie zum Launchen einer On-Demand-Instance verwenden würden. In Schritt 10 konfigurieren Sie die Spot-Instance-Anforderung.

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Navigationsleiste oben auf dem Bildschirm eine Region aus.
3. Wählen Sie im Dashboard der EC2 Amazon-Konsole die Option Launch instance aus.
4. (Optional) Unter Name and Tags (Name und Tags) können Sie Ihre Instance benennen und die Spot-Instance-Anforderung, die Instance, die Volumes und die elastischen Grafiken markieren. Informationen zu Tags siehe Kennzeichnen Sie Ihre EC2 Amazon-Ressourcen.

   a. Geben Sie unter Name einen beschreibenden Namen für Ihre Instance ein.

      Der Instance-Name ist ein Tag, wobei der Schlüssel Name ist und es sich bei dem Wert um den von Ihnen angegebenen Namen handelt. Wenn Sie keinen Namen angeben, kann die Instance anhand der ID identifiziert werden, die beim Starten der Instance automatisch generiert wird.

   b. Um die Spot-Instance-Anforderung, die Instance, die Volumes und die elastischen Grafiken zu markieren, wählen Sie Add additional tags (Zusätzliche Tags hinzufügen) aus. Klicken Sie auf Tag hinzufügen, geben Sie dann einen Schlüssel und einen Wert ein und wählen Sie den Ressourcentyp aus, den Sie markieren möchten. Wählen Sie für jedes weitere Tag Add another Tag (Weiteres Tag hinzufügen) aus.
5. Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) das Betriebssystem (OS) für Ihre Instance aus und wählen Sie dann eine AMI aus. Weitere Informationen finden Sie unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image).
6. Wählen Sie unter Instance type (Instance-Typ) den Instance-Typ aus, der Ihren Anforderungen für die Hardware-Konfiguration und Größe Ihrer Instance entspricht. Weitere Informationen finden Sie unter Instance-Typ.
7. Wählen Sie unter Key pair (login) (Schlüsselpaar (Login) ein vorhandenes Schlüsselpaar aus oder wählen Sie Create new key pair (Neues Schlüsselpaar erstellen), um ein neues zu erstellen. Weitere Informationen finden Sie unter EC2 Amazon-Schlüsselpaare und EC2 Amazon-Instances.

> **Important**
>
> Wenn Sie die Option Proceed without key pair (Not recommended) (Ohne Schlüsselpaar fortfahren (Nicht empfohlen)) auswählen, können Sie keine Verbindung zur Instance herstellen, es sei denn, Sie wählen ein AMI aus, das entsprechend konfiguriert ist, um Benutzern eine andere Anmeldemöglichkeit zu erlauben.

8. Verwenden Sie unter Network settings (Netzwerkeinstellungen) die Standardeinstellungen oder wählen Sie Edit (Bearbeiten), um die Netzwerkeinstellungen nach Bedarf zu konfigurieren.

   Sicherheitsgruppen sind Teil der Netzwerkeinstellungen und definieren Firewall-Regeln für Ihre Instance. Diese Regeln legen fest, welcher eingehende Netzwerkverkehr an Ihre Instance übertragen wird.

   Weitere Informationen finden Sie unter Netzwerkeinstellungen.

9. Die von Ihnen ausgewählte AMI beinhaltet ein oder mehrere Speicher-Volumes, einschließlich eines Root-Gerät-Volumes. Unter Configure Storage (Speicher konfigurieren) können Sie zusätzliche Volumes angeben, die der Instance angefügt werden, indem Sie Add New Volume (Neues Volume hinzufügen) auswählen. Weitere Informationen finden Sie unter Speicher konfigurieren.

10. Unter Advanced details (Erweiterte Details) konfigurieren Sie die Spot-Instance-Anforderung wie folgt:

    a. Wählen Sie Unter Kaufoption das Kontrollkästchen Spot Instances anfordern.

    b. Sie können entweder die Standardkonfiguration für die Spot-Instance-Anforderung beibehalten oder Customize (Anpassen) rechts auswählen, um benutzerdefinierte Einstellungen für Ihre Spot-Instance-Anfrage festzulegen.

       Wenn Sie Customize (Anpassen) wählen, werden die folgenden Felder angezeigt.

       i. Maximum price (Maximaler Preis): Sie können Spot Instances zum Spot-Preis anfordern, der auf den On-Demand-Preis begrenzt ist oder den Höchstbetrag angeben, den Sie zu zahlen bereit sind.

> **Warning**
>
> Wenn Sie einen Höchstpreis angeben, werden Ihre Instances häufiger unterbrochen, als wenn Sie No maximum price (Kein Höchstpreis) auswählen.
> Wenn Sie einen Höchstpreis angeben, muss dieser mehr als 0,001 USD betragen. Wenn Sie einen Wert unter 0,001 USD angeben, schlägt der Start fehl.

- No maximum price (Kein maximaler Preis): Ihre Spot Instance wird zum aktuellen Spot-Preis gestartet. Der Preis wird niemals den On-Demand-Preis überschreiten. (Empfohlen)
- Set your maximum price (per instance/hour) (Festlegen Ihres Höchstpreises (pro Instance/Stunde)): Sie können den Höchstbetrag angeben, den Sie zahlen möchten.
  - Wenn Sie einen Höchstpreis angeben, der unter dem aktuellen Spot-Preis liegt, wird Ihre Spot Instance nicht gestartet.
  - Wenn Sie einen Höchstpreis angeben, der über dem aktuellen Spot-Preis liegt, wird Ihre Spot Instance zum aktuellen Spot-Preis gelauncht und berechnet. Wenn Ihre Spot-Instance läuft und der Spot-Preis über Ihren Höchstpreis steigt, EC2 unterbricht Amazon Ihre Spot-Instance.
  - Unabhängig vom Höchstpreis, den Sie angeben, wird Ihnen immer der aktuelle Spot-Preis in Rechnung gestellt.

  Informationen zu den Entwicklungen der Spot-Preise finden Sie unter Spot-Instance-Preisverlauf anzeigen.

ii. Request type (Typ der Anforderung): Der von Ihnen gewählte Spot-Instance-Anforderungstyp bestimmt, was passiert, wenn Ihre Spot Instance unterbrochen wird.

- Einmalig: Amazon EC2 stellt eine einmalige Anfrage für Ihre Spot-Instance. Wenn Ihre Spot Instance unterbrochen wird, wird die Anforderung nicht erneut gesendet.

- Dauerhafte Anfrage: Amazon EC2 stellt eine persistente Anfrage für Ihre Spot-Instance. Wenn Ihre Spot Instance unterbrochen wird, wird sie erneut übermittelt, um die unterbrochene Spot Instance aufzufüllen.

Wenn Sie keinen Wert angeben, handelt es sich standardmäßig um eine einmalige Anforderung.

iii. Valid to (Gültig bis): Das Ablaufdatum einer persistenten Spot-Instance-Anforderung.

Dieses Feld wird für einmalige Anforderungen nicht unterstützt. Eine one-time-Anfrage bleibt so lange aktiv, bis alle Instances startet, die Anfrage abläuft oder Sie die Anfrage abbrechen.

- No request expiry date (Kein Ablaufdatum der Anforderung): Die Anforderung bleibt so lange aktiv, bis Sie sie abbrechen.
- Set your request expiry date (Festlegen eines Ablaufdatums für die Anforderung): Die dauerhafte Anforderung bleibt bis zu dem von Ihnen angegebenen Datum oder bis zum Abbruch aktiv.

iv. Interruption behavior (Verhalten bei Unterbrechungen): Das von Ihnen gewählte Verhalten bestimmt, was passiert, wenn eine Spot Instance unterbrochen wird.

- Gültige Werte für persistente Anforderungen sind Stop (Anhalten) und Hibernate (Ruhezustand). Wenn eine Instance angehalten wird, fallen Gebühren für EBS-Volume-Speicher an.

> **Note**
>
> Spot Instances nutzen jetzt die gleiche Ruhezustandsfunktion wie On-Demand-Instances. Um den Ruhezustand zu aktivieren, können Sie entweder hier Ruhezustand auswählen oder Aktivieren aus dem Feld Stopp – Ruhezustand auswählen, das weiter unten im Launch Instance Wizard angezeigt wird. Informationen zu den Voraussetzungen für den Ruhezustand finden Sie unter EC2 Voraussetzungen für den Ruhezustand der Instance.

- Für einmalige Anforderungen ist nur Terminate (Beenden) gültig.

Wenn Sie keinen Wert angeben, ist der Standard Terminate (Beenden), was für eine dauerhafte Spot-Instance-Anforderung nicht gültig ist. Wenn Sie den Standardwert beibehalten und versuchen, eine dauerhafte Spot-Instance-Anfrage zu starten, wird eine Fehlermeldung angezeigt.

Weitere Informationen finden Sie unter Verhalten von Spot-Instance-Unterbrechungen.

11. Geben Sie im Bereich Summary (Zusammenfassung) für Number of Instances (Anzahl der Instances) die Anzahl der Instances ein, die gelauncht werden sollen.

> **Note**
>
> Amazon EC2 erstellt für jede Spot-Instance eine separate Anfrage.

12. Überprüfen Sie im Übersichts-Bereich die Details Ihrer Instance und nehmen Sie ggf. Änderungen vor. Nachdem Sie Ihre Spot-Instance-Anforderung übermittelt haben, können Sie die Parameter der Anforderung nicht mehr ändern. Sie können direkt zu einem Abschnitt im Launch Instance Wizard navigieren, indem Sie den entsprechenden Link im Übersichts-Bereich auswählen. Weitere Informationen finden Sie unter Zusammenfassung.
13. Wenn Sie bereit sind, Ihre Instance zu starten, wählen Sie Instance starten aus.

    Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Fehlerbehebung bei Amazon-EC2-Instances.

AWS CLI

So erstellen Sie eine Spot-Instance-Anforderung mit run-instances

Verwenden Sie den Befehl run-instances und geben Sie die Spot-Instance-Optionen im Parameter `--instance-market-options` an.

```
--instance-market-options file://spot-options.json
```

Nachfolgend finden Sie die Datenstruktur, die in der JSON-Datei anzugeben ist. Sie können auch `ValidUntil` und `InstanceInterruptionBehavior` angeben. Wenn Sie kein Feld in der Datenstruktur angeben, wird der Standardwert verwendet.

Das folgende Beispiel erstellt eine `persistent`-Anforderung.

```
{
  "MarketType": "spot",
  "SpotOptions": {
    "SpotInstanceType": "persistent"
  }
}
```

Um eine Spot-Instance-Anfrage zu erstellen, verwenden Sie request-spot-instances

> **Note**
>
> Wir raten dringend davon ab, den request-spot-instancesBefehl zum Anfordern einer Spot-Instance zu verwenden, da es sich um eine veraltete API handelt, für die keine geplanten Investitionen erforderlich sind. Weitere Informationen finden Sie unter Was ist die beste Spot-Request-Methode?.

Verwenden Sie den request-spot-instancesBefehl, um eine einmalige Anfrage zu erstellen.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json
```

Verwenden Sie den request-spot-instancesBefehl, um eine persistente Anfrage zu erstellen.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "persistent" \
    --launch-specification file://specification.json
```

Beispiel-Startkonfigurationsdateien, die mit diesen Befehlen verwendet werden können, finden Sie unter Beispiel-Startspezifikationen für Spot-Instance-Anforderung. Wenn Sie eine Startspezifikationsdatei von der Spot-Requests-Konsole herunterladen, müssen Sie stattdessen den request-spot-fleetBefehl verwenden (die Spot-Requests-Konsole spezifiziert eine Spot-Instance-Anfrage mithilfe einer Spot-Flotte).

PowerShell

So erstellen Sie eine Spot-Instance-Anforderung

Verwenden Sie das New-EC2InstanceCmdlet und geben Sie die Spot-Instance-Optionen mithilfe des `-InstanceMarketOption` Parameters an.

```
-InstanceMarketOptions $marketOptions
```

Erstellen Sie die Datenstruktur für die Spot-Instance-Optionen wie folgt.

```
$spotOptions = New-Object Amazon.EC2.Model.SpotMarketOptions
$spotOptions.SpotInstanceType="persistent"
$marketOptions = New-Object Amazon.EC2.Model.InstanceMarketOptionsRequest
$marketOptions.MarketType = "spot"
$marketOptions.SpotOptions = $spotOptions
```

Beispiel-Startspezifikationen für Spot-Instance-Anforderung

Die folgenden Beispiele zeigen Startkonfigurationen, die Sie mit dem request-spot-instancesBefehl verwenden können, um eine Spot-Instance-Anfrage zu erstellen. Weitere Informationen finden Sie unter Ihre Spot Instances verwalten.

> **Important**
>
> Wir raten dringend davon ab, den request-spot-instancesBefehl zum Anfordern einer Spot-Instance zu verwenden, da es sich um eine veraltete API handelt, für die keine geplanten Investitionen erforderlich sind. Weitere Informationen finden Sie unter Was ist die beste Spot-Request-Methode?.

Beispiele

- Beispiel 1: Spot Instances starten
- Beispiel 2: Starten von Spot Instances in der angegebenen Availability Zone
- Beispiel 3: Starten von Spot Instances im angegebenen Subnetz
- Beispiel 4: Starten einer Dedicated-Spot-Instance

Beispiel 1: Spot Instances starten

Das folgende Beispiel enthält keine Availability Zone oder ein Subnetz. Amazon EC2 wählt eine Availability Zone für Sie aus. Amazon EC2 startet die Instances im Standardsubnetz der ausgewählten Availability Zone.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Beispiel 2: Starten von Spot Instances in der angegebenen Availability Zone

Das folgende Beispiel enthält eine Availability Zone. Amazon EC2 startet die Instances im Standardsubnetz der angegebenen Availability Zone.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "Placement": {
    "AvailabilityZone": "us-west-2a"
  },
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Beispiel 3: Starten von Spot Instances im angegebenen Subnetz

Das folgende Beispiel enthält ein Subnetz. Amazon EC2 startet die Instances im angegebenen Subnetz. Wenn es sich bei der VPC nicht um eine Standard-VPC handelt, erhält die Instance standardmäßig keine öffentliche IPv4 Adresse.

```
{
```

```
  "ImageId": "ami-0abcdef1234567890",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "SubnetId": "subnet-1a2b3c4d",
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Um einer Instance in einer nicht standardmäßigen VPC eine öffentliche IPv4 Adresse zuzuweisen, geben Sie das `AssociatePublicIpAddress` Feld wie im folgenden Beispiel gezeigt an. Wenn Sie eine Netzwerkschnittstelle angeben, müssen Sie die Subnetz-ID und die Sicherheitsgruppen-ID über die Netzwerkschnittstelle angeben, anstatt die Felder `SubnetId` und `SecurityGroupIds` aus dem vorherigen Codeblock zu verwenden.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "InstanceType": "m5.medium",
  "NetworkInterfaces": [
    {
      "DeviceIndex": 0,
      "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
      "Groups": [ "sg-1a2b3c4d5e6f7g8h9" ],
      "AssociatePublicIpAddress": true
    }
  ],
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Beispiel 4: Starten einer Dedicated-Spot-Instance

Im folgenden Beispiel wird eine Spot-Instance mit der Tenancy `dedicated` angefordert. Eine Dedicated-Spot-Instance muss in einer VPC gestartet werden.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "c5.8xlarge",
```

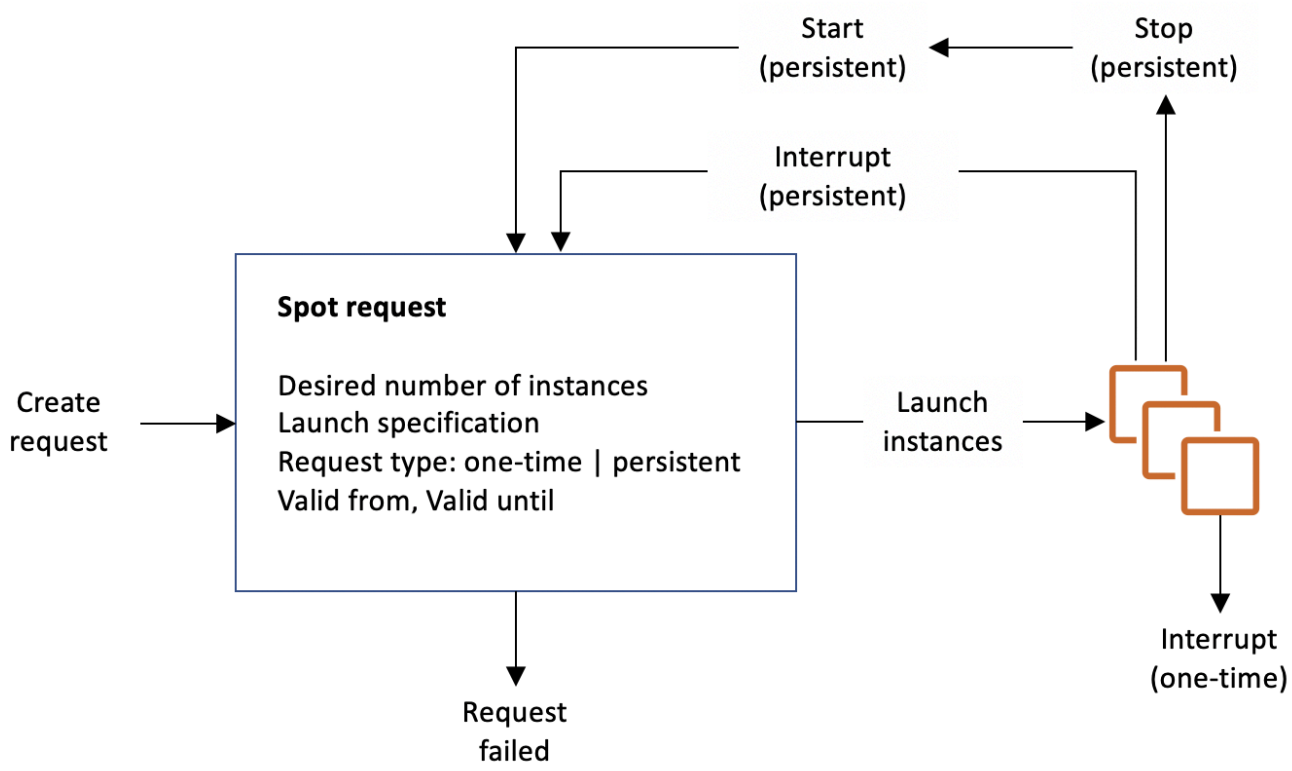
```
  "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
  "Placement": {
    "Tenancy": "dedicated"
  }
}
```

Den Status einer Spot-Instance-Anfrage abrufen

Verwenden Sie den von Amazon bereitgestellten Anforderungsstatus, damit Sie Ihre Spot-Instance-Anfragen verfolgen und Ihre Nutzung von Spot-Instances planen können EC2. Durch den Anforderungsstatus erfahren Sie beispielsweise den Grund dafür, warum Ihre Spot-Anforderung noch nicht erfüllt wurde oder der Anforderungsstatus listet die Bedingungen auf, die verhindern, dass Ihre Spot-Anforderung erfüllt wird.

In jedem Schritt des Prozesses, der auch als Lebenszyklus der Spot-Anforderung bezeichnet wird, legen spezifische Ereignisse sukzessive Anforderungsstatus fest.

In der folgenden Abbildung ist die Arbeitsweise von Spot-Instance-Anforderungen dargestellt. Beachten Sie, dass der Anforderungstyp (einmalig oder dauerhaft) bestimmt, ob die Anfrage erneut geöffnet wird, wenn Amazon eine Spot-Instance EC2 unterbricht oder wenn Sie eine Spot-Instance beenden. Wenn die Anforderung persistent ist, wird sie nach der Unterbrechung Ihrer Spot-Instance erneut geöffnet. Wenn die Anforderung persistent ist und Sie die Spot-Instance anhalten, wird die Anforderung erst geöffnet, nachdem Sie die Spot-Instance gestartet haben.



Inhalt

- Anfordern von Anforderungsstatusinformationen
- Statuscodes für Spotanforderungen
- EC2 Ereignis zur Erfüllung von Spot-Instance-Anfragen
- Statusänderungen für eine Spot-Anforderung

Anfordern von Anforderungsstatusinformationen

Sie können Statusinformationen zu Ihrer Spot-Instance-Anforderung abrufen.

Console

So können Sie Informationen zum Anforderungsstatus abrufen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Spot-Anforderungen und wählen Sie die Spot-Anforderung aus.

3. Um den Status zu überprüfen, aktivieren Sie auf der Registerkarte Beschreibung das Feld Status.

AWS CLI

So können Sie Informationen zum Anforderungsstatus abrufen

Verwenden Sie den folgenden describe-spot-instance-requests-Befehl.

```
aws ec2 describe-spot-instance-requests --spot-instance-request-
ids sir-0e54a519c9EXAMPLE
```

PowerShell

So können Sie Informationen zum Anforderungsstatus abrufen

Verwenden Sie das cmdlet Get-EC2SpotInstanceRequest.

```
Get-EC2SpotInstanceRequest -SpotInstanceRequestId sir-0e54a519c9EXAMPLE
```

Statuscodes für Spotanforderungen

Spot-Anforderungsstatusinformationen bestehen aus einem Statuscode, der Aktualisierungszeit und einer Statusmeldung. Gemeinsam helfen Ihnen diese Informationen, die Disposition Ihrer Spot-Anforderung zu ermitteln.

Im Folgenden finden Sie die möglichen Spot-Anforderungsstatuscodes:

`az-group-constraint`

Amazon EC2 kann nicht alle von Ihnen angeforderten Instances in derselben Availability Zone starten.

`bad-parameters`

Ein oder mehrere Parameter für Ihre Spot-Anforderung sind nicht gültig (beispielsweise existiert die angegebene AMI nicht). Die Statusmeldung gibt an, welcher Parameter nicht gültig ist.

`canceled-before-fulfillment`

Der Benutzer hat die Spot-Anforderung abgebrochen, bevor sie erfüllt wurde.

`capacity-not-available`

Es ist nicht genügend Kapazität für die angeforderten Instances vorhanden.

`constraint-not-fulfillable`

Die Spot-Anforderung kann nicht erfüllt werden, da eine oder mehrere Bedingungen nicht gültig sind (beispielsweise ist die Availability Zone nicht vorhanden). Die Statusmeldung gibt an, welche Bedingung nicht gültig ist.

`fulfilled`

Die Spot-Anfrage ist`active`, und Amazon EC2 startet Ihre Spot-Instances.

`instance-stopped-by-price`

Ihre Instance wurde beendet, da der Spot-Preis Ihren Höchstpreis überschritten hat.

`instance-stopped-by-user`

Ihre Instance wurde angehalten, weil ein Benutzer die Instance angehalten oder den Befehl „shutdown“ von der Instance ausgeführt hat.

`instance-stopped-no-capacity`

Ihre Instance wurde aufgrund von EC2 Kapazitätsmanagementanforderungen gestoppt.

`instance-terminated-by-price`

Ihre Instance wurde beendet, da der Spot-Preis Ihren Höchstpreis überschritten hat. Wenn Ihre Anforderung persistent ist, wird der Prozess neu gestartet, sodass die Evaluierung Ihrer Anforderung noch aussteht.

`instance-terminated-by-schedule`

Ihre Spot-Instance wurde am Ende ihrer geplanten Dauer beendet.

`instance-terminated-by-service`

Ihre Instance wurde in einem angehaltenen Zustand beendet.

`instance-terminated-by-user` oder `spot-instance-terminated-by-user`

Sie haben eine Spot-Instance beendet, die bereits erfüllt wurde, deshalb lautet der Anforderungsstatus `closed` (außer bei einer persistenten Anforderung) und der Instance-Status `terminated`.

`instance-terminated-launch-group-constraint`

Eine oder mehrere Instances in Ihrer Startgruppe wurde beendet, sodass die Bedingung für die Startgruppe nicht mehr erfüllt wird.

`instance-terminated-no-capacity`

Ihre Instance wurde aufgrund von standardmäßigen Kapazitätsverwaltungsprozessen beendet.

`launch-group-constraint`

Amazon EC2 kann nicht alle Instances, die Sie angefordert haben, gleichzeitig starten. Alle Instances in einer Startgruppe werden zusammen gestartet und beendet.

`limit-exceeded`

Das Limit für die Anzahl an EBS-Volumes oder der Volume-Gesamtspeicher wurde überschritten. Weitere Informationen finden Sie unter Kontingente für Amazon EBS im Benutzerhandbuch für Amazon EBS.

`marked-for-stop`

Die Spot-Instance wird zum Stoppen markiert.

`marked-for-termination`

Die Spot-Instance wird für das Beenden markiert.

`not-scheduled-yet`

Die Spot-Anfrage wird erst zum geplanten Termin ausgewertet.

`pending-evaluation`

Nachdem Sie eine Spot-Instance-Anforderung erstellt haben, wird diese in den Status `pending-evaluation` versetzt, während das System die Parameter Ihrer Anforderung evaluiert.

`pending-fulfillment`

Amazon EC2 versucht, Ihre Spot-Instances bereitzustellen.

`placement-group-constraint`

Die Spot-Anforderung kann noch nicht erfüllt werden, da eine Spot-Instance zu diesem Zeitpunkt nicht der Platzierungsgruppe hinzugefügt werden kann.

`price-too-low`

Die Anforderung kann noch nicht erfüllt werden, da der Höchstpreis den Spot-Preis unterschreitet. In diesem Fall wird keine Instance gestartet und Ihre Anforderung verbleibt im Status `open`.

`request-canceled-and-instance-running`

Sie haben die Spot-Anforderung abgebrochen, die Spot Instances werden jedoch weiterhin ausgeführt. Die Anforderung weist den Status `cancelled`, die Instances jedoch den Status `running` auf.

`schedule-expired`

Die Spot-Anforderung ist abgelaufen, da sie vor dem angegebenen Datum nicht erfüllt wurde.

`system-error`

Es ist ein unerwarteter Systemfehler aufgetreten. Wenn es sich um ein wiederkehrendes Problem handelt, wenden Sie sich bitte an uns, AWS -Support um Unterstützung zu erhalten.

EC2 Ereignis zur Erfüllung von Spot-Instance-Anfragen

Wenn eine Spot-Instance-Anfrage erfüllt ist, EC2 sendet Amazon ein EC2 Spot-Instance-Request-Erfüllungsereignis an Amazon EventBridge. Sie können eine Regel erstellen, um bei diesem Ereignis jeweils eine Aktion auszuführen, wie z. B. das Aufrufen einer Lambda-Funktion oder das Benachrichtigen eines Amazon-SNS-Themas.

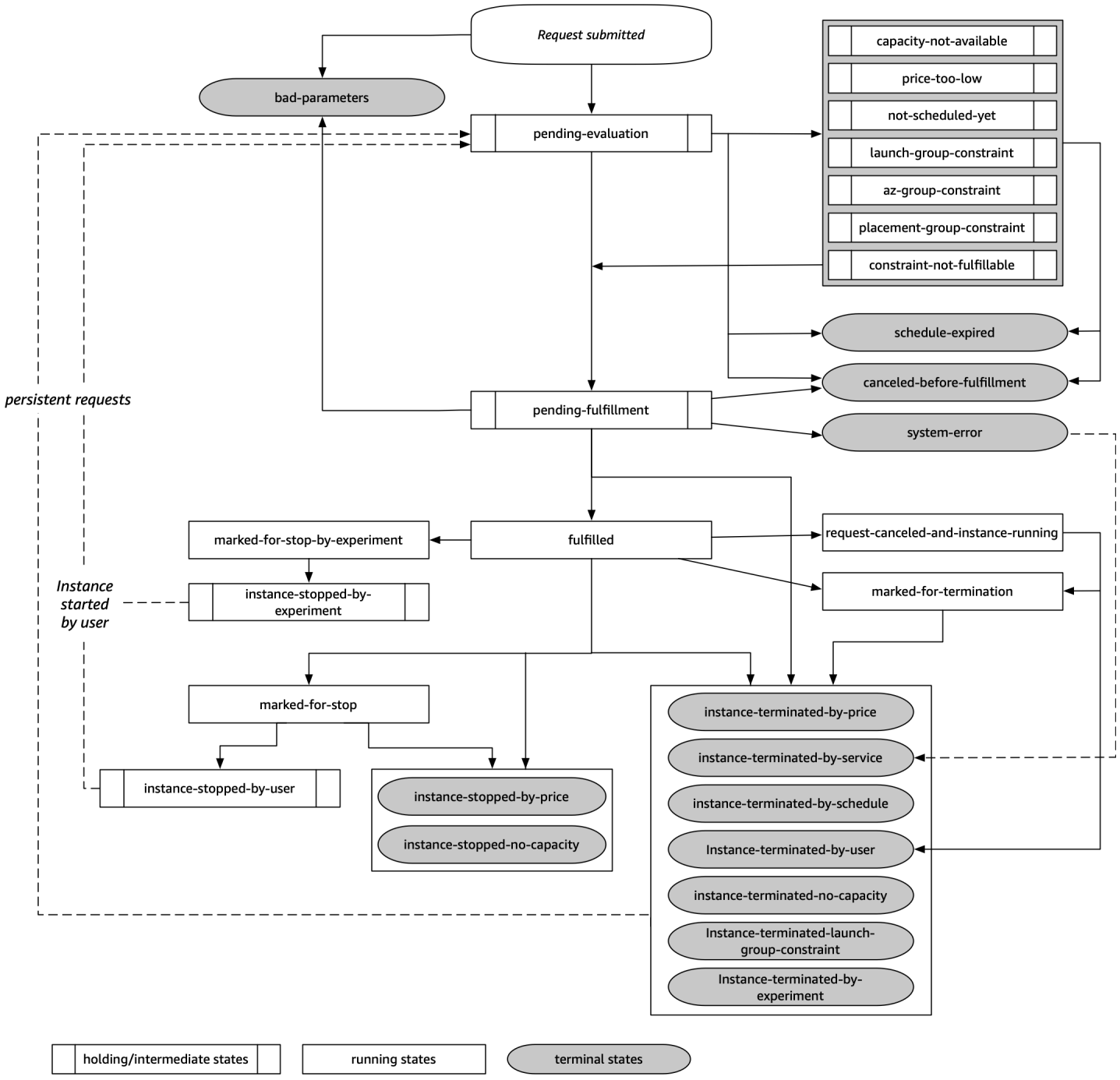
Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "01234567-1234-0123-1234-012345678901",
    "detail-type": "EC2 Spot Instance Request Fulfillment",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "spot-instance-request-id": "sir-0e54a519c9EXAMPLE",
        "instance-id": "i-1234567890abcdef0"
    }
}
```

Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Statusänderungen für eine Spot-Anforderung

Das folgende Diagramm zeigt die Pfade, denen Ihre Spot-Anfrage während ihres Lebenszyklus folgen kann, von der Übermittlung bis zur Beendigung. Die einzelnen Schritte werden durch Knoten dargestellt und der Statuscode für die einzelnen Knoten beschreibt den Status der Spot-Anfrage und der Spot-Instance.



Evaluierung ausstehend

Sobald Sie eine Spot-Instance-Anforderung erstellen, wird diese in den Status `pending-evaluation` versetzt – allerdings nur, wenn keine ungültigen Anforderungsparameter vorliegen (`bad-parameters`).

Statuscode	Anforderungsstatus	Instance-Status
`pending-evaluation`	`open`	Nicht zutreffend
`bad-parameters`	`closed`	Nicht zutreffend

Wartestatus

Wenn eine oder mehrere Anforderungsbedingungen gültig sind, jedoch noch nicht erfüllt werden können oder wenn nicht genügend Kapazität vorhanden ist, geht die Anforderung in einem Wartestatus über, bis die Bedingungen erfüllt werden. Die Anforderungsoptionen wirken sich auf die Wahrscheinlichkeit aus, dass die Anforderung erfüllt wird. Wenn beispielsweise keine Kapazität vorhanden ist, bleibt Ihre Anforderung so lange im Wartestatus, bis Kapazität verfügbar ist. Wenn Sie eine Gruppe von Availability Zones angeben, bleibt die Anforderung so lange im Wartestatus, bis die Bedingung der Availability Zone erfüllt wird.

Im Falle eines Ausfalls einer der Availability Zones besteht die Möglichkeit, dass die freie EC2 Kapazität, die für Spot-Instance-Anfragen in anderen Availability Zones verfügbar ist, beeinträchtigt wird.

Statuscode	Anforderungsstatus	Instance-Status
`capacity-not-available`	`open`	Nicht zutreffend
`price-too-low`	`open`	Nicht zutreffend
`not-scheduled-yet`	`open`	Nicht zutreffend
`launch-group-constraint`	`open`	Nicht zutreffend

Statuscode	Anforderungsstatus	Instance-Status
`az-group-constraint`	`open`	Nicht zutreffend
`placement-group-constraint`	`open`	Nicht zutreffend
`constraint-not-fulfillable`	`open`	Nicht zutreffend

Evaluierung/Erfüllung ausstehend – Terminal

Ihre Spot-Instance-Anforderung kann den Status `terminal` annehmen, wenn Sie eine Anforderung erstellen, die nur während eines bestimmten Zeitraums gültig ist und dieser Zeitraum abläuft, bevor Ihre Anforderung die Phase der ausstehenden Erfüllung erreicht. Dies kann auch vorkommen, wenn Sie die Anforderung abbrechen oder wenn ein Systemfehler auftritt.

Statuscode	Anforderungsstatus	Instance-Status
`schedule-expired`	`cancelled`	Nicht zutreffend
`canceled-before-fulfillment` [1]	`cancelled`	Nicht zutreffend
`bad-parameters`	`failed`	Nicht zutreffend
`system-error`	`closed`	Nicht zutreffend

[1] Wenn Sie die Anforderung abbrechen.

Ausstehende Erfüllung

Wenn die von Ihnen angegebenen Bedingungen (sofern vorhanden) erfüllt werden, geht Ihre Spot-Anforderung in den `pending-fulfillment`-Zustand.

Derzeit bereitet EC2 sich Amazon darauf vor, die von Ihnen angeforderten Instances bereitzustellen. Wenn der Prozess zu diesem Zeitpunkt beendet wird, liegt dies wahrscheinlich daran, dass er durch den Benutzer abgebrochen wurde, bevor eine Spot-Instance gestartet wurde. Dies kann auch daran liegen, dass ein unerwarteter Systemfehler aufgetreten ist.

Statuscode	Anforderungsstatus	Instance-Status
`pending-fulfillment`	`open`	Nicht zutreffend

Erfüllt

Wenn alle Spezifikationen für Ihre Spot Instances erfüllt sind, wird Ihre Spot-Anforderung erfüllt. Amazon EC2 startet die Spot-Instances, was einige Minuten dauern kann. Wenn eine Spot-Instance bei einer Unterbrechung in den Ruhezustand versetzt oder angehalten wird, verbleibt sie in diesem Zustand, bis die Anforderung wieder erfüllt werden kann oder abgebrochen wird.

Statuscode	Anforderungsstatus	Instance-Status
`fulfilled`	`active`	`pending` → `running`
`fulfilled`	`active`	`stopped` → `running`

Wenn Sie eine Spot-Instance stoppen, wird Ihre Spot-Anforderung in den Status `marked-for-stop` oder `instance-stopped-by-user` versetzt, bis die Spot-Instance erneut gestartet werden kann oder die Anforderung storniert wird.

Statuscode	Anforderungsstatus	Instance-Status
`marked-for-stop`	`active`	`stopping`
`instance-stopped-by-user`[1]	`disabled` oder `cancelled` [2]	`stopped`

[1] Eine Spot Instance geht in den `instance-stopped-by-user`-Zustand über, wenn Sie die Instance anhalten oder den Shutdown-Befehl von der Instance aus ausführen. Wenn Sie die Instance

angehalten haben, können Sie sie erneut starten. Beim Neustart kehrt die Spot-Instance-Anfrage in den `pending-evaluation` Status zurück und Amazon EC2 startet dann eine neue Spot-Instance, wenn die Einschränkungen erfüllt sind.

² Der Status der Spot-Anforderung lautet `disabled`, wenn Sie die Spot Instance beenden, aber die Anforderung nicht abbrechen. Der Anforderungsstatus lautet `cancelled`, wenn Ihre Spot-Instance gestoppt wird und die Anforderung abläuft.

Erfüllt – Terminal

Ihre Spot Instance laufen weiter, solange die Kapazität für Ihren Instance-Typ verfügbar ist und Sie die Instance nicht beenden. Wenn Amazon Ihre Spot-Instances beenden EC2 muss, geht die Spot-Anfrage in einen Terminalstatus über. Eine Anforderung geht auch in den Terminal-Status über, wenn Sie die Spot-Anforderung abbrechen oder die Spot Instances beenden.

Statuscode	Anforderungsstatus	Instance-Status
`request-canceled-and-instance-running`	`cancelled`	`running`
`marked-for-stop`	`active`	`running`
`marked-for-termination`	`active`	`running`
`instance-stopped-by-price`	`disabled`	`stopped`
`instance-stopped-by-user`	`disabled`	`stopped`
`instance-stopped-no-capacity`	`disabled`	`stopped`
`instance-terminated-by-price`	`closed` (einmalig), `open` (persistent)	`terminated`
`instance-terminated-by-schedule`	`closed`	`terminated`

Statuscode	Anforderungsstatus	Instance-Status
`instance-terminated-by-service`	`cancelled`	`terminated`
`instance-terminated-by-user`	`closed` oder `cancelled` [1]	`terminated`
`instance-terminated-no-capacity`	`closed` (einmalig), `open` (persistent)	`running` †
`instance-terminated-no-capacity`	`closed` (einmalig), `open` (persistent)	`terminated`
`instance-terminated-launch-group-constraint`	`closed` (einmalig), `open` (persistent)	`terminated`

[1] Der Anforderungsstatus lautet `closed`, wenn Sie die Instance beenden, die Anforderung jedoch nicht abbrechen. Der Anforderungsstatus lautet `cancelled`, wenn Sie die Instance beenden und die Anforderung abbrechen. Selbst wenn Sie eine Spot-Instance beenden, bevor Sie ihre Anfrage stornieren, kann es zu einer Verzögerung kommen, bis Amazon EC2 feststellt, dass Ihre Spot-Instance beendet wurde. In diesem Fall kann der Anforderungsstatus entweder `closed` oder `cancelled` lauten.

† Wenn Amazon eine Spot-Instance EC2 unterbricht, wenn sie die Kapazität wieder benötigt, und die Instance so konfiguriert ist, dass sie bei einer Unterbrechung beendet wird, wird der Status sofort auf `instance-terminated-no-capacity` (nicht gesetzt`marked-for-termination`) gesetzt. Die Instance bleibt jedoch 2 Minuten lang im Status `running`, um den 2-Minuten-Zeitraum widerzuspiegeln, in dem die Instance die Unterbrechungsmitteilung für die Spot-Instance erhält. Nach 2 Minuten wird der Instance-Status auf `terminated` festgelegt.

Unterbrechungsversuche

Sie können AWS Fault Injection Service damit eine Spot-Instance-Unterbrechung einleiten, sodass Sie testen können, wie die Anwendungen auf Ihren Spot-Instances reagieren. Wenn eine Spot-Instance AWS FIS gestoppt wird, wechselt Ihre Spot-Anfrage in den `marked-for-stop-by-experiment` Status und dann in den `instance-stopped-by-experiment` Status. Wenn

eine Spot-Instance AWS FIS beendet wird, wechselt Ihre Spot-Anfrage in den `instance-terminated-by-experiment` Status. Weitere Informationen finden Sie unter the section called "Eine Unterbrechung einleiten".

Statuscode	Anforderungsstatus	Instance-Status
`marked-for-stop-by-experiment`	`active`	`running`
`instance-stopped-by-experiment`	`disabled`	`stopped`
`instance-terminated-by-experiment`	`closed`	`terminated`

Persistente Anforderungen

Wenn Ihre Spot-Instances beendet werden (entweder von Ihnen oder Amazon EC2) und es sich bei der Spot-Anfrage um eine persistente Anfrage handelt, kehrt sie in den `pending-evaluation` Status zurück, und Amazon EC2 kann dann eine neue Spot-Instance starten, wenn die Einschränkungen erfüllt sind.

Spot-Instance-Anforderungen markieren

Um die Kategorisierung und Verwaltung Ihrer Spot-Instance-Anforderungen zu vereinfachen, können Sie sie mit benutzerdefinierten Metadaten markieren. Sie können einer Spot-Instance-Anforderung beim Erstellen oder danach einen Tag (Markierung) zuweisen. Sie können Tags mithilfe der EC2 Amazon-Konsole oder eines Befehlszeilentools zuweisen.

Wenn Sie eine Spot-Instance-Anforderung markieren, werden die Instances und Volumes, die von der Spot-Instance-Anforderung gestartet werden, nicht automatisch markiert. Sie müssen die von der Spot-Instance-Anforderungen gestarteten Instances und Volumes explizit markieren. Sie können ein Tag (Markierung) zu einer Spot-Instance und Volumes während des Starts oder danach zuweisen.

Weitere Informationen zur Funktionsweise von Tags (Markierungen) finden Sie unter Kennzeichnen Sie Ihre EC2 Amazon-Ressourcen.

Inhalt

- Voraussetzungen

- Neue Spot-Instance-Anforderung markieren
- So markieren Sie eine vorhandene Spot-Instance-Anforderung:
- Anzeigen von Anforderungs-Tags (Markierungen) der Spot-Instance

Voraussetzungen

Gewähren Sie dem Benutzer die Berechtigung zum Markieren von Ressourcen. Weitere Informationen zu IAM-Richtlinien und Beispielrichtlinien finden Sie unter Beispiel: Markieren von Ressourcen.

Die von Ihnen erstellte IAM-Richtlinie wird anhand der Methode bestimmt, mit der Sie eine Spot-Instance-Anforderung erstellen.

- Wenn Sie den Launch Instance Wizard oder `run-instances` zum Anfordern von Spot Instances verwenden, finden Sie weitere Informationen unter To grant a user the permission to tag resources when using the launch instance wizard or run-instances.
- Wenn Sie den `request-spot-instances`-Befehl verwenden, um Spot Instances anzufordern, lesen Sie To grant a user the permission to tag resources when using request-spot-instances.

So gewähren Sie einem Benutzer die Berechtigung, Ressourcen zu markieren, wenn er den Launch Instance Wizard oder zum Ausführen von Instances verwendet

Erstellen Sie eine IAM-Richtlinie, die Folgendes beinhaltet:

- Die Aktion `ec2:RunInstances`. Dadurch wird dem Benutzer die Berechtigung zum Starten einer Instance gewährt.
- Legen Sie für `Resource` die Option `spot-instances-request` fest. Auf diese Weise können Benutzer Spot-Instance-Anforderungen erstellen, die Spot Instances anfordern.
- Die Aktion `ec2:CreateTags`. Dadurch erhält der Benutzer die Berechtigung zum Erstellen von Tags.
- Legen Sie für `Resource` die Option `*` fest. Auf diese Weise können Benutzer alle Ressourcen markieren, die während des Instance-Starts erstellt werden.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowLaunchInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagSpotInstanceRequests",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Wenn Sie die RunInstances Aktion verwenden, um Spot-Instance-Anfragen zu erstellen und die Spot-Instance-Anfragen bei der Erstellung zu taggen, müssen Sie wissen, wie Amazon EC2 die `spot-instances-request` Ressource in der RunInstances Erklärung bewertet, sie wird in der IAM-Richtlinie wie folgt bewertet:

- Wenn Sie eine Spot-Instance-Anfrage bei der Erstellung EC2 nicht taggen, bewertet Amazon die `spot-instances-request` Ressource in der RunInstances Abrechnung nicht.
- Wenn Sie eine Spot-Instance-Anfrage bei der Erstellung taggen, EC2 bewertet Amazon die `spot-instances-request` Ressource in der RunInstances Abrechnung.

Daher gelten für die `spot-instances-request`-Ressource die folgenden Regeln für die IAM-Richtlinie:

- Wenn Sie RunInstances eine Spot-Instance-Anfrage erstellen und nicht beabsichtigen, die Spot-Instance-Anfrage bei der Erstellung zu taggen, müssen Sie die `spot-instances-request` Ressource nicht explizit zulassen. Der Aufruf ist erfolgreich.
- Wenn Sie RunInstances eine Spot-Instance-Anfrage erstellen und beabsichtigen, die Spot-Instance-Anfrage bei der Erstellung zu taggen, müssen Sie die `spot-instances-request` Ressource in die RunInstances Allow-Anweisung aufnehmen, andernfalls schlägt der Aufruf fehl.
- Wenn Sie RunInstances eine Spot-Instance-Anfrage erstellen und beabsichtigen, die Spot-Instance-Anfrage bei der Erstellung zu taggen, müssen Sie die `spot-instances-request` Ressource angeben oder einen * Platzhalter in der Allow-Anweisung CreateTags angeben, andernfalls schlägt der Aufruf fehl.

Beispiele für IAM-Richtlinien, einschließlich Richtlinien, die für Spot-Instance-Anforderungen nicht unterstützt werden, finden Sie unter Arbeiten mit Spot-Instances.

Um einem Benutzer die Erlaubnis zu erteilen, Ressourcen zu taggen, wenn er request-spot-instances

Erstellen Sie eine IAM-Richtlinie, die Folgendes beinhaltet:

- Die Aktion `ec2:RequestSpotInstances`. Dadurch erhält der Benutzer die Berechtigung zum Erstellen einer Spot-Instance-Anforderung.
- Die Aktion `ec2:CreateTags`. Dadurch erhält der Benutzer die Berechtigung zum Erstellen von Tags.
- Legen Sie für `Resource` die Option `spot-instances-request` fest. Auf diese Weise können Benutzer nur die Spot-Instance-Anforderung markieren.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotInstanceRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:RequestSpotInstances",
                "ec2:CreateTags"
            ],
```

```
            "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-instances-
request/*"
        }
    ]
}
```

Neue Spot-Instance-Anforderung markieren

Konfigurieren Sie in den PowerShell Beispielen AWS CLI und die Spot-Instance-Anfrage wie folgt:

- Legen Sie für `ResourceType` die Option `spot-instances-request` fest. Wenn Sie einen anderen Wert angeben, schlägt die Spot-Instance-Anforderung fehl.
- Geben Sie für `Tags` das Schlüssel-Wert-Paar an. Sie können mehr als ein Schlüssel-Wert-Paar angeben.

Console

So markieren Sie eine neue Spot-Instance-Anforderung

1. Folgen Sie dem Verfahren unter Ihre Spot Instances verwalten.
2. Um ein Tags (Markierungen) hinzuzufügen, wählen Sie auf der Seite Add Tags (Tags (Markierungen) hinzufügen) die Option Add Tags (Tags (Markierungen) hinzufügen) und geben Sie den Schlüssel und den Wert für den Tag (Markierung) ein. Wählen Sie für jedes weitere Tags (Markierungen) Add another Tag (Weiteren Tag (Markierungen) hinzufügen) .

   Für jeden Tag (Markierung) können Sie die Spot-Instance-Anforderung, die Spot Instances und die Volumes mit demselben Tag (Markierung) markieren. Um alle drei zu markieren, stellen Sie sicher, dass Instances , Volumes und Spot-Instance-Anforderungen ausgewählt sind. Wenn Sie nur ein oder zwei mit Tags (Markierungen) markieren möchten, stellen Sie sicher, dass die Ressourcen, die Sie markieren möchten, ausgewählt sind und die anderen Ressourcen gelöscht wurden.
3. Füllen Sie die erforderlichen Felder aus, um eine Spot-Instance-Anforderung zu erstellen, und wählen Sie dann Launch (Starten) aus. Weitere Informationen finden Sie unter Ihre Spot Instances verwalten.

AWS CLI

So markieren Sie eine neue Spot-Instance-Anforderung

Verwenden Sie den Befehl request-spot-instances mit der Option `--tag-specification` .

Die Tag-Spezifikation fügt der Spot-Instance-Anfrage zwei Tags hinzu: `Environment=Production` und `Cost-Center=123`.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json \
    --tag-specification 'ResourceType=spot-instances-
request,Tags=[{Key=Environment,Value=Production},{Key=Cost-Center,Value=123}]'
```

PowerShell

So markieren Sie eine neue Spot-Instance-Anforderung

Verwenden Sie das Request-EC2SpotInstanceCmdlet mit dem `-TagSpecification` Parameter.

```
-TagSpecification $tagspec
```

Die Tag-Spezifikation ist wie folgt definiert. Es werden der Spot-Instance-Anforderung zwei Tags hinzugefügt: `Environment=Production` und `Cost-Center=123`.

```
$tag1 = @{Key="Environment"; Value="Production"}
$tag2 = @{Key="Cost-Center"; Value="123"}
$tagspec = New-Object Amazon.EC2.Model.TagSpecification
$tagspec.ResourceType = "spot-instances-request"
$tagspec.Tags = @($tag1,$tag2)
```

So markieren Sie eine vorhandene Spot-Instance-Anforderung:

Console

So markieren Sie eine vorhandene Spot-Instance-Anforderung

Nachdem Sie eine Spot-Instance-Anforderung erstellt haben, können Sie der Spot-Instance-Anforderung mithilfe der Konsole Tags (Markierungen) hinzufügen.

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Instance-Anforderung aus.
4. Wählen Sie die Registerkarte Tags (Markierungen), und wählen Sie Create Tags (Tags (Markierungen) erstellen).

So markieren Sie eine bestehende Spot-Instance-Anforderung mithilfe der Konsole:

Nachdem Ihre Spot-Instance-Anforderung Ihre Spot-Instance gestartet hat, können Sie der Instance mithilfe der Konsole Tags (Markierungen) hinzufügen. Weitere Informationen finden Sie unter Hinzufügen von Tags mithilfe der Konsole.

AWS CLI

So markieren Sie eine vorhandene Spot-Instance-Anforderung oder Spot Instance

Verwenden Sie den Befehl create-tags, um vorhandene Ressourcen zu markieren. Im folgenden Beispiel werden die vorhandene Spot-Instance-Anforderung und die Spot Instance mit `purpose=test` markiert.

```
aws ec2 create-tags \
    --resources sir-0e54a519c9EXAMPLE i-1234567890abcdef0 \
    --tags Key=purpose,Value=test
```

PowerShell

So markieren Sie eine vorhandene Spot-Instance-Anforderung oder Spot Instance

Verwenden Sie das cmdlet New-EC2Tag. Im folgenden Beispiel wird das Tag `purpose=test` zu der vorhandenen Spot-Instance-Anforderung und der Spot-Instance hinzugefügt.

```
New-EC2Tag `
    -Resource sir-0e54a519c9EXAMPLE, i-1234567890abcdef0 `
    -Tag @{Key="purpose"; Value="test"}
```

Anzeigen von Anforderungs-Tags (Markierungen) der Spot-Instance

Console

So können Sie Tags für die Spot-Instance-Anforderung anzeigen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Instance-Anforderung und dann die Registerkarte Tags aus.

AWS CLI

So beschreiben Sie Anforderungs-Tags (Markierungen) der Spot-Instance:

Verwenden Sie den describe-spot-instance-requestsBefehl, um die Konfiguration der angegebenen Spot-Instance-Anfrage anzuzeigen, einschließlich aller Tags, die für die Anfrage angegeben wurden.

```
aws ec2 describe-spot-instance-requests \
    --spot-instance-request-ids sir-0e54a519c9EXAMPLE \
    --query "SpotInstanceRequests[*].Tags"
```

Es folgt eine Beispielausgabe.

```
[
    [
        {
            "Key": "Environment",
            "Value": "Production"
        },
        {
            "Key": "Department",
            "Value": "101"
        }
    ]
]
```

PowerShell

So beschreiben Sie Anforderungs-Tags (Markierungen) der Spot-Instance:

Verwenden Sie das cmdlet Get-EC2SpotInstanceRequest.

```
(Get-EC2SpotInstanceRequest `
    -SpotInstanceRequestId sir-0e54a519c9EXAMPLE).Tags
```

Es folgt eine Beispielausgabe.

```
Key         Value
---         -----
Environment Production
Department  101
```

Stornieren einer Spot-Instance-Anforderung

Wenn Sie Ihre Spot-Instance-Anforderung nicht mehr benötigen, können Sie sie abbrechen. Sie können nur Spot-Instance-Anforderungen stornieren, deren Status `open`, `active` oder `disabled` lautet.

- Ihre Spot-Instance-Anforderung weist den Status `open` auf, wenn sie noch nicht erfüllt wurde und keine Instances gestartet wurden.
- Ihre Spot-Instance-Anforderung weist den Status `active` auf, wenn sie erfüllt wurde und Spot Instances infolgedessen gestartet wurden.
- Ihre Spot-Instance-Anforderung weist den Status `disabled` auf, wenn Sie die Spot-Instance stoppen.

Wenn der Status Ihrer Spot-Instance-Anforderung `active` ist und eine zugehörige Spot-Instance läuft, wird diese Instance durch das Stornieren der Anforderung nicht beendet. Weitere Informationen zum Beenden von Spot-Instances finden Sie unter Beenden einer Spot-Instance.

Console

So stornieren Sie eine Spot-Instance-Anforderung

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie die Spot-Instance-Anfrage aus.
4. Wählen Sie Actions (Aktionen), Cancel request (Anforderungen abbrechen).

5. (Optional) Wenn Sie die zugehörigen Spot Instances nicht mehr benötigen, können Sie diese beenden. Wählen Sie im Dialogfeld Cancel Spot request (Spot-Anforderung abbrechen) die Option Terminate instances (Instances beenden) und klicken Sie dann auf Confirm (Bestätigen).

AWS CLI

So stornieren Sie eine Spot-Instance-Anforderung

Verwenden Sie den folgenden cancel-spot-instance-requests-Befehl.

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-
ids sir-0e54a519c9EXAMPLE
```

PowerShell

So stornieren Sie eine Spot-Instance-Anforderung

Verwenden Sie das cmdlet Stop-EC2SpotInstanceRequest.

```
Stop-EC2SpotInstanceRequest -SpotInstanceRequestId sir-0e54a519c9EXAMPLE
```

Ihre Spot Instances verwalten

Amazon EC2 startet eine Spot-Instance, wenn Kapazität verfügbar ist. Eine Spot-Instance wird so lange ausgeführt, bis sie entweder unterbrochen oder von Ihnen beendet wird.

Inhalt

- Ihre Spot Instances finden
- Instances suchen, die durch eine bestimmte Anforderung gestartet wurden
- Anhalten einer Spot-Instance
- Starten einer Spot-Instance
- Beenden einer Spot-Instance

Ihre Spot Instances finden

Eine Spot Instance wird zusammen mit On-Demand-Instances auf der Instance-Seite in der Konsole angezeigt. Gehen Sie wie folgt vor, um Ihre Spot Instances zu finden.

Console

So suchen Sie Ihre Spot Instances

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Um alle Spot Instances zu finden, wählen Sie im Suchbereich Instance lifecycle =spot.
4. Um zu überprüfen, ob es sich bei einer Instance um eine Spot Instance handelt, wählen Sie die Instance aus, wählen Sie die Registerkarte Details und überprüfen Sie den Wert von Lifecycle. Der Wert für eine Spot Instance ist `spot` und der Wert für eine On-Demand-Instance ist `normal`.

AWS CLI

So suchen Sie Ihre Spot Instances

Verwenden Sie den folgenden describe-instances-Befehl.

```
aws ec2 describe-instances --filters "Name=instance-lifecycle,Values=spot"
```

So stellen Sie fest, ob es sich bei einer Instance um eine Spot Instance handelt

Verwenden Sie den folgenden describe-instances-Befehl.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[*].Instances[*].InstanceLifecycle" \
    --output text
```

Wenn der Wert `spot` ist, ist die Instance eine Spot Instance. Wenn keine Ausgabe erfolgt, ist die Instance eine On-Demand-Instance.

PowerShell

So suchen Sie Ihre Spot Instances

Verwenden Sie das cmdlet Get-EC2Instance.

```
Get-EC2Instance -Filter @{Name="instance-lifecycle"; Values="spot"}
```

So stellen Sie fest, ob es sich bei einer Instance um eine Spot Instance handelt

Verwenden Sie das cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.InstanceLifecycle
```

Wenn der Wert `Spot` ist, ist die Instance eine Spot Instance. Wenn keine Ausgabe erfolgt, ist die Instance eine On-Demand-Instance.

Instances suchen, die durch eine bestimmte Anforderung gestartet wurden

Gehen Sie wie folgt vor, um die Spot Instances zu suchen, die über eine bestimmte Spot-Instance- oder Spot-Flotte-Anfrage gestartet wurden.

Console

So suchen Sie die Spot Instances für eine Anforderung

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus. Die Liste enthält sowohl Spot-Instance-Anfragen als auch Spot-Flotte-Anfragen.
3. Wenn eine Spot-Instance-Anfrage erfüllt wurde, ist Kapazität die ID der Spot Instance. Bei einer Spot-Flotte zeigt Kapazität an, wie viel der angeforderten Kapazität erfüllt wurde. Um die IDs Instances in einer Spot-Flotte anzuzeigen, klicken Sie auf den Erweiterungspfeil oder wählen Sie die Flotte aus und wählen Sie Instances.
4. Bei einer Spot-Flotte zeigt Kapazität an, wie viel der angeforderten Kapazität erfüllt wurde. Um die IDs Instances in einer Spot-Flotte anzuzeigen, wählen Sie die Flotten-ID aus, um die zugehörige Detailseite zu öffnen und den Bereich Instances zu suchen.

AWS CLI

So suchen Sie die Spot Instances für eine Anforderung

Verwenden Sie den folgenden describe-spot-instance-requests-Befehl.

```
aws ec2 describe-spot-instance-requests \
    --spot-instance-request-ids sir-0e54a519c9EXAMPLE \
    --query "SpotInstanceRequests[*].{ID:InstanceId}"
```

Das Folgende ist eine Beispielausgabe:

```
[
    {
        "ID": "i-1234567890abcdef0"
    },
    {
        "ID": "i-0598c7d356eba48d7"
    }
]
```

PowerShell

So suchen Sie die Spot Instances für eine Anforderung

Verwenden Sie das cmdlet Get-EC2SpotInstanceRequest.

```
(Get-EC2SpotInstanceRequest -SpotInstanceRequestId sir-0e54a519c9EXAMPLE).InstanceId
```

Anhalten einer Spot-Instance

Wenn Sie die Spot Instances jetzt nicht benötigen, sie aber später neu starten möchten, ohne die Daten auf dem Amazon-EBS-Volume zu verlieren, können Sie sie anhalten. Die Schritte zum Anhalten einer Spot-Instance ähneln den Schritten zum Anhalten einer On-Demand-Instance.

> **Note**
>
> Wenn eine Spot-Instance angehalten wird, können Sie mache Instance-Attribute ändern, aber nicht den Instance-Typ.
> Wir stellen für eine angehaltene Spot-Instance keine abgerechneten Nutzungsgebühren oder Gebühren für die Datenübertragung in Rechnung. Für Speicher für Amazon EBS-Volumes fallen jedoch Gebühren an.

Einschränkungen

- Sie können eine Spot-Instance nur anhalten, wenn die Spot-Instance aus einer `persistent`-Spot-Instance-Anforderung gestartet wurde.
- Sie können eine Spot-Instance nicht anhalten, wenn die zugehörige Spot-Instance-Anforderung abgebrochen wurde. Wenn die Spot-Instance-Anforderung abgebrochen wurde, können Sie nur die Spot-Instance beenden.

- Sie können eine Spot-Instance nicht anhalten, wenn sie Teil einer Flotte, einer Startgruppe oder einer Availability-Zone-Gruppe ist.

Console

So halten Sie eine Spot Instance an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Spot Instance aus. Wenn Sie die Instance-ID der Spot Instance nicht gespeichert haben, finden Sie weitere Informationen unter the section called “Ihre Spot Instances finden”.
4. Wählen Sie Instance state (Instance-Status), Stop instance (Instance anhalten).
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Stop aus.

AWS CLI

So halten Sie eine Spot Instance an

Verwenden Sie den Befehl stop-instances, um eine oder mehrere Spot Instances manuell anzuhalten.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

PowerShell

So halten Sie eine Spot Instance an

Verwenden Sie das cmdlet Stop-EC2Instance.

```
Stop-EC2Instance -InstanceId i-1234567890abcdef0
```

Starten einer Spot-Instance

Sie können eine Spot-Instance starten, die Sie zuvor angehalten haben.

Voraussetzungen

Sie können eine Spot-Instance nur starten, wenn:

- Sie die Spot-Instance manuell angehalten haben.
- Die Spot-Instance eine EBS-gestützte Instance ist.
- Spot-Instance-Kapazität verfügbar ist.
- Der Spot-Preis niedriger ist als Ihr Höchstpreis.

Einschränkungen

- Sie können eine Spot-Instance nicht starten, wenn sie Teil einer Flotte, einer Startgruppe oder einer Availability-Zone-Gruppe ist.

Die Schritte zum Starten einer Spot-Instance ähneln den Schritten zum Starten einer On-Demand-Instance.

Console

So starten Sie eine Spot Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Spot Instance aus. Wenn Sie die Instance-ID der Spot Instance nicht gespeichert haben, finden Sie weitere Informationen unter the section called “Ihre Spot Instances finden”.
4. Wählen Sie Instance state (Instance-Status), Start instance (Instance starten).

AWS CLI

So starten Sie eine Spot Instance

Verwenden Sie den Befehl start-instances, um eine oder mehrere Spot Instances manuell zu starten.

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

PowerShell

So starten Sie eine Spot Instance

Verwenden Sie das cmdlet Start-EC2Instance.

```
Start-EC2Instance -InstanceId i-1234567890abcdef0
```

Beenden einer Spot-Instance

> **Warning**
>
> Das Beenden einer Instance ist dauerhaft und irreversibel.
> Nachdem Sie eine Instance beendet haben, können Sie keine Verbindung mehr zu ihr herstellen und sie kann nicht wiederhergestellt werden. Alle angehängten Amazon-EBS-Volumes, die so konfiguriert sind, dass sie beim Beenden gelöscht werden, werden ebenfalls dauerhaft gelöscht und können nicht wiederhergestellt werden. Alle auf den Instance-Speicher-Volumes gespeicherten Daten gehen dauerhaft verloren. Weitere Informationen finden Sie unter Wie die Kündigung von Instances funktioniert.
> Bevor Sie eine Instance beenden, stellen Sie sicher, dass Sie alle Daten, die Sie nach der Beendigung behalten müssen, im persistenten Speicher gesichert haben.

Wenn Sie eine laufende oder angehaltene Spot-Instance beenden, die durch eine persistente Spot-Instance-Anforderung gestartet wurde, geht die Spot-Instance-Anforderung in den Status `open` über, sodass eine neue Spot-Instance gestartet werden kann. Um sicherzustellen, dass keine neue Spot-Instance gestartet wird, müssen Sie zuerst die Spot-Instance-Anforderung stornieren.

Wenn Sie eine `active`-Spot-Instance-Anfrage mit einer laufenden Spot-Instance abbrechen, wird die laufende Spot-Instance nicht automatisch beendet. Sie müssen die Spot-Instance manuell beenden.

Wenn Sie eine `disabled` Spot-Instance-Anfrage stornieren, die eine gestoppte Spot-Instance hat, wird die gestoppte Spot-Instance automatisch vom Amazon EC2 Spot-Service beendet. Es kann eine kurze Verzögerung zwischen dem Abbrechen der Spot-Instance-Anfrage und dem Zeitpunkt geben, an dem der Spot-Service die Spot-Instance beendet.

Weitere Informationen finden Sie unter Stornieren einer Spot-Instance-Anforderung.

Console

So beenden Sie eine Spot Instance manuell

1. Stellen Sie vor dem Beenden einer Instance sicher, dass Sie keine Daten verlieren werden, indem Sie sich vergewissern, dass Ihre Amazon EBS-Volumes beim Abschalten nicht

gelöscht werden und dass Sie alle Daten kopiert haben, die Sie von Ihren Instance-Speicher-Volumes für persistenten Speicher wie Amazon EBS oder Amazon S3 benötigen.

2. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
3. Wählen Sie im Navigationsbereich Instances aus.
4. Wählen Sie die Spot Instance aus. Wenn Sie die Instance-ID der Spot Instance nicht gespeichert haben, finden Sie weitere Informationen unter the section called “Ihre Spot Instances finden”.
5. Wählen Sie Instance-Status, Instance beenden (löschen).
6. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Beenden (löschen) aus.

AWS CLI

So beenden Sie eine Spot Instance manuell

Verwenden Sie den Befehl terminate-instances, um Spot Instances manuell zu beenden.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7
```

PowerShell

So beenden Sie eine Spot Instance manuell

Verwenden Sie das cmdlet Remove-EC2Instance.

```
Remove-EC2Instance -InstanceId i-1234567890abcdef0
```

Spot-Instance-Unterbrechungen

Sie können Spot-Instances mit freier EC2 Kapazität starten und erhalten hohe Rabatte. Im Gegenzug erhalten Sie die Instances im Gegenzug, wenn Amazon die Kapazität wieder EC2 benötigt. Wenn Amazon eine Spot-Instance EC2 zurückfordert, bezeichnen wir dieses Ereignis als Spot-Instance-Unterbrechung.

Die Nachfrage nach Spot-Instances kann von Moment zu Moment erheblich variieren, und die Verfügbarkeit von Spot-Instances kann ebenfalls erheblich variieren, je nachdem, wie viele ungenutzte EC2 Instances verfügbar sind. Zudem besteht immer die Möglichkeit, dass Ihre Spot-Instance unterbrochen wird. Im Folgenden sind die möglichen Gründe aufgeführt, aus denen Amazon Ihre Spot-Instances unterbrechen EC2 könnte:

Kapazität

Amazon EC2 kann Ihre Spot-Instance unterbrechen, wenn sie wieder benötigt wird. EC2 nimmt Ihre Instance hauptsächlich für die Wiederverwendung von Kapazität zurück. Dies kann jedoch auch aus anderen Gründen geschehen, z. B. zur Wartung des Hosts oder zur Außerbetriebnahme von Hardware.

Preis

Der Spotpreis ist höher als Ihr Höchstpreis.

Sie können den Höchstpreis in Ihrer Spot-Anforderung angeben. Wenn Sie jedoch einen Höchstpreis angeben, werden Ihre Instances häufiger unterbrochen, als wenn Sie dies nicht tun.

Beschränkungen

Wenn Ihre Spot-Anforderung eine Bedingung enthält, z. B. eine Startgruppe oder eine Gruppe von Availability Zones, werden die Spot Instances als Gruppe beendet, wenn die Bedingung nicht mehr erfüllt werden kann.

Wenn Amazon eine Spot-Instance EC2 unterbricht, wird die Instance entweder beendet, gestoppt oder in den Ruhezustand versetzt, je nachdem, welches Unterbrechungsverhalten Sie bei der Erstellung der Spot-Anfrage angegeben haben.

Inhalt

- Verhalten von Spot-Instance-Unterbrechungen
- Auf Spot-Instance-Unterbrechungen vorbereiten
- Initiieren einer Spot-Instance-Unterbrechung
- Spot-Instance-Unterbrechungsbenachrichtigungen
- Finden von unterbrochenen Spot-Instances
- Ermitteln Sie, ob Amazon eine Spot-Instance EC2 beendet hat
- Fakturierung für unterbrochene Spot-Instances

Verhalten von Spot-Instance-Unterbrechungen

Sie können das Unterbrechungsverhalten angeben, wenn Sie eine Spot-Anforderung erstellen. Die folgenden Verhaltensweisen sind bei Unterbrechungen möglich:

- Stoppen

- Hibernate
- Beenden

Das Standardverhalten ist, dass Amazon Spot-Instances EC2 beendet, wenn sie unterbrochen werden.

Unterbrochene Spot Instances anhalten

Sie können angeben, dass Amazon Ihre Spot-Instances EC2 stoppt, wenn sie unterbrochen werden. Der Spot Instance-Anfrage-Typ muss `persistent` sein. Sie können in der Spot-Instance-Anforderung keine Startgruppe angeben. Für EC2 Fleet oder Spot Fleet muss der Anfragetyp lauten`maintain`.

Überlegungen

- Nur Amazon EC2 kann eine unterbrochene, gestoppte Spot-Instance neu starten.
- Für eine Spot-Instance, die durch eine `persistent` Spot-Instance-Anfrage gestartet wurde: Amazon EC2 startet die gestoppte Instance neu, wenn Kapazität in derselben Availability Zone und für denselben Instance-Typ wie die gestoppte Instance verfügbar ist (es muss dieselbe Startspezifikation verwendet werden).
- Wenn eine Spot-Instance angehalten wird, können Sie mache Instance-Attribute ändern, aber nicht den Instance-Typ. Wenn Sie ein EBS-Volume trennen oder löschen, wird es nicht neu zugeordnet, wenn die Spot-Instance gestartet wird. Wenn Sie das Root-Volume trennen und Amazon EC2 versucht, die Spot-Instance zu starten, kann die Instance nicht gestartet werden und Amazon EC2 beendet die gestoppte Instance.
- Sie können eine Spot-Instance beenden, wenn sie angehalten wird.
- Wenn Sie eine Spot-Instance-Anfrage, eine EC2 Flotte oder eine Spot-Flotte stornieren, EC2 beendet Amazon alle zugehörigen Spot-Instances, die gestoppt wurden.
- Während eine unterbrochene Spot-Instance angehalten wird, werden nur Gebühren für die EBS-Volumes berechnet, die beibehalten werden. Mit EC2 Fleet und Spot Fleet können Sie, wenn Sie viele gestoppte Instances haben, das Limit für die Anzahl der EBS-Volumes für Ihr Konto überschreiten. Weitere Informationen zur Kostenberechnung, wenn eine Spot-Instance unterbrochen wird, finden Sie unter Fakturierung für unterbrochene Spot-Instances.
- Stellen Sie sicher, dass Sie mit den Auswirkungen des Stoppens einer Instance vertraut sind. Weitere Informationen darüber, was passiert und was Sie tun können, wenn eine Instance angehalten wird, finden Sie unter Unterschiede zwischen Instance-Status.

Unterbrochene Spot Instances in den Ruhezustand versetzen

Sie können angeben, dass Amazon Ihre Spot-Instances in EC2 den Ruhezustand versetzt, wenn sie unterbrochen werden. Weitere Informationen finden Sie unter Versetzen Sie Ihre Amazon-Instance in den Ruhezustand EC2 .

Amazon bietet EC2 jetzt dasselbe Ruhezustandserlebnis für Spot-Instances wie derzeit für On-Demand-Instances. Es bietet eine umfassendere Unterstützung, wobei für den Ruhezustand von Spot Instances jetzt Folgendes unterstützt wird:

- Mehr Unterstützung AMIs
- Weitere unterstützte Instance-Familien
- Vom Benutzer initiierter Ruhezustand

Unterbrochene Spot Instances beenden

Wenn Amazon eine Spot-Instance EC2 unterbricht, wird die Instance standardmäßig beendet, es sei denn, Sie geben ein anderes Unterbrechungsverhalten an, z. B. Stop oder Hibernate. Weitere Informationen finden Sie unter EC2 Amazon-Instances beenden.

Auf Spot-Instance-Unterbrechungen vorbereiten

Die Nachfrage nach Spot-Instances kann von einem Moment zum nächsten erheblich variieren, und die Verfügbarkeit von Spot-Instances kann sich abhängig von der Verfügbarkeit ungenutzter EC2-Instances ebenfalls erheblich unterscheiden. Zudem besteht immer die Möglichkeit, dass Ihre Spot-Instance unterbrochen wird. Aus diesem Grund müssen Sie sicherstellen, dass Ihre Anwendung auf eine Spot-Instance-Unterbrechung vorbereitet ist.

Wir empfehlen, dass Sie sich an die folgenden bewährten Methoden halten, damit Sie auf eine Unterbrechung der Spot-Instance vorbereitet sind.

- Erstellen Sie Ihre Spot-Anfrage mithilfe einer Amazon EC2 Auto Scaling Scaling-Gruppe. Wenn Ihre Spot-Instances unterbrochen werden, startet die Amazon EC2 Auto Scaling Scaling-Gruppe automatisch Ersatz-Instances. Weitere Informationen finden Sie unter Amazon EC2 Auto Scaling Scaling-Gruppen mit mehreren Instance-Typen und Kaufoptionen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.
- Stellen Sie sicher, dass Ihre Instance einsatzbereit ist, sobald die Anforderung erfüllt ist, indem Sie ein Amazon Machine Image (AMI) verwenden, das die erforderliche Softwarekonfiguration enthält. Sie können auch Benutzerdaten verwenden, um beim Startup Befehle auszuführen.

- Daten auf Instance-Speicher-Volumes gehen verloren, wenn die Instance angehalten oder beendet wird. Sichern Sie alle wichtigen Daten auf Instance-Speicher-Volumes auf einem persistenteren Speicher wie Amazon S3, Amazon EBS oder Amazon DynamoDB.
- Speichern Sie wichtige Daten regelmäßig an einem Ort, der vom Beenden der Spot-Instance nicht betroffen ist. Sie können beispielsweise Amazon S3, Amazon EBS oder DynamoDB verwenden.
- Teilen Sie die Arbeit in kleine Aufgaben auf (mit einer Grid-, Hadoop- oder warteschlangenbasierten Architektur) oder verwenden Sie Prüfpunkte, damit Sie Ihre Arbeit häufig speichern können.
- Amazon EC2 sendet ein Empfehlungssignal zur Neuverteilung an die Spot-Instance, wenn für die Instance ein erhöhtes Risiko einer Unterbrechung besteht. Sie können sich auf die Neuausgleichsempfehlung verlassen, um Spot-Instance-Unterbrechungen proaktiv zu verwalten, ohne auf die zweiminütige Spot-Instance-Unterbrechungsbenachrichtigung warten zu müssen. Weitere Informationen finden Sie unter EC2 Empfehlungen zur Neugewichtung von Instanzen.
- Verwenden Sie die zweiminütigen Spot-Instance-Unterbrechungsbenachrichtigungen, um den Status Ihrer Spot Instances zu überwachen. Weitere Informationen finden Sie unter Spot-Instance-Unterbrechungsbenachrichtigungen.
- Obwohl wir bemüht sind, diese Warnmeldungen so schnell wie möglich bereitzustellen, besteht die Möglichkeit, dass Ihre Spot-Instance unterbrochen ist, bevor die Warnmeldungen bereitgestellt werden können. Testen Sie Ihre Anwendung und stellen Sie sicher, dass unerwartete Unterbrechungen von Instances elegant abgewickelt werden, auch wenn Sie die Neuausgleichsempfehlungsignale und Benachrichtigungen über Unterbrechungen durchführen überwachen. Führen Sie hierzu die Anwendung mithilfe einer On-Demand-Instance aus und beenden Sie die On-Demand-Instance anschließend selbst.
- Führen Sie ein kontrolliertes Fault-Injection-Experiment mit durch AWS Fault Injection Service , um zu testen, wie Ihre Anwendung reagiert, wenn Ihre Spot-Instance unterbrochen wird. Weitere Informationen finden Sie im Tutorial: Testen von Spot-Instance-Unterbrechungen mit AWS FIS im AWS Fault Injection Service -Benutzerhandbuch.

Initiieren einer Spot-Instance-Unterbrechung

Sie können in der EC2 Amazon-Konsole eine Spot-Instance-Anfrage oder eine Spot-Flotte-Anfrage auswählen und eine Spot-Instance-Unterbrechung einleiten, sodass Sie testen können, wie die Anwendungen auf Ihren Spot-Instances mit Unterbrechungen umgehen. Wenn Sie eine Spot-Instance-Unterbrechung einleiten, EC2 benachrichtigt Sie Amazon, dass Ihre Spot-Instance in zwei Minuten unterbrochen wird, und dann, nach zwei Minuten, wird die Instance unterbrochen.

Der zugrunde liegende Service, der die Spot-Instance-Unterbrechung durchführt, ist AWS Fault Injection Service (AWS FIS). Informationen zu finden AWS FIS Sie unter AWS Fault Injection Service.

> **Note**
>
> Verhaltensweisen bei Unterbrechungen sind `terminate`, `stop` und `hibernate`. Wenn Sie das Unterbrechungsverhalten auf `hibernate` einstellen, erfolgt bei Initiierung einer Spot-Instance-Unterbrechung umgehend der Übergang in den Ruhezustand.

Das Initiieren einer Spot-Instance-Unterbrechung wird in allen Ländern AWS-Regionen außer im asiatisch-pazifischen Raum (Jakarta), im asiatisch-pazifischen Raum (Osaka), in China (Peking), in China (Ningxia) und im Nahen Osten (VAE) unterstützt.

Inhalt

- Initiieren einer Spot-Instance-Unterbrechung
- Überprüfen der Spot-Instance-Unterbrechung
- Kontingente

Initiieren einer Spot-Instance-Unterbrechung

Sie können die EC2 Konsole verwenden, um schnell eine Spot-Instance-Unterbrechung einzuleiten. Wenn Sie eine Spot-Instance-Anfrage auswählen, können Sie die Unterbrechung einer Spot-Instance einleiten. Wenn Sie eine Spot-Flotte-Anfrage auswählen, können Sie die Unterbrechung mehrerer Spot-Instances gleichzeitig einleiten.

Für komplexere Experimente zum Testen von Spot-Instance-Unterbrechungen können Sie mit der AWS FIS Konsole Ihre eigenen Experimente erstellen.

Um die Unterbrechung einer Spot-Instance in einer Spot-Instance-Anfrage über die EC2 Konsole zu initiieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests (Spot-Anforderungen) aus.
3. Wählen Sie eine Spot-Instance-Anforderung und dann Actions (Aktionen) sowie Initiate interruption (Unterbrechung beginnen) aus. Sie können nicht mehrere Spot-Instance-Anfragen auswählen, um eine Unterbrechung einzuleiten.

4. Verwenden Sie im Dialogfeld Initiate Spot Instance interruption (Spot-Instance-Unterbrechung initiieren) unter Service access (Service-Zugriff) entweder die Standardrolle oder wählen Sie eine vorhandene Rolle aus. Um eine Rolle auszuwählen, klicken Sie auf Use an existing service role (Vorhandene Servicerolle verwenden). Wählen Sie dann unter IAM role (IAM-Rolle) die zu verwendende Rolle aus.
5. Wenn Sie bereit sind, die Spot-Instance-Unterbrechung zu initiieren, wählen Sie Initiate interruption (Unterbrechung initiieren) aus.

Um die Unterbrechung einer oder mehrerer Spot-Instances in einer Spot-Flottenanfrage über die EC2 Konsole einzuleiten

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests (Spot-Anforderungen) aus.
3. Wählen Sie eine Spot-Flotten-Anforderung und dann Actions (Aktionen) sowie Initiate interruption (Unterbrechung beginnen) aus. Sie können nicht mehrere Spot-Flotten-Anfragen auswählen, um eine Unterbrechung einzuleiten.
4. Geben Sie im Dialogfeld „Anzahl der Spot-Instances angeben“ unter Anzahl der zu unterbrechenden Instances die Anzahl der zu unterbrechenden Spot-Instances ein und wählen Sie dann „Bestätigen“.

> **Note**
>
> Die Anzahl darf die Anzahl der Spot-Instances in der Flotte oder Ihr Kontingent für die Anzahl der Spot-Instances, die pro Experiment unterbrochen AWS FIS werden können, nicht überschreiten.

5. Verwenden Sie im Dialogfeld Initiate Spot Instance interruption (Spot-Instance-Unterbrechung initiieren) unter Service access (Service-Zugriff) entweder die Standardrolle oder wählen Sie eine vorhandene Rolle aus. Um eine Rolle auszuwählen, klicken Sie auf Use an existing service role (Vorhandene Servicerolle verwenden). Wählen Sie dann unter IAM role (IAM-Rolle) die zu verwendende Rolle aus.
6. Wenn Sie bereit sind, die Spot-Instance-Unterbrechung zu initiieren, wählen Sie Initiate interruption (Unterbrechung initiieren) aus.

So erstellen Sie weitergehende Experimente zum Testen von Spot-Instance-Unterbrechungen über die AWS FIS -Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests (Spot-Anforderungen) aus.
3. Wählen Sie Actions (Aktionen) und dann Create advanced experiments (Erweiterte Experimente erstellen) aus.

   Die AWS FIS Konsole wird geöffnet. Weitere Informationen finden Sie unter Tutorial: Testen von Spot-Instance-Unterbrechungen mit AWS FIS im Benutzerhandbuch von AWS Fault Injection Service .

Überprüfen der Spot-Instance-Unterbrechung

Nach Initiierung der Unterbrechung geschieht Folgendes:

- Für die Spot Instance wird eine Empfehlung zum Neuausgleich der Instance ausgesprochen.
- Zwei Minuten vor der Unterbrechung Ihrer Instance wird eine Benachrichtigung zur AWS FIS Unterbrechung der Spot-Instance ausgegeben.
- Nach zwei Minuten wird die Spot Instance unterbrochen.
- Eine Spot-Instance, die gestoppt wurde, AWS FIS bleibt gestoppt, bis Sie sie neu starten.

So überprüfen Sie, ob die Instance nach Initiierung der Unterbrechung unterbrochen wurde

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Öffnen Sie im Navigationsbereich Spot Requests (Spot-Anforderungen) und Instances in separaten Browser-Registerkarten oder -Fenstern.
3. Wählen Sie für Spot-Anfragen die Spot-Instance-Anfrage oder die Spot-Flotten-Anfrage aus. Der ursprüngliche Status ist `fulfilled`. Nach Unterbrechung der Instance ändert sich der Status je nach Unterbrechungsverhalten wie folgt:
   - `terminate` – Der Status ändert sich zu `instance-terminated-by-experiment`.
   - `stop` – Der Status ändert sich zu `marked-for-stop-by-experiment` und dann zu `instance-stopped-by-experiment`.
4. Wählen Sie unter Instances die Spot Instance aus. Der ursprüngliche Status ist `Running`. Zwei Minuten nach Erhalt der Benachrichtigung über eine Spot-Instance-Unterbrechung ändert sich der Status je nach Unterbrechungsverhalten wie folgt:

- `stop` – Der Status ändert sich zu `Stopping` und dann zu `Stopped`.
- `terminate` – Der Status ändert sich zu `Shutting-down` und dann zu `Terminated`.

Kontingente

Ihre AWS-Konto hat das folgende Standardkontingent für die Anzahl der Spot-Instances, die pro Experiment unterbrochen AWS FIS werden können.

Name	Standard	Anpassbar	Description
Ziel SpotInstances für aws:ec2: send-spot-instance-interruptions	Jede unterstützte Region: 5	Yes (Ja)	Die maximale Anzahl von Spot-Instances, auf die aws:ec2: abzielen send-spot -instance-interrup tions kann, wenn Sie Ziele mithilfe von Tags identifizieren, pro Experiment.

Sie können eine Kontingenterhöhung beantragen. Weitere Informationen finden Sie unter Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Um alle Kontingente für anzuzeigen AWS FIS, öffnen Sie die Konsole Service Quotas. Wählen Sie im Navigationsbereich AWS -Services und dann AWS Fault Injection Service aus. Sie können sich auch alle Kontingente für AWS Fault Injection Service im AWS Fault Injection Service Benutzerhandbuch ansehen.

Spot-Instance-Unterbrechungsbenachrichtigungen

Eine Benachrichtigung zur Unterbrechung der Spot-Instance ist eine Warnung, die zwei Minuten vor dem EC2 Stopp oder der Kündigung Ihrer Spot-Instance durch Amazon ausgegeben wird. Wenn Sie den Ruhezustand als Verhalten bei Unterbrechungen festlegen, erhalten Sie eine Benachrichtigung über die Unterbrechung. Sie erhalten jedoch eine zweiminütige Warnung, da sofort in den Ruhezustand übergegangen wird.

Der beste Weg, um Spot-Instance-Unterbrechungen ordnungsgemäß zu handhaben, besteht darin, Ihre Anwendung so zu konzipieren, dass sie eine Fehlertoleranz aufweist. Um dies zu erreichen, können Sie die Vorteile von Benachrichtigungen über die Unterbrechung der Spot-Instance nutzen. Wir empfehlen, alle 5 Sekunden zu prüfen, ob derartige Benachrichtigungen über die Unterbrechung vorliegen.

Die Unterbrechungsbenachrichtigungen werden als EventBridge Ereignis und als Elemente in den Instance-Metadaten auf der Spot-Instance verfügbar gemacht. Unterbrechungsmitteilungen werden nach bestem Bemühen ausgegeben.

EC2 Spot Instance Interruption Warning event

Wenn Amazon EC2 Ihre Spot-Instance unterbricht, gibt es zwei Minuten vor der eigentlichen Unterbrechung ein Ereignis aus (mit Ausnahme des Ruhezustands, bei dem die Unterbrechungsbenachrichtigung angezeigt wird, aber nicht zwei Minuten im Voraus, da der Ruhezustand sofort beginnt). Dieses Ereignis kann von Amazon erkannt werden EventBridge. Weitere Informationen zu EventBridge Veranstaltungen finden Sie im EventBridge Amazon-Benutzerhandbuch. Ein ausführliches Beispiel, das Sie Schritt für Schritt durch die Erstellung und Verwendung von Ereignisregeln führt, finden Sie unter Die Vorteile von Amazon EC2 Spot-Instance Interruption Notices nutzen.

Das folgende Beispiel zeigt ein Ereignis für eine Spot-Instance-Unterbrechung. Die möglichen Werte für `instance-action` sind `hibernate`, `stop` und `terminate`.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Spot Instance Interruption Warning",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2a:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0",
        "instance-action": "action"
    }
}
```

> **Note**
>
> Das ARN-Format des Spot-Instance-Unterbrechungsereignisses ist `arn:aws:ec2:`*`availability-zone`*`:instance/`*`instance-id`*. Dieses Format unterscheidet sich vom ARN-Format der EC2 Ressource.

instance-action

Das Element `instance-action` gibt die Aktion sowie den ungefähren Zeitpunkt in UTC an, an dem die Aktion ausgeführt wird.

Wenn Ihre Spot-Instance von Amazon als gestoppt oder beendet gekennzeichnet ist EC2, ist das `instance-action` Element in Ihren Instance-Metadaten enthalten. Andernfalls ist es nicht vorhanden. Sie können die Version 2 (IMDSv2) des `instance-action` Using Instance Metadata Service wie folgt abrufen.

Linux

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/spot/instance-action
```

Windows

```
[string]$token = Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/instance-action
```

Die folgende Beispielausgabe zeigt den Zeitpunkt an, an dem diese Instance angehalten wird.

```
{"action": "stop", "time": "2017-09-18T08:22:00Z"}
```

Die folgende Beispielausgabe zeigt den Zeitpunkt an, an dem diese Instance beendet wird.

```
{"action": "terminate", "time": "2017-09-18T08:22:00Z"}
```

Wenn Amazon EC2 sich nicht darauf vorbereitet, die Instance zu stoppen oder zu beenden, oder wenn Sie die Instance selbst beendet haben, `instance-action` ist dies nicht in den Instance-Metadaten enthalten und Sie erhalten einen HTTP 404-Fehler, wenn Sie versuchen, sie abzurufen.

termination-time

Das Element `termination-time` gibt den ungefähren Zeitpunkt in UTC an, an dem die Instance das Signal für das Herunterfahren empfängt.

> **Note**
>
> Dieses Element wird nur beibehalten, um die Abwärtskompatibilität zu gewährleisten. Sie sollten stattdessen `instance-action` verwenden.

Wenn Ihre Spot-Instance von Amazon zur Kündigung markiert ist EC2 (entweder aufgrund einer Spot-Instance-Unterbrechung, auf die das Unterbrechungsverhalten eingestellt ist`terminate`, oder aufgrund der Stornierung einer persistenten Spot-Instance-Anfrage), ist das `termination-time` Element in Ihren Instance-Metadaten vorhanden. Andernfalls ist es nicht vorhanden. Sie können die `termination-time` Verwendung IMDSv2 wie folgt abrufen.

Linux

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`
if curl -H "X-aws-ec2-metadata-token: $TOKEN" -s http://169.254.169.254/latest/meta-data/spot/termination-time | grep -q .*T.*Z; then echo termination_scheduled; fi
```

Windows

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/termination-time
```

Es folgt eine Beispielausgabe.

```
2015-01-05T18:02:00Z
```

Wenn Amazon EC2 sich nicht darauf vorbereitet, die Instance zu beenden (entweder weil es keine Spot-Instance-Unterbrechung gibt oder weil Ihr Unterbrechungsverhalten auf `stop` oder eingestellt ist`hibernate`), oder wenn Sie die Spot-Instance selbst beendet haben, ist das `termination-time` Element entweder nicht in den Instance-Metadaten vorhanden (Sie erhalten also einen HTTP 404-Fehler) oder enthält einen Wert, der kein Zeitwert ist.

Wenn Amazon die Instance EC2 nicht beenden kann, wird der Anforderungsstatus auf gesetzt`fulfilled`. Beachten Sie, dass der `termination-time`-Wert mit der ursprünglichen ungefähren Zeit, die jetzt in der Vergangenheit liegt, in den Instance-Metadaten verbleibt.

Finden von unterbrochenen Spot-Instances

Wenn Sie Ihre EC2 Instances beschreiben, schließen die Ergebnisse Ihre Spot-Instances mit ein. Der Instance-Lebenszyklus einer Spot Instance ist `spot`. Der Instance-Status einer Spot Instance ist entweder `stopped` oder `terminated`, abhängig vom von Ihnen konfigurierten Unterbrechungsverhalten. Bei einer Spot-Instance im Ruhezustand lautet der Instance-Status `stopped`.

Weitere Informationen zum Grund der Unterbrechung finden Sie im Statuscode für Spot-Anfragen. Weitere Informationen finden Sie unter the section called “Den Status einer Spot-Instance-Anfrage abrufen”.

Console

So suchen Sie eine unterbrochene Spot Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wenden Sie den folgenden Filter an: Instance-Lebenszyklus=Spot.
4. Wenden Sie je nach dem von Ihnen konfigurierten Unterbrechungsverhalten den Filter Instance-Status=angehalten oder Instance-Status=beendet an.
5. Suchen Sie für jede Spot Instance auf der Registerkarte Details unter Instance-Details nach der Meldung zum Statusübergang. Die folgenden Codes geben an, dass die Spot Instance unterbrochen wurde.

   - `Server.SpotInstanceShutdown`
   - `Server.SpotInstanceTermination`

AWS CLI

So suchen Sie unterbrochene Spot Instances

Verwenden Sie den Befehl describe-instances mit der Option `--filters`. Um nur die Instance IDs in der Ausgabe aufzulisten, fügen Sie die `--query` Option hinzu.

Wenn das Unterbrechungsverhalten darin besteht, die Spot Instances zu beenden, verwenden Sie das folgende Beispiel:

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot \
              Name=instance-state-name,Values=terminated \
              Name=state-reason-code,Values=Server.SpotInstanceTermination \
    --query "Reservations[*].Instances[*].InstanceId"
```

Wenn das Unterbrechungsverhalten darin besteht, die Spot Instances anzuhalten, verwenden Sie das folgende Beispiel:

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot \
              Name=instance-state-name,Values=stopped \
              Name=state-reason-code,Values=Server.SpotInstanceShutdown \
    --query "Reservations[*].Instances[*].InstanceId"
```

PowerShell

So suchen Sie unterbrochene Spot Instances

Verwenden Sie das cmdlet Get-EC2Instance.

Wenn das Unterbrechungsverhalten darin besteht, die Spot Instances zu beenden, verwenden Sie das folgende Beispiel:

```
(Get-EC2Instance `
    -Filter @{Key="instance-lifecycle"; Values="spot"} `
            @{Key="instance-state-name"; Values="terminated"} `
            @{Key="state-reason-code";
 Values="Server.SpotInstanceTermination"}).Instances.InstanceId
```

Wenn das Unterbrechungsverhalten darin besteht, die Spot Instances anzuhalten, verwenden Sie das folgende Beispiel:

```
(Get-EC2Instance `
    -Filter @{Key="instance-lifecycle"; Values="spot"} `
            @{Key="instance-state-name"; Values="stopped"} `
            @{Key="state-reason-code";
 Values="Server.SpotInstanceTermination"}).Instances.InstanceId
```

Ermitteln Sie, ob Amazon eine Spot-Instance EC2 beendet hat

Eine Spot-Instance läuft, bis Amazon sie als Reaktion auf eine Spot-Instance-Unterbrechung EC2 beendet oder bis Sie sie selbst beenden. Weitere Informationen finden Sie unter the section called “Verhalten bei Unterbrechungen”.

Nachdem eine Spot-Instance beendet wurde, können Sie AWS CloudTrail damit sehen, ob Amazon sie EC2 beendet hat. Wenn das CloudTrail Protokoll eine enthält, bedeutet dies`BidEvictedEvent`, dass Amazon die Spot-Instance EC2 beendet hat. Wenn Sie stattdessen ein `TerminateInstances`-Ereignis sehen, bedeutet dies, dass ein Benutzer die Spot Instance beendet hat.

Wenn Sie eine Benachrichtigung darüber erhalten möchten, dass Amazon Ihre Spot-Instance unterbrechen EC2 wird, können Sie alternativ Amazon verwenden, EventBridge um auf das Ereignis EC2 Spot-Instance-Unterbrechungswarnung zu reagieren.

Um BidEvictedEvent Ereignisse anzuzeigen in CloudTrail

1. Öffnen Sie die CloudTrail Konsole unter https://console.aws.amazon.com/cloudtrail/.
2. Wählen Sie im Navigationsbereich Ereignisverlauf aus.
3. Wählen Sie in der Liste Ereignisname und geben Sie dann in das Filterfeld rechts **`BidEvictedEvent`** ein.
4. (Optional) Wählen Sie einen Zeitraum aus.
5. Wenn die Liste nicht leer ist, wählen Sie BidEvictedEventaus dem resultierenden Eintrag, um die zugehörige Detailseite zu öffnen. Im Ereignisaufzeichnungsbereich finden Sie Informationen über die Spot Instance, einschließlich der ID der Spot Instance. Es folgt ein Beispiel für diese Ereignisaufzeichnung.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
```

```
        "invokedBy": "ec2.amazonaws.com"
    },
    "eventTime": "2016-08-16T22:30:00Z",
    "eventSource": "ec2.amazonaws.com",
    "userAgent": "ec2.amazonaws.com",
    "sourceIPAddress": "ec2.amazonaws.com",
    "eventName": "BidEvictedEvent",
    "awsRegion": "us-east-2",
    "eventID": "d27a6096-807b-4bd0-8c20-a33a83375054",
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123456789012",
    "RequestParameters": null,
    "ResponseElements": null,
    "serviceEventDetails": {
        "instanceIdSet": [
          "i-1eb2ac8eEXAMPLE"
        ]
    }
}
```

6. Wenn Sie keinen Eintrag für das `BidEvictedEvent`-Ereignis gefunden haben, geben Sie **`TerminateInstances`** als Namen für das Ereignis ein. Weitere Informationen zur Ereignisaufzeichnung für `TerminateInstances` finden Sie unter the section called “Amazon-EC2-API-Ereignisbeispiele”.

Fakturierung für unterbrochene Spot-Instances

Wenn eine Spot Instance unterbrochen wird, werden Ihnen die Kosten für die Nutzung der Instance und des EBS-Volumes in Rechnung gestellt und es können weitere Gebühren anfallen.

Instance-Nutzung

Wer die Spot-Instance unterbricht	Betriebssystem	Unterbrochen in der ersten Stunde	Unterbrochen in jeder beliebigen Stunde nach der ersten Stunde
Wenn Sie die Spot-Instance anhalten oder beenden	Windows und Linux (ausgenommen SUSE)	Berechnung der genutzten Sekunden	Berechnung der genutzten Sekunden

Wer die Spot-Instance unterbricht	Betriebssystem	Unterbrochen in der ersten Stunde	Unterbrochen in jeder beliebigen Stunde nach der ersten Stunde
Wenn Amazon die EC2 Spot-Instance unterbricht	SUSE	Berechnung der vollen Stunde, selbst wenn Sie sie nicht ganz genutzt haben	Berechnung der vollen genutzten Stunden; Berechnung einer ganzen Stunde für die unterbrochene Teilstunde
	Windows und Linux (ausgenommen SUSE)	Keine Gebühren	Berechnung der genutzten Sekunden
	SUSE	Keine Gebühren	Berechnung der vollen genutzten Stunden, keine Berechnung für die unterbrochene Teilstunde

EBS-Volume-Nutzung

Während eine unterbrochene Spot-Instance angehalten wird, werden nur Gebühren für die EBS-Volumes berechnet, die beibehalten werden.

Mit EC2 Fleet und Spot Fleet können Sie, wenn Sie über viele gestoppte Instances verfügen, das Limit für die Anzahl der EBS-Volumes für Ihr Konto überschreiten.

EC2 Empfehlungen zur Neugewichtung von Instanzen

Eine Empfehlung zur Neuverteilung von EC2 Instances ist ein Signal, das Sie benachrichtigt, wenn bei einer Spot-Instance ein erhöhtes Risiko einer Unterbrechung besteht. Das Signal kann früher als die zweiminütige Unterbrechungsbenachrichtigung der Spot-Instance eintreffen, sodass Sie die Möglichkeit haben, die Spot-Instance proaktiv zu verwalten. Sie können entscheiden, Ihr Workload

auf neue oder bestehende Spot Instances auszugleichen, die nicht einem erhöhten Risiko einer Unterbrechung ausgesetzt sind.

Es ist Amazon EC2 nicht immer möglich, das Signal zur Neugewichtsempfehlung vor der zweiminütigen Benachrichtigung über die Unterbrechung der Spot-Instance zu senden. Daher kann das Neuausgleichsempfehlungsignal zusammen mit der zweiminütigen Unterbrechungsbenachrichtigung eingehen.

Empfehlungen zur Neuverteilung werden als EventBridge Ereignis und als Element in den Instance-Metadaten auf der Spot-Instance zur Verfügung gestellt. Ereignisse werden auf bestmögliche Weise ausgegeben.

> **Note**
>
> Neuausgleichsempfehlungen werden nur für Spot-Instances unterstützt, die nach dem 5. November 2020 00:00 UTC gestartet werden.

Inhalt

- Ausgleich von Aktionen, die Sie ergreifen können
- Überwachen von Signalen für Neuausgleichsempfehlungen
- Dienste, die das Neuausgleichsempfehlungssignal verwenden

Ausgleich von Aktionen, die Sie ergreifen können

Dies sind einige der möglichen Neuausgleichsaktionen, die Sie ergreifen können:

Korrektes Herunterfahren

Wenn Sie das Neuausgleichsempfehlungsignal für eine Spot-Instance erhalten, können Sie Ihre Instance-Abschaltverfahren starten, wozu auch gehören kann, sicherzustellen, dass Prozesse abgeschlossen sind, bevor Sie sie anhalten. Sie können beispielsweise System- oder Anwendungsprotokolle auf Amazon Simple Storage Service (Amazon S3) hochladen, Amazon-SQS-Mitarbeiter herunterfahren oder die Abmeldung vom Domain Name System (DNS) durchführen. Sie können Ihre Arbeit auch im externen Speicher speichern und zu einem späteren Zeitpunkt wieder aufnehmen.

Verhindern, dass neue Arbeit geplant wird

Wenn Sie das Neuausgleichsempfehlungsignal für eine Spot-Instance erhalten, können Sie verhindern, dass neue Arbeiten auf der Instance geplant werden, während Sie die Instance weiterhin verwenden, bis die geplante Arbeit abgeschlossen ist.

Proaktiv neue Ersatz-Instances starten

Sie können Amazon EC2 Auto Scaling Scaling-Gruppen, EC2 Fleet oder Spot Fleet so konfigurieren, dass automatisch Ersatz-Spot-Instances gestartet werden, wenn ein Empfehlungssignal für die Neuverteilung ausgegeben wird. Weitere Informationen finden Sie unter Verwenden von Capacity Rebalancing zur Behandlung von Amazon EC2 Spot-Unterbrechungen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch und Den Kapazitätsausgleich in der EC2-Flotte und der Spot-Flotte verwenden, um gefährdete Spot Instances zu ersetzen in diesem Benutzerhandbuch.

Überwachen von Signalen für Neuausgleichsempfehlungen

Sie können das Signal für die Neuausgleichsempfehlung überwachen, damit Sie bei der Absendung des Signals die im vorherigen Abschnitt angegebenen Aktionen ausführen können. Das Rebalance-Empfehlungssignal wird als Ereignis, das an Amazon gesendet wird EventBridge (früher bekannt als Amazon CloudWatch Events), und als Instance-Metadaten auf der Spot-Instance zur Verfügung gestellt.

Überwachen von Signalen für Neuausgleichsempfehlungen:

- Verwenden Sie Amazon EventBridge
- Verwenden von Instance-Metadaten

Verwenden Sie Amazon EventBridge

Wenn das Rebalance-Empfehlungssignal für eine Spot-Instance ausgegeben wird, wird das Ereignis für das Signal an Amazon EventBridge gesendet. Wenn ein Ereignismuster EventBridge erkannt wird, das einem in einer Regel definierten Muster entspricht, EventBridge ruft es ein oder mehrere in der Regel angegebene Ziel (oder Ziele) auf.

Es folgt ein Beispielereignis für das Neuausgleichsempfehlungssignal.

```
{
    "version": "0",
```

```
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Instance Rebalance Recommendation",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0"
    }
}
```

Die folgenden Felder bilden das in der Regel definierte Ereignismuster:

`"detail-type": "EC2 Instance Rebalance Recommendation"`

Gibt an, dass das Ereignis ein Neuausgleichsempfehlungsereignis ist

`"source": "aws.ec2"`

Identifiziert, dass das Ereignis von Amazon stammt EC2

Erstellen Sie eine EventBridge Regel

Sie können eine EventBridge Regel schreiben und automatisieren, welche Aktionen ausgeführt werden, wenn das Ereignismuster mit der Regel übereinstimmt.

Im folgenden Beispiel wird eine EventBridge Regel erstellt, mit der jedes Mal, wenn Amazon ein Empfehlungssignal zur Neugewichtung EC2 ausgibt, eine E-Mail, eine Textnachricht oder eine mobile Push-Benachrichtigung gesendet wird. Das Signal wird als `EC2 Instance Rebalance Recommendation`-Ereignis ausgegeben, das die durch die Regel definierte Aktion auslöst.

Bevor Sie die EventBridge Regel erstellen, müssen Sie das Amazon SNS SNS-Thema für die E-Mail, Textnachricht oder mobile Push-Benachrichtigung erstellen.

Um eine EventBridge Regel für ein Remalance-Empfehlungsereignis zu erstellen

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie Regel erstellen aus.
3. Zum Define rule detail (Festlegen der Regeldetails) gehen Sie folgendermaßen vor:

    a. Geben Sie für die Regel einen Name (Namen) und optional eine Beschreibung ein.

Eine Regel darf nicht denselben Namen wie eine andere Regel in derselben Region und auf demselben Event Bus haben.

b. Bei Event bus (Ereignisbus) wählen Sie default (Standard) aus. Wenn ein AWS -Service in Ihrem Konto ein Ereignis ausgibt, wird dieses stets an den standardmäßigen Event Bus Ihres Kontos weitergeleitet.

c. Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.

d. Wählen Sie Weiter aus.

4. Bei Build event pattern (Ereignis-Muster erstellen) gehen Sie wie folgt vor:

a. Wählen Sie als Eventquelle AWS Events oder EventBridge Partnerevents aus.

b. Bei Event pattern (Ereignismuster) in diesem Beispiel geben Sie das folgende Ereignismuster an, um mit dem `EC2 Instance Rebalance Recommendation`-Ereignis übereinzustimmen, und wählen dann Save (Speichern) aus.

```
{
 "source": ["aws.ec2"],
 "detail-type": ["EC2 Instance Rebalance Recommendation"]
}
```

Um das Ereignismuster hinzuzufügen, können Sie entweder eine Vorlage verwenden, indem Sie Event pattern form (Ereignismusterformular) auswählen oder Sie spezifizieren Ihr eigenes Muster, indem Sie Custom pattern (JSON-Editor) (Benutzerdefiniertes Muster (JSON-Editor)) auswählen, siehe nachfolgend:

i. Gehen Sie wie folgt vor, um eine Vorlage zum Erstellen des Ereignismusters zu erstellen:

A. Wählen Sie Event pattern form (Ereignismusterformular) aus.

B. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.

C. Wählen Sie AWS unter Service die Option EC2 Spot Fleet aus.

D. Wählen Sie als Ereignistyp die Option EC2 Instance Rebalance Recommendation aus.

E. Um die Vorlage anzupassen, wählen Sie Edit pattern (Muster bearbeiten) und nehmen Sie Ihre Änderungen vor, damit sie dem Beispiel-Ereignismuster entsprechen.

ii. (Alternativ) So geben Sie ein benutzerdefiniertes Ereignismuster an:

A. Wählen Sie Custom pattern (JSON editor) (Benutzerdefiniertes Muster (JSON-Editor)) aus.

B. In dem Feld Event pattern (Ereignismuster) fügen Sie das Ereignismuster für dieses Beispiel hinzu.

c. Wählen Sie Weiter aus.

5. Bei Select target(s) (Ziel(e) auswählen) gehen Sie wie folgt vor:

a. Bei Target types (Zieltypen) wählen Sie AWS -Service aus.

b. Bei Select a target (Ziel auswählen) wählen Sie SNS topic (SNS-Thema) aus, um eine E-Mail, eine SMS oder eine mobile Push-Benachrichtigung zu senden, wenn das Ereignis eintritt.

c. Wählen Sie für Topic (Thema) ein vorhandenes Thema aus. Sie müssen zuerst mit der Amazon-SNS-Konsole ein Amazon-SNS-Thema erstellen. Weitere Informationen finden Sie unter Verwenden von Amazon SNS für application-to-person (A2P) -Messaging im Amazon Simple Notification Service Developer Guide.

d. (Optional) Unter Additional settings (Zusätzliche Einstellungen) können Sie optional zusätzliche Einstellungen konfigurieren. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch unter EventBridge Amazon-Regeln erstellen, die auf Ereignisse reagieren (Schritt 16).

e. Wählen Sie Weiter aus.

6. (Optional) Bei Tags können Sie Ihrer Regel optional einen Tag oder mehrere Tags hinzufügen und dann Next (Weiter) auswählen.

7. Bei Review and create (Überprüfen und erstellen) gehen Sie wie folgt vor:

a. Überprüfen Sie die Details der Regel und ändern Sie sie nach Bedarf.

b. Wählen Sie Regel erstellen aus.

Weitere Informationen finden Sie unter EventBridge Amazon-Regeln und EventBridge Amazon-Ereignismuster im EventBridge Amazon-Benutzerhandbuch

Verwenden von Instance-Metadaten

Die Kategorie der Instance-Metadaten `events/recommendations/rebalance` gibt die ungefähre Zeit in UTC an, zu der das Neuausgleichsempfehlungssignal für eine Spot-Instance ausgegeben wurde.

Wir empfehlen Ihnen, alle 5 Sekunden nach Neuausgleichsempfehlungssignalen zu suchen, damit Sie keine Gelegenheit verpassen, auf den Neuausgleich zu reagieren.

Wenn die Spot-Instance eine Neuausgleichsempfehlung erhält, ist der Zeitpunkt, zu dem das Signal ausgegeben wurde, in den Instance-Metadaten vorhanden. Sie können die Zeit, zu der das Signal gesendet wurde, wie folgt abrufen.

IMDSv2

Linux

Führen Sie den folgenden Befehl in Ihrer Linux-Instance aus.

IMDSv2

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/events/recommendations/rebalance
```

Windows

Führen Sie das folgende cmdlet von Ihrer Windows-Instance aus.

```
[string]$token = Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/events/recommendations/
rebalance
```

IMDSv1

Linux

Führen Sie den folgenden Befehl in Ihrer Linux-Instance aus.

```
curl http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

Windows

Führen Sie das folgende cmdlet in Ihrer Windows-Instance aus.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/events/
recommendations/rebalance
```

Im Folgenden finden Sie eine Beispielausgabe, die die Zeit in UTC angibt, zu der das Neuausgleichsempfehlungssignal für die Spot-Instance ausgegeben wurde.

```
{"noticeTime": "2020-10-27T08:22:00Z"}
```

Wenn das Signal für die Instance nicht ausgegeben wurde, ist `events/recommendations/rebalance` nicht vorhanden und Sie erhalten einen HTTP-404-Fehler, wenn Sie versuchen, sie abzurufen.

Dienste, die das Neuausgleichsempfehlungssignal verwenden

Amazon EC2 Auto Scaling, EC2 Fleet und Spot Fleet verwenden das Empfehlungssignal für die Neuverteilung, um Ihnen die Aufrechterhaltung der Workload-Verfügbarkeit zu erleichtern, indem Sie Ihre Flotte proaktiv um eine neue Spot-Instance erweitern, bevor eine laufende Instance die zweiminütige Spot-Instance-Unterbrechungsbenachrichtigung erhält. Sie können diese Dienste Änderungen überwachen lassen und proaktiv auf Änderungen reagieren lassen, die sich auf die Verfügbarkeit Ihrer Spot-Instances auswirken. Weitere Informationen finden Sie hier:

- Verwenden Sie Capacity Rebalancing zur Behandlung von Amazon EC2 Spot-Unterbrechungen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch
- Den Kapazitätsausgleich in der EC2-Flotte und der Spot-Flotte verwenden, um gefährdete Spot Instances zu ersetzenim Thema EC2 Fleet and Spot Fleet in diesem Benutzerhandbuch

Spot-Platzierungsbewertung

Die Funktion „Spot-Platzierungsbewertung“ kann eine AWS Region oder Availability Zone auf der Grundlage Ihrer Spot-Kapazitätsanforderungen empfehlen. Die Spot-Kapazität schwankt und Sie

können nicht sicher sein, dass Sie immer die Kapazität erhalten, die Sie benötigen. Eine Spot-Platzierungsbewertung gibt an, wie wahrscheinlich es ist, dass eine Spot-Anforderung in einer Region oder Availability Zone erfolgreich ist.

> **Note**
>
> Eine Spot-Platzierungsbewertung bietet keine Garantien in Bezug auf die verfügbare Kapazität oder das Risiko einer Unterbrechung. Eine Spot-Platzierungsbewertung dient nur als Empfehlung.

Anwendungsfälle

Sie können das Spot-Platzierungsbewertungsfeature für Folgendes verwenden:

- Verlagerung und Skalierung der Spot-Rechenkapazität nach Bedarf in einer anderen Region als Reaktion auf einen erhöhten Kapazitätsbedarf oder eine verringerte verfügbare Kapazität in der aktuellen Region.
- Um die optimale Availability Zone zu identifizieren, in der Single-Availability-Zone-Workloads ausgeführt werden sollen.
- Um zukünftige Spot-Kapazitätsanforderungen zu simulieren, damit Sie eine optimale Region für die Erweiterung Ihrer Spot-basierten Workloads auswählen können.
- Um eine optimale Kombination von Instance-Typen zu finden, Ihre Spot-Kapazitätsanforderungen erfüllen.

Inhalt

- Einschränkungen
- Kosten
- So funktioniert die Spot-Platzierungsbewertung
- Erforderliche Berechtigungen für Spot-Platzierungsbewertung
- Eine Spot-Platzierungsbewertung berechnen

Einschränkungen

- Zielkapazitätslimit – Ihr Zielkapazitätslimit für die Spot-Platzierung basiert auf Ihrer jüngsten Spot-Nutzung und berücksichtigt gleichzeitig ein potenzielles Nutzungswachstum. Wenn Sie in letzter

Zeit keine Spot-Nutzung haben, bieten wir Ihnen ein niedriges Standardlimit, das auf Ihr Spot-Anfragelimit abgestimmt ist.

- Limit für Konfigurationen anfordern – Wir können die Anzahl neuer Anforderungskonfigurationen innerhalb eines Zeitraums von 24 Stunden begrenzen, wenn wir Muster erkennen, die nicht mit der beabsichtigten Verwendung des Spot-Platzierungsbewertungsfeatures verbunden sind. Wenn Sie das Limit erreicht haben, können Sie die bereits verwendeten Anforderungskonfigurationen wiederholen, aber neue Anforderungskonfigurationen lassen sich erst im nächsten Zeitraum von 24 Stunden angeben.
- Mindestanzahl von Instance-Typen — Wenn Sie Instance-Typen angeben, müssen Sie mindestens drei verschiedene Instance-Typen angeben. Andernfalls gibt Amazon EC2 einen niedrigen Spot-Platzierungswert zurück. Wenn Sie Instance-Aattribute angeben, müssen diese auf mindestens drei verschiedene Instance-Typen aufgelöst werden. Instance-Typen gelten als unterschiedlich, wenn sie einen anderen Namen haben. Zum Beispiel gelten m5.8xlarge, m5a.8xlarge und m5.12xlarge als unterschiedlich.

Kosten

Für die Nutzung des Spot-Platzierungsbewertungsfeatures fallen keine zusätzlichen Gebühren an.

So funktioniert die Spot-Platzierungsbewertung

Wenn Sie die Spot-Placement-Score-Funktion verwenden, geben Sie zunächst Ihre Rechenanforderungen für Ihre Spot-Instances an, und dann EC2 gibt Amazon den zehn besten Regionen oder Availability Zones zurück, in denen Ihre Spot-Anfrage wahrscheinlich erfolgreich sein wird. Jede Region oder Availability Zone wird auf einer Skala von 1 bis 10 bewertet. 10 gibt an, dass Ihre Spot-Anforderung sehr wahrscheinlich erfolgreich ist und 1 zeigt an, dass Ihre Spot-Anforderung wahrscheinlich nicht erfolgreich sein wird.

Gehen Sie wie folgt vor, um das Spot-Platzierungsbewertungsfeature zu verwenden:

- Schritt 1: Geben Sie Ihre Spot-Anforderungen an
- Schritt 2: Filtern Sie die Antwort auf die Spot-Platzierungsbewertung
- Schritt 3: Überprüfen Sie die Empfehlungen
- Schritt 4: Nutzen Sie die Empfehlungen

Schritt 1: Geben Sie Ihre Spot-Anforderungen an

Zuerst geben Sie wie folgt Ihre gewünschte Ziel-Spot-Kapazität und die Rechenanforderungen an:

1. Geben Sie die Ziel-Spot-Kapazität und optional die Zielkapazitätseinheit an.

   Sie können Ihre gewünschte Ziel-Spot-Kapazität als Anzahl der Instances oder v CPUs oder als Speichermenge in MiB angeben. Um die Zielkapazität als Anzahl von v CPUs oder als Speichermenge anzugeben, müssen Sie die Zielkapazitätseinheit als `vcpu` oder `memory-mib` angeben. Andernfalls wird standardmäßig die Anzahl der Instances angegeben.

   Wenn Sie Ihre Zielkapazität in Form der Anzahl von v CPUs oder der Speichermenge angeben, können Sie diese Einheiten beim Zählen der Gesamtkapazität verwenden. Wenn Sie beispielsweise eine Mischung aus Instances unterschiedlicher Größe verwenden möchten, können Sie die Zielkapazität als Gesamtzahl von v angebenCPUs. Die Spot-Placement-Score-Funktion berücksichtigt dann jeden Instance-Typ in der Anfrage anhand seiner Anzahl von v CPUs und zählt bei der Summierung der Zielkapazität nicht die Gesamtzahl der Instances, CPUs sondern die Gesamtzahl der Instances.

   Angenommen, Sie geben eine Gesamtzielkapazität von 30 V CPUs an und Ihre Instance-Typenliste besteht aus c5.xlarge (4 vCPUs), m5.2xlarge (8 v) und r5.large (2 vCPUs). CPUs Um insgesamt 30 V zu erreichenCPUs, könnten Sie eine Mischung aus 2 c5.xlarge (2*4 vCPUs), 2 m5.2xlarge (2*8 vCPUs) und 3 r5.large (3*2 vCPUs) erhalten.

2. Geben Sie Instance-Typen oder Instance-Attribute an.

   Sie können entweder die zu verwendenden Instance-Typen oder die Instance-Attribute angeben, die Sie für Ihre Rechenanforderungen benötigen, und Amazon dann die Instance-Typen mit diesen Attributen EC2 identifizieren lassen. Das wird als attributbasierte Instance-Typauswahl bezeichnet.

   Sie können nicht sowohl Instance-Typen als auch Instance-Attribute in derselben Anforderung einer Spot-Platzierungsbewertung angeben.

   Wenn Sie Instance-Typen angeben, müssen Sie mindestens drei verschiedene Instance-Typen angeben, andernfalls gibt Amazon EC2 einen niedrigen Spot-Platzierungswert zurück. Wenn Sie Instance-Aattribute angeben, müssen diese auf mindestens drei verschiedene Instance-Typen aufgelöst werden.

Beispiele für verschiedene Möglichkeiten zur Festlegung Ihrer Spot-Anforderungen finden Sie unter Beispielkonfigurationen.

Schritt 2: Filtern Sie die Antwort auf die Spot-Platzierungsbewertung

Amazon EC2 berechnet den Spot-Platzierungswert für jede Region oder Availability Zone und gibt entweder die Top 10 Regionen oder die Top 10 Availability Zones zurück, in denen Ihre Spot-Anfrage wahrscheinlich erfolgreich sein wird. Standardmäßig wird eine Liste der bewerteten Regionen zurückgegeben. Wenn Sie planen, Ihre gesamte Spot-Kapazität in einer einzigen Availability Zone zu starten, ist es hilfreich, eine Liste der bewerteten Availability Zones anzufordern.

Sie können einen Regionsfilter angeben, um die Regionen einzugrenzen, die in der Antwort zurückgegeben werden.

Sie können den Regionsfilter und eine Anforderung für bewertete Availability Zones kombinieren. Auf diese Weise beschränken sich die bewerteten Availability Zones auf die Regionen, nach denen Sie gefiltert haben. Um die am höchsten bewertete Availability Zone in einer Region zu finden, geben Sie nur diese Region an. Die Antwort gibt eine Liste aller Availability Zones in dieser Region zurück.

Schritt 3: Überprüfen Sie die Empfehlungen

Die Spot-Platzierungsbewertung für jede Region oder Availability Zone wird basierend auf der Zielkapazität, der Zusammensetzung der Instance-Typen, den historischen und aktuellen Spot-Nutzungstrends und dem Zeitpunkt der Anfrage berechnet. Da die Spot-Kapazität ständig schwankt, kann dieselbe Anforderung der Spot-Platzierungsbewertung zu unterschiedlichen Bewertungen führen, wenn sie zu unterschiedlichen Zeiten berechnet wird.

Regionen und Availability Zones werden auf einer Skala von 1 bis 10 bewertet. Eine Punktzahl von 10 zeigt an, dass Ihre Spot-Anforderung sehr wahrscheinlich erfolgreich sein wird – sicher ist das aber nicht. Ein Ergebnis von 1 zeigt an, dass Ihre Spot-Anforderung sehr wahrscheinlich nicht erfolgreich sein wird. Dasselbe Ergebnis kann für verschiedene Regionen oder Availability Zones zurückgegeben werden.

Wenn niedrige Punktzahlen zurückgegeben werden, können Sie Ihre Berechnungsanforderungen bearbeiten und den Punktestand neu berechnen. Sie können auch Empfehlungen für die Spot-Bewertung für die gleichen Berechnungsanforderungen zu verschiedenen Tageszeiten anfordern.

Schritt 4: Nutzen Sie die Empfehlungen

Eine Spot-Platzierungsbewertung ist nur relevant, wenn Ihre Spot-Anforderung genau dieselbe Konfiguration wie die Spot-Platzierungsbewertung hat (Zielkapazität, Zielkapazitätseinheit und Instance-Typen oder Instance-Attribute) und für die Verwendung der `capacity-optimized`-

Zuweisungsstrategie konfiguriert ist. Andernfalls stimmt die Wahrscheinlichkeit, die verfügbare Spot-Kapazität zu erhalten, nicht mit der Bewertung überein.

Während eine Spot-Platzierungsbewertung als Richtlinie dient und nicht garantiert, dass Ihre Spot-Anforderung vollständig oder teilweise erfüllt wird, können Sie die folgenden Informationen verwenden, um die besten Ergebnisse zu erzielen:

- Dieselbe Konfiguration verwenden — Der Spot-Platzierungswert ist nur relevant, wenn die Spot-Anforderungskonfiguration (Zielkapazität, Zielkapazitätseinheit und Instance-Typen oder Instance-Attribute) in Ihrer Amazon EC2 Auto Scaling Scaling-Gruppe, EC2 Flotte oder Spot-Flotte der entspricht, die Sie eingegeben haben, um den Spot-Platzierungswert zu erhalten.

  Wenn Sie in Ihrer Spot-Placement-Score-Anfrage die attributbasierte Instance-Typauswahl verwendet haben, können Sie die attributbasierte Instance-Typauswahl verwenden, um Ihre Amazon EC2 Auto Scaling Scaling-Gruppe, EC2 -Flotte oder Spot-Flotte zu konfigurieren. Weutere Informationen finden Sie unter Erstellen einer gemischten Instances-Gruppe mit attributbasierter Auswahl des Instance-Typs und Geben Sie Attribute für die Auswahl von Instance-Typen für EC2-Flotte oder Spot-Flotte an.

  > **Note**
  >
  > Wenn Sie Ihre Zielkapazität in Form der Anzahl von v CPUs oder der Speichermenge angegeben haben und Sie Instance-Typen in Ihrer Spot-Platzierungs-Score-Konfiguration angegeben haben, beachten Sie, dass Sie diese Konfiguration derzeit nicht in Ihrer Amazon EC2 Auto Scaling Scaling-Gruppe, EC2 Flotte oder Spot-Flotte erstellen können. Stattdessen müssen Sie die Instance-Gewichtung manuell festlegen, indem Sie den `WeightedCapacity`-Parameter verwenden.

- Verwenden der **`capacity-optimized`**-Zuweisungsstrategie – Bei jeder Bewertung wird davon ausgegangen, dass Ihre Flotten-Anforderung so konfiguriert ist, dass alle Availability Zones (für die Anforderung von Kapazität über Regionen hinweg) oder eine einzelne Availability Zone (wenn Sie Kapazität in einer Availability Zone anfordern) und die `capacity-optimized`-Spot-Zuweisungsstrategie für Ihre Anforderung der Spot-Kapazität erfolgreich sind. Wenn Sie andere Zuweisungsstrategien verwenden, z. B. `lowest-price`, stimmt die Wahrscheinlichkeit, dass Spot-Kapazität verfügbar ist, nicht mit der Bewertung überein.
- Handeln Sie sofort bei einer Punktzahl – Die Empfehlung der Spot-Platzierungsbewertung spiegelt die verfügbare Spot-Kapazität zum Zeitpunkt der Anforderung wider und dieselbe Konfiguration kann zu unterschiedlichen Ergebnissen führen, wenn sie aufgrund von Spot-

Kapazitätsschwankungen zu unterschiedlichen Zeiten berechnet wird. Eine Punktzahl von 10 bedeutet zwar, dass Ihre Spot-Kapazitätsanforderung mit hoher Wahrscheinlichkeit – aber nicht garantiert – erfolgreich ist, aber für beste Ergebnisse empfehlen wir Ihnen, sofort auf eine Punktzahl zu reagieren. Wir empfehlen Ihnen auch, bei jedem Erstellen einer Kapazitätsanforderung eine neue Bewertung einzuholen.

Erforderliche Berechtigungen für Spot-Platzierungsbewertung

IAM-Identitäten (Benutzer, Rollen oder Gruppen) sind standardmäßig nicht berechtigt, the section called “Spot-Platzierungsbewertung” zu verwenden. Damit IAM-Identitäten den Spot Placement Score verwenden können, müssen Sie eine IAM-Richtlinie erstellen, die die Erlaubnis zur Verwendung der `ec2:GetSpotPlacementScores` EC2 API-Aktion erteilt. Anschließend fügen Sie die Richtlinie an die IAM-Identitäten an, die diese Berechtigung erfordern.

Im Folgenden finden Sie ein Beispiel für eine IAM-Richtlinie, die die Erlaubnis zur Verwendung der API-Aktion erteilt. `ec2:GetSpotPlacementScores` EC2

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:GetSpotPlacementScores",
            "Resource": "*"
        }
    ]
}
```

Informationen zum Bearbeiten einer IAM-Richtlinie finden Sie unter Bearbeiten von IAM-Richtlinien im IAM-Benutzerhandbuch.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Eine Spot-Platzierungsbewertung berechnen

Sie können eine Spot-Platzierungsbewertung berechnen, die auf der Zielkapazität und den Datenverarbeitungsanforderungen basiert. Weitere Informationen finden Sie unter the section called “So funktioniert die Spot-Platzierungsbewertung”.

Erforderliche -Berechtigungen

Stellen Sie zuerst sicher, dass Sie über die erforderlichen Berechtigungen verfügen. Weitere Informationen finden Sie unter the section called “Erforderliche Berechtigungen”.

Optionen

- Mithilfe von Instance-Attributen berechnen
- Mithilfe von Instance-Typen berechnen
- Berechnen Sie mit AWS CLI

Suchen Sie nach einer automatisierten Lösung? Anstatt die manuellen Schritte in diesem Benutzerhandbuch zu befolgen, können Sie ein Spot-Placement-Score-Tracker-Dashboard erstellen, das die Ergebnisse automatisch erfasst und in Amazon speichert CloudWatch. Weitere Informationen finden Sie unter Anleitung zur Erstellung eines Spot-Platzierungsbewertungs-Tracker-Dashboard in AWS.

Mithilfe von Instance-Attributen berechnen

So berechnen Sie eine Spot-Platzierungsbewertung durch Angabe von Instance-Attributen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Klicken Sie auf den Abwärtspfeil neben Spot Instances anfordern und wählen Sie Spot-Platzierungsbewertung berechnen aus.
4. Wählen Sie Anforderungen eingeben aus.
5. Geben Sie für Zielkapazität Ihre gewünschte Kapazität in Form der Anzahl der Instanzen oder v CPUs oder der Speichermenge (MiB) ein.
6. Um Ihre Rechenanforderungen zu spezifizieren und Amazon die optimalen Instance-Typen mit diesen Anforderungen EC2 ermitteln zu lassen, wählen Sie unter Instance-Attribute angeben, die Ihren Rechenanforderungen entsprechen.
7. Geben Sie für v CPUs die gewünschte Mindest- und Höchstzahl von v einCPUs. Um kein Limit anzugeben, wählen Sie Kein Minimum, Kein Maximum oder beides aus.
8. Geben Sie für Arbeitsspeicher (GiB) den gewünschten Mindest- und Höchstwert ein. Um kein Limit anzugeben, wählen Sie Kein Minimum, Kein Maximum oder beides.
9. Wählen Sie für CPU-Architektur die erforderliche Instance-Architektur aus.
10. (Optional) Für Zusätzliche Instance-Attribute können Sie optional ein oder mehrere Attribute angeben, um Ihre Computinganforderungen genauer auszudrücken. Jedes zusätzliche Attribut fügt Ihrer Anforderung weitere Einschränkungen hinzu. Sie können die zusätzlichen Attribute weglassen. In diesem Fall werden die Standardwerte verwendet. Eine Beschreibung der einzelnen Attribute und ihrer Standardwerte finden Sie unter get-spot-placement-scores.
11. (Optional) Um die Instance-Typen mit Ihren angegebenen Attributen anzuzeigen, erweitern Sie Vorschau der übereinstimmenden Instance-Typen. Um Instance-Typen von der Verwendung in der Platzierungsauswertung auszuschließen, wählen Sie die Instances aus und wählen Sie dann Ausgewählte Instance-Typen ausschließen.
12. Klicken Sie auf Platzierungsbewertungen laden und überprüfen Sie die Ergebnisse.
13. (Optional) Um die Spot-Platzierungsbewertung für bestimmte Regionen anzuzeigen, wählen Sie für Auszuwertende Regionen die zu bewertenden Regionen und dann Platzierungsbewertungen berechnen aus.
14. (Optional) Um die Spot-Platzierungsbewertung für die Availability Zones in den angezeigten Regionen anzuzeigen, aktivieren Sie das Kontrollkästchen Platzierungsbewertungen pro Availability Zone bereitstellen. Eine Liste der bewerteten Availability Zones ist nützlich, wenn Sie Ihre gesamte Spot-Kapazität in einer einzigen Availability Zone starten möchten.
15. (Optional) Um Ihre Rechenanforderungen zu bearbeiten und einen neuen Platzierungswert zu erhalten, wählen Sie Bearbeiten, nehmen Sie die notwendigen Anpassungen vor und wählen Sie dann Berechnen von Platzierungswerten aus.

Mithilfe von Instance-Typen berechnen

So berechnen Sie eine Spot-Platzierungsbewertung durch Angabe von Instance-Typen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Klicken Sie auf den Abwärtspfeil neben Spot Instances anfordern und wählen Sie Spot-Platzierungsbewertung berechnen aus.
4. Wählen Sie Anforderungen eingeben aus.
5. Geben Sie für Zielkapazität Ihre gewünschte Kapazität in Form der Anzahl der Instanzen oder v CPUs oder der Speichermenge (MiB) ein.
6. Um die zu verwendenden Instance-Typen anzugeben, wählen Sie unter Instance-Typanforderungen die Option Instance-Typen manuell auswählen aus.
7. Klicken Sie auf Instance-Typen auswählen, wählen Sie die Instance-Typen aus, die verwendet werden sollen und klicken Sie dann auf Auswählen. Um Instance-Typen schnell zu finden, können Sie die Instance-Typen mithilfe der Filterleiste nach verschiedenen Eigenschaften filtern.
8. Klicken Sie auf Platzierungsbewertungen laden und überprüfen Sie die Ergebnisse.
9. (Optional) Um die Spot-Platzierungsbewertung für bestimmte Regionen anzuzeigen, wählen Sie für Auszuwertende Regionen die zu bewertenden Regionen und dann Platzierungsbewertungen berechnen aus.
10. (Optional) Um die Spot-Platzierungsbewertung für die Availability Zones in den angezeigten Regionen anzuzeigen, aktivieren Sie das Kontrollkästchen Platzierungsbewertungen pro Availability Zone bereitstellen. Eine Liste der bewerteten Availability Zones ist nützlich, wenn Sie Ihre gesamte Spot-Kapazität in einer einzigen Availability Zone starten möchten.
11. (Optional) Um die Liste der Instance-Typen zu bearbeiten und einen neuen Platzierungswert zu erhalten, wählen Sie Bearbeiten, nehmen Sie die notwendigen Anpassungen vor und wählen Sie dann Berechnen von Platzierungswerten aus.

Berechnen Sie mit AWS CLI

Berechnen Sie die Spot-Platzierungsbewertung

1. (Optional) Verwenden Sie den get-spot-placement-scoresBefehl und den Parameter, um alle möglichen Parameter zu generieren, die für die Konfiguration des Punktplatzierungswerts angegeben werden können. `--generate-cli-skeleton`

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
    --generate-cli-skeleton
```

Es folgt eine Beispielausgabe.

```
{
    "InstanceTypes": [
        ""
    ],
    "TargetCapacity": 0,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "RegionNames": [
        ""
    ],
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": [
            "x86_64_mac"
        ],
        "VirtualizationTypes": [
            "hvm"
        ],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 0,
                "Max": 0
            },
            "MemoryMiB": {
                "Min": 0,
                "Max": 0
            },
            "CpuManufacturers": [
                "amd"
            ],
            "MemoryGiBPerVCpu": {
                "Min": 0.0,
                "Max": 0.0
            },
            "ExcludedInstanceTypes": [
                ""
            ],
```

```
            "InstanceGenerations": [
                "previous"
            ],
            "SpotMaxPricePercentageOverLowestPrice": 0,
            "OnDemandMaxPricePercentageOverLowestPrice": 0,
            "BareMetal": "excluded",
            "BurstablePerformance": "excluded",
            "RequireHibernateSupport": true,
            "NetworkInterfaceCount": {
                "Min": 0,
                "Max": 0
            },
            "LocalStorage": "included",
            "LocalStorageTypes": [
                "hdd"
            ],
            "TotalLocalStorageGB": {
                "Min": 0.0,
                "Max": 0.0
            },
            "BaselineEbsBandwidthMbps": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorTypes": [
                "fpga"
            ],
            "AcceleratorCount": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorManufacturers": [
                "amd"
            ],
            "AcceleratorNames": [
                "vu9p"
            ],
            "AcceleratorTotalMemoryMiB": {
                "Min": 0,
                "Max": 0
            }
        }
    },
    "DryRun": true,
```

```
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Erstellen Sie eine JSON-Konfigurationsdatei mit der Ausgabe des vorherigen Schritts und konfigurieren Sie sie wie folgt:

   a. Geben Sie für `TargetCapacity` die gewünschte Spot-Kapazität in Form der Anzahl der Instances oder v CPUs oder der Speichermenge (MiB) ein.

   b. Geben Sie für `TargetCapacityUnitType` die Einheit für die Zielkapazität ein. Wenn Sie diesen Parameter weglassen, wird standardmäßig `units` verwendet.

      Zulässige Werte: `units` (bedeutet eine Anzahl der Instances) | `vcpu` | `memory-mib`

   c. Geben Sie für `SingleAvailabilityZone` `true` für eine Antwort an, die eine Liste bewerteter Availability Zones zurückgibt. Eine Liste der bewerteten Availability Zones ist nützlich, wenn Sie Ihre gesamte Spot-Kapazität in einer einzigen Availability Zone starten möchten. Wenn Sie diesen Parameter weglassen, wird standardmäßig `false` verwendet und die Antwort gibt eine Liste der bewerteten Regionen zurück.

   d. (Optional) Geben Sie für `RegionNames` die Regionen an, die als Filter verwendet werden soll(en). Sie müssen den Regionscode angeben, z. B. `us-east-1`.

      Bei einem Regionsfilter gibt die Antwort nur die von Ihnen angegebenen Regionen zurück. Wenn Sie `true` für `SingleAvailabilityZone` angegeben haben, gibt die Antwort nur die Availability Zones in den angegebenen Regionen zurück.

   e. Sie können entweder `InstanceTypes` oder `InstanceRequirements` aufnehmen, jedoch nicht beide in derselben Konfiguration.

      Geben Sie in Ihrer JSON-Konfiguration eine der folgenden Optionen an:

      - Um eine Liste der Instance-Typen anzugeben, geben Sie die Instance-Typen im `InstanceTypes`-Parameter an. Geben Sie mindestens drei verschiedene Instance-Typen an. Wenn Sie nur einen oder zwei Instance-Typen angeben, gibt die Spot-Bewertungsplatzierung eine niedrige Bewertung zurück. Eine Liste der Instance-Typen finden Sie unter EC2 Amazon-Instance-Typen.
      - Um die Instance-Attribute anzugeben, sodass Amazon EC2 die Instance-Typen identifiziert, die diesen Attributen entsprechen, geben Sie die Attribute an, die sich in der `InstanceRequirements` Struktur befinden.

Sie müssen Werte für `VCpuCount`, `MemoryMiB` und `CpuManufacturers` angeben. Sie können die anderen Attribute weglassen. In diesem Fall werden die Standardwerte verwendet. Eine Beschreibung der einzelnen Attribute und ihrer Standardwerte finden Sie unter get-spot-placement-scores.

Beispielkonfigurationen finden Sie unter Beispielkonfigurationen.

3. Um den Spot-Platzierungswert für die Anforderungen abzurufen, die Sie in der JSON-Datei angegeben haben, verwenden Sie den get-spot-placement-scoresBefehl und geben Sie mithilfe des `--cli-input-json` Parameters den Namen und den Pfad zu Ihrer JSON-Datei an.

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

Beispielausgabe, wenn `SingleAvailabilityZone` auf `false` gesetzt oder weggelassen ist (in diesem Fall wird standardmäßig `false` verwendet) – eine bewertete Liste von Regionen wird zurückgegeben.

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "Score": 7
    },
    {
        "Region": "us-west-1",
        "Score": 5
    },
   ...
```

Beispielausgabe, wenn `SingleAvailabilityZone` auf `true` gesetzt ist – eine bewertete Liste von Availability Zones wird zurückgegeben.

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "use1-az1",
        "Score": 8
    },
```

```
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "usw2-az3",
        "Score": 6
    },
   ...
```

Beispielkonfigurationen

Wenn Sie den verwenden AWS CLI, können Sie die folgenden Beispielkonfigurationen verwenden.

Beispielkonfigurationen

- Beispiel: Instance-Typen und Zielkapazität angeben
- Beispiel: Instance-Typen und Zielkapazität in Bezug auf Arbeitsspeicher angeben
- Beispiel: Angeben von Attributen für die attributbasierte Instance-Typauswahl
- Beispiel: Geben Sie Attribute für die attributbasierte Instance-Typauswahl an und geben Sie eine bewertete Liste von Availability Zones zurück

Beispiel: Instance-Typen und Zielkapazität angeben

Die folgende Beispielkonfiguration gibt drei verschiedene Instance-Typen und eine Ziel-Spot-Kapazität von 500 Spot Instances an.

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500
}
```

Beispiel: Instance-Typen und Zielkapazität in Bezug auf Arbeitsspeicher angeben

Die folgende Beispielkonfiguration gibt drei verschiedene Instance-Typen und eine Ziel-Spot-Kapazität von 500 000 MiB Speicher an, wobei die Anzahl der zu startenden Spot Instances insgesamt 500 000 MiB Speicher bereitstellen muss.

```
{
```

```
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500000,
    "TargetCapacityUnitType": "memory-mib"
}
```

Beispiel: Angeben von Attributen für die attributbasierte Instance-Typauswahl

Die folgende Beispielkonfiguration ist für die attributbasierte Instance-Typauswahl konfiguriert, gefolgt von einer Texterklärung der Beispielkonfiguration.

```
{
    "TargetCapacity": 5000,
    "TargetCapacityUnitType": "vcpu",
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

`InstanceRequirementsWithMetadata`

Um die attributbasierte Instance-Typauswahl zu verwenden, müssen Sie die `InstanceRequirementsWithMetadata`-Struktur in Ihre Konfiguration aufnehmen und die gewünschten Attribute für die Spot Instances angeben.

Im vorherigen Beispiel werden die folgenden erforderlichen Instance-Attribute angegeben:

- `ArchitectureTypes` – Der Architekturtyp der Instance-Typen muss `arm64` sein.
- `VirtualizationTypes` – Der Virtualisierungstyp der Instance-Typen muss `hvm` sein.

- `VCpuCount`— Die Instance-Typen müssen mindestens 1 und maximal 12 V habenCPUs.
- `MemoryMiB` – Die Instance-Typen müssen mindestens 512 MiB Speicher aufweisen. Indem Sie den `Max`-Parameter weglassen, geben Sie an, dass es keine Höchstgrenze gibt.

Beachten Sie, dass es mehrere andere optionale Attribute gibt, die Sie angeben können. Eine Liste der Attribute finden Sie unter get-spot-placement-scores.

`TargetCapacityUnitType`

Der `TargetCapacityUnitType`-Parameter gibt die Einheit für die Zielkapazität an. Im Beispiel sind die Zielkapazität `5000` und der Typ der Zielkapazitätseinheit`vcpu`, die zusammen eine gewünschte Zielkapazität von 5000 v angebenCPUs, wobei die Anzahl der zu startenden Spot-Instances insgesamt 5000 v ergeben mussCPUs.

Beispiel: Geben Sie Attribute für die attributbasierte Instance-Typauswahl an und geben Sie eine bewertete Liste von Availability Zones zurück

Die folgende Beispielkonfiguration ist für die attributbasierte Instance-Typauswahl konfiguriert. Indem Sie `"SingleAvailabilityZone": true` angeben, gibt die Antwort eine Liste der bewerteten Availability Zones zurück.

```
{
    "TargetCapacity": 1000,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

Ihre Spot-Instance-Kosten mithilfe des Spot-Instance-Daten-Feeds verfolgen

Um Ihnen zu helfen, die Gebühren für Ihre Spot-Instances zu verstehen, EC2 stellt Amazon einen Datenfeed zur Verfügung, der Ihre Spot-Instance-Nutzung und Preise beschreibt. Dieser Daten-Feed wird an den Amazon S3-Bucket gesendet, den Sie beim Abonnieren des Daten-Feeds angegeben haben.

Daten-Feed-Dateien treffen in der Regel einmal pro Stunde in Ihrem Bucket ein. Wenn während einer bestimmten Stunde keine Spot-Instance ausgeführt wird, erhalten Sie für diese Stunde keine Daten-Feed-Datei.

Jede Stunde Spot-Instance-Nutzung wird in der Regel in einer einzelnen Datendatei abgedeckt. Diese Dateien werden komprimiert (gzip), bevor sie an Ihren Bucket geliefert werden. Amazon EC2 kann mehrere Dateien für eine bestimmte Nutzungsstunde schreiben, wenn die Dateien groß sind (z. B. wenn der Dateiinhalt für die Stunde vor der Komprimierung 50 MB überschreitet).

> **Note**
>
> Sie können jeweils nur einen Spot-Instance-Datenfeed erstellen AWS-Konto.

Der Spot-Instance-Datenfeed wird in allen AWS Regionen außer China (Peking), China (Ningxia), AWS GovCloud (USA) und den Regionen unterstützt, die standardmäßig deaktiviert sind.

Inhalt

- Name und Format der Daten-Feed-Datei
- Anforderungen für den Amazon S3-Bucket
- Abonnieren eines Spot-Instance-Date-Feeds
- Daten in Ihrem Datenfeed anzeigen
- Löschen Ihres Spot-Instance-Daten-Feeds

Name und Format der Daten-Feed-Datei

Der Name der Daten-Feed-Datei für eine Spot-Instance weist das folgende Format auf (Datum und Uhrzeit in UTC):

```
bucket-name.s3.amazonaws.com/optional-prefix/aws-account-id.YYYY-MM-DD-HH.n.unique-id.gz
```

Wenn Ihr Bucket-Name beispielsweise **amzn-s3-demo-bucket** lautet und Ihr Präfix **my-prefix**, dann sehen Ihre Dateinamen in etwa wie folgt aus:

```
amzn-s3-demo-bucket.s3.amazonaws.com/my-
prefix/111122223333.2023-12-09-07.001.b959dbc6.gz
```

Weitere Informationen zu Bucket-Namen finden Sie unter Regeln für die Bucket-Benennung im Benutzerhandbuch für Amazon S3.

Die Daten-Feed-Dateien für die Spot-Instance verwenden Tabulatoren als Trennzeichen. Jede Zeile in der Datendatei entspricht einer Instance-Stunde und enthält die in der folgenden Tabelle aufgeführten Felder.

Feld	Beschreibung
`Timestamp`	Der Zeitstempel, der zur Berechnung des Preises für diese Instance-Nutzung verwendet wird.
`UsageType`	Die Art der Nutzung und der Instance-Typ, für die diese Kosten anfallen. Für `m1.small` Spot-Instances ist dieses Feld auf `SpotUsage` festgelegt. Bei allen anderen Instance-Typen ist dieses Feld auf `SpotUsage:` {Instance-type} eingestellt. Beispiel, `SpotUsage:c1.medium` .
`Operation`	Das Produkt, für das diese Kosten anfallen. Bei Linux-Spot-Instances ist dieses Feld auf `RunInstances` eingestellt. Bei Windows-Spot-Instances ist dieses Feld auf `RunInstances:0002` eingestellt. Die Spot-Nutzung wird nach den Availability Zones gruppiert.
`InstanceID`	Die ID der Spot-Instance, die diese Instance-Nutzung generiert hat.
`MyBidID`	Die ID der Spot-Instance-Anforderung, die diese Instance-Nutzung generiert hat.
`MyMaxPrice`	Der für diese Spot-Anforderung angegebene Höchstpreis.

Feld	Beschreibung
`MarketPrice`	Der Spot-Preis zu dem im Feld `Timestamp` angegebenen Zeitpunkt.
`Charge`	Der für diese Instance-Nutzung berechnete Preis
`Version`	Die Version des Datenfeeds. Die mögliche Version ist 1.0.

Anforderungen für den Amazon S3-Bucket

Beim Abonnieren des Daten-Feeds müssen einen Amazon S3-Bucket angeben, in dem die Daten-Feed-Dateien gespeichert werden sollen.

Beachten Sie bei der Auswahl eines Amazon S3-Buckets für den Daten-Feed Folgendes:

- Sie müssen eine `FULL_CONTROL`-Berechtigung für den Bucket haben. Wenn Sie der Bucket-Eigentümer sind, verfügen Sie standardmäßig über diese Berechtigung. Andernfalls muss der Bucket-Besitzer Ihnen AWS-Konto diese Erlaubnis erteilen.
- Wenn Sie einen Datenfeed abonnieren, werden diese Berechtigungen verwendet, um die Bucket-ACL zu aktualisieren, sodass dem AWS Datenfeed-Konto die entsprechenden `FULL_CONTROL` Berechtigungen erteilt werden. Das AWS Datenfeed-Konto schreibt Datenfeed-Dateien in den Bucket. Wenn Ihr Konto nicht über die erforderlichen Berechtigungen verfügt, können die Daten-Feed-Dateien nicht in den Bucket geschrieben werden. Weitere Informationen finden Sie unter An Amazon S3 gesendete Logs im Amazon CloudWatch Logs-Benutzerhandbuch.

  Wenn Sie die ACL aktualisieren und die Berechtigungen für das AWS Datenfeed-Konto entfernen, können die Datenfeed-Dateien nicht in den Bucket geschrieben werden. Sie müssen den Daten-Feed erneut abonnieren, um die Daten-Feed-Dateien zu erhalten.
- Jede Daten-Feed-Datei verfügt über eine eigene ACL (unabhängig von der ACL für den Bucket). Der Bucket-Eigentümer verfügt über eine `FULL_CONTROL`-Berechtigung für die Datendateien. Das AWS Datenfeed-Konto hat Lese- und Schreibberechtigungen.
- Wenn Sie Ihr Datenfeed-Abonnement löschen, EC2 entzieht Amazon weder dem Bucket noch den AWS Datendateien die Lese- und Schreibberechtigungen für das Datenfeed-Konto. Sie müssen diese Berechtigungen selbst entfernen.
- Wenn Sie Ihren Amazon S3 S3-Bucket mit serverseitiger Verschlüsselung mit einem in AWS Key Management Service (SSE-KMS) gespeicherten AWS KMS Schlüssel verschlüsseln, müssen

Sie einen vom Kunden verwalteten Schlüssel verwenden. Weitere Informationen finden Sie unter serverseitige Amazon S3 S3-Bucket-Verschlüsselung im Amazon CloudWatch Logs-Benutzerhandbuch.

Abonnieren eines Spot-Instance-Date-Feeds

Sie können Ihren Spot-Instance-Daten-Feed jederzeit abonnieren. Sie können diese Aufgabe nicht mit der EC2 Amazon-Konsole abschließen.

Wenn Sie eine Fehlermeldung erhalten, dass der Bucket nicht über genügend Berechtigungen verfügt, finden Sie Informationen zur Fehlerbehebung im folgenden Artikel: Problembehandlung beim Daten-Feed für Spot Instances.

AWS CLI

So abonnieren Sie Ihren Daten-Feed

Verwenden Sie den Befehl create-spot-datafeed-subscription.

Verwenden Sie das folgende Beispiel, um einen Bucket mit einem Präfix anzugeben:

```
aws ec2 create-spot-datafeed-subscription \
    --bucket amzn-s3-demo-bucket \
    --prefix my-prefix
```

Verwenden Sie das folgende Beispiel, um einen Bucket ohne einem Präfix anzugeben:

```
aws ec2 create-spot-datafeed-subscription \
    --bucket amzn-s3-demo-bucket
```

PowerShell

So abonnieren Sie Ihren Daten-Feed

Verwenden Sie das cmdlet New-EC2SpotDatafeedSubscription.

Verwenden Sie das folgende Beispiel, um einen Bucket mit einem Präfix anzugeben:

```
New-EC2SpotDatafeedSubscription `
    -Bucket amzn-s3-demo-bucket `
    -Prefix my-prefix
```

Verwenden Sie das folgende Beispiel, um einen Bucket ohne einem Präfix anzugeben:

```
New-EC2SpotDatafeedSubscription `
    -Bucket amzn-s3-demo-bucket
```

Daten in Ihrem Datenfeed anzeigen

In der AWS-Managementkonsole, öffne AWS CloudShell. Verwenden Sie den folgenden s3-Sync-Befehl, um die GZ-Dateien für Ihren Datenfeed aus dem S3-Bucket abzurufen und sie in dem von Ihnen angegebenen Ordner zu speichern.

```
aws s3 sync s3://amzn-s3-demo-bucket ./data-feed
```

Um den Inhalt einer .gz-Datei anzuzeigen, wechseln Sie zu dem Ordner, in dem Sie den Inhalt des S3-Buckets gespeichert haben.

```
cd data-feed
```

Verwenden Sie den ls-Befehl, um die Namen der Dateien anzuzeigen. Verwenden Sie den zcat-Befehl mit dem Namen der Datei, um den Inhalt der komprimierten Datei anzuzeigen. Nachfolgend finden Sie ein Beispielbefehl.

```
zcat  111122223333.2023-12-09-07.001.b959dbc6.gz
```

Es folgt eine Beispielausgabe.

```
#Version: 1.0
#Fields: Timestamp UsageType Operation InstanceID MyBidID MyMaxPrice MarketPrice Charge
 Version
2023-12-09 07:13:47 UTC USE2-SpotUsage:c7a.medium       RunInstances:SV050
 i-0c3e0c0b046e050df     sir-pwq6nmfp    0.0510000000 USD        0.0142000000 USD
  0.0142000000 USD        1
```

Löschen Ihres Spot-Instance-Daten-Feeds

Wenn Sie den Spot-Instance-Daten-Feed nicht mehr benötigen, können Sie ihn löschen.

AWS CLI

So löschen Sie den Daten-Feed

Verwenden Sie den Befehl delete-spot-datafeed-subscription.

```
aws ec2 delete-spot-datafeed-subscription
```

PowerShell

So löschen Sie den Daten-Feed

Verwenden Sie das cmdlet Remove-EC2SpotDatafeedSubscription.

```
Remove-EC2SpotDatafeedSubscription
```

Serviceverknüpfte Rolle für Spot-Instance-Anforderungen

Amazon EC2 verwendet dienstbezogene Rollen für die Berechtigungen, die erforderlich sind, um andere AWS Dienste in Ihrem Namen aufzurufen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit einer verknüpft ist. AWS-Service Dienstbezogene Rollen bieten eine sichere Möglichkeit, Berechtigungen zu delegieren, AWS-Services da nur der verknüpfte Dienst eine dienstbezogene Rolle übernehmen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollen im IAM-Benutzerhandbuch.

Amazon EC2 verwendet die servicebezogene Rolle namens AWSServiceRoleForEC2Spot, um Spot-Instances in Ihrem Namen zu starten und zu verwalten.

Berechtigungen vonAWSServiceRoleForEC2Spot

Amazon EC2 verwendet AWSServiceRoleForEC2Spot, um die folgenden Aktionen durchzuführen:

- `ec2:DescribeInstances`: Spot-Instances beschreiben
- `ec2:StopInstances`: Spot-Instances stoppen
- `ec2:StartInstances`: Spot-Instances starten

Erstellen der serviceverknüpften Rolle

Größtenteils müssen Sie die serviceverknüpfte Rolle nicht manuell erstellen. Amazon EC2 erstellt die mit dem AWSServiceRoleForEC2Spot-Dienst verknüpfte Rolle, wenn Sie zum ersten Mal eine Spot-Instance über die Konsole anfordern.

Wenn Sie vor Oktober 2017, als Amazon EC2 begann, diese servicebezogene Rolle zu unterstützen, eine aktive Spot-Instance-Anfrage hatten, EC2 hat Amazon die AWSServiceRoleForEC2Spot-Rolle in Ihrem AWS Konto erstellt. Weitere Informationen finden Sie unter In meinem Konto wird eine neue Rolle angezeigt im IAM-Benutzerhandbuch.

Wenn Sie die AWS CLI oder eine API verwenden, um eine Spot-Instance anzufordern, müssen Sie zunächst sicherstellen, dass diese Rolle existiert.

Um AWSServiceRoleForEC2Spot mit der Konsole zu erstellen

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Rollen aus.
3. Wählen Sie Create role (Rolle erstellen) aus.
4. Wählen Sie auf der Seite Typ der vertrauenswürdigen Entität auswählen EC2die Optionen EC2 - Spot-Instances und Weiter: Berechtigungen aus.
5. Klicken Sie auf der nächsten Seite auf Next: Review (Nächster Schritt: Prüfen).
6. Wählen Sie auf der Seite Review (Prüfen) Create role (Rolle erstellen) aus.

Um AWSServiceRoleForEC2Spot mit dem zu erstellen AWS CLI

Verwenden Sie den create-service-linked-role-Befehl wie folgt:

```
aws iam create-service-linked-role --aws-service-name spot.amazonaws.com
```

Wenn Sie Spot-Instances nicht mehr verwenden müssen, empfehlen wir Ihnen, die AWSServiceRoleForEC2Spot-Rolle zu löschen. Nachdem diese Rolle aus Ihrem Konto gelöscht wurde, erstellt Amazon EC2 die Rolle erneut, wenn Sie Spot-Instances anfordern.

Gewähren Sie Zugriff auf vom Kunden verwaltete Schlüssel zur Verwendung mit verschlüsselten AMIs und EBS-Snapshots

Wenn Sie ein verschlüsseltes AMI oder einen verschlüsselten Amazon EBS-Snapshot für Ihre Spot-Instances angeben und einen vom Kunden verwalteten Schlüssel für die Verschlüsselung verwenden, müssen Sie der AWSServiceRoleForEC2Spot-Rolle die Erlaubnis erteilen, den vom Kunden verwalteten Schlüssel zu verwenden, damit Amazon Spot-Instances in Ihrem Namen starten EC2 kann. Dazu müssen Sie dem vom Kunden verwalteten Schlüssel eine Erteilung hinzufügen, wie im Folgenden gezeigt:

Bei der Einrichtung von Berechtigungen ist die Erteilung von Berechtigung eine Alternative zu Schüsselrichtlinien. Weitere Informationen finden Sie unter Verwenden von Erteilungen und Verwenden von Schlüsselrichtlinien in AWS KMS im Developer-Handbuch für AWS Key Management Service .

Um der AWSServiceRoleForEC2Spot-Rolle Berechtigungen zur Verwendung des vom Kunden verwalteten Schlüssels zu erteilen

- Verwenden Sie den Befehl create-grant, um dem vom Kunden verwalteten Schlüssel einen Grant hinzuzufügen und den Principal (die mit dem AWSServiceRoleForEC2Spot-Dienst verknüpfte Rolle) anzugeben, der die Berechtigung zur Ausführung der durch die Gewährung erlaubten Operationen erhält. Der vom Kunden verwaltete Schlüssel wird durch den `key-id`-Parameter und den ARN des vom Kunden verwalteten Schlüssels angegeben. Der Principal wird durch den `grantee-principal` Parameter und den ARN der mit dem AWSServiceRoleForEC2Spot-Dienst verknüpften Rolle angegeben.

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
spot.amazonaws.com/AWSServiceRoleForEC2Spot \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Kontingente für Spot-Instances

Es gibt Kontingente für die Anzahl von ausgeführten Spot-Instances und von ausstehenden Spot-Instance-Anforderungen pro AWS-Konto und Region. Sobald eine ausstehende Spot-Instance-Anfrage erfüllt wurde, wird die Anfrage nicht mehr auf das Kontingent angerechnet, da die ausgeführte Instance auf das Kontingent angerechnet wird.

Spot-Instance-Kontingente werden anhand der Anzahl der virtuellen Zentraleinheiten (vCPUs) verwaltet, die Ihre laufenden Spot-Instances entweder verwenden oder bis zur Erfüllung offener Spot-Instance-Anfragen verwenden werden. Wenn Sie Ihre Spot-Instances beenden, aber die Spot-Instance-Anfragen nicht stornieren, werden die Anfragen auf Ihr Spot-Instance-vCPU-Kontingent angerechnet, bis Amazon die Spot-Instance-Kündigungen EC2 erkennt und die Anfragen schließt.

Wir bieten die folgenden Kontingenttypen für Spot Instances.

Name	Standard	Anpassbar
Alle DL-Spot-Instance-Anforderungen	0	Ja
Alle F-Spot-Instance-Anforderungen	0	Ja
Alle G- und VT-Spot-Instance-Anforderungen	0	Ja
Alle Inf-Spot-Instance-Anforderungen	0	Ja
Alle P4-, P3- und P2-Spot-Instance-Anfragen	0	Ja
Alle P5-Spot-Instance-Anfragen	0	Ja
Alle Spot-Instance-Standard-Anforderungen (A, C, D, H, I, M, R, T, Z)	5	Ja
Alle Anforderungen von Trn-Spot-Instances	0	Ja
Alle X-Spot-Instance-Anforderungen	0	Ja

Auch wenn Amazon Ihre Spot-Instance-Kontingente EC2 automatisch an Ihre Nutzung anpasst, können Sie bei Bedarf eine Erhöhung des Kontingents beantragen. Wenn Sie beispielsweise mehr Spot Instances starten möchten, als Ihr aktuelles Kontingent zulässt, können Sie eine Kontingenterhöhung anfordern. Sie können auch eine Kontingenterhöhung anfordern, wenn Sie eine Spot-Instance-Anforderung senden und der Fehler `Max spot instance count exceeded` angezeigt wird. Zum Anfordern einer Kontingenterhöhung können Sie die in EC2 Amazon-Servicekontingente beschriebene Service-Quotas-Konsole verwenden.

Sie können jede beliebige Kombination von Instance-Typen starten, die Ihren wechselnden Anwendungsanforderungen entspricht. Bei einem Kontingent für alle Standard-Spot-Instance-Anfragen von 256 v könnten Sie CPUs beispielsweise 32 `m5.2xlarge` Spot-Instances (32 x 8 vCPUs) oder 16 `c5.4xlarge` Spot-Instances (16 x 16 vCPUs) anfordern.

Mit der Integration von Amazon CloudWatch Metrics können Sie die EC2 Nutzung anhand Ihrer Kontingente überwachen. Sie können auch Alarme konfigurieren, um vor beinahe erreichten

Kontingenten zu warnen. Weitere Informationen finden Sie unter Service Quotas und CloudWatch Amazon-Alarme im Service-Kontingents-Benutzerhandbuch .

EC2 Dedizierte Amazon-Hosts

Ein Amazon EC2 Dedicated Host ist ein physischer Server, der vollständig für Ihre Nutzung reserviert ist. Sie können sich optional dafür entscheiden, die Instance-Kapazität mit anderen AWS -Konten zu teilen. Weitere Informationen finden Sie unter Kontoübergreifendes Amazon EC2 Dedicated Host-Sharing.

Dedicated Hosts bieten Transparenz und Kontrolle über die Platzierung von Instances und unterstützen Host-Affinität. Das bedeutet, dass Sie Instances auf bestimmten Hosts starten und ausführen können und dass Sie sicherstellen können, dass Instances nur auf bestimmten Hosts ausgeführt werden. Weitere Informationen finden Sie unter Automatische Platzierung und Host-Affinität EC2 für Amazon Dedicated Host.

Dedicated Hosts bieten umfassenden Support für Bring Your Own License (BYOL). Sie ermöglichen es Ihnen, Ihre vorhandenen Softwarelizenzen pro Socket, pro Kern oder pro VM, einschließlich Windows Server, SQL Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux oder andere Softwarelizenzen, die an Sockets oder physische Kerne gebunden sind, gemäß Ihren Lizenzbedingungen zu verwenden. VMs

Wenn Sie möchten, dass Ihre Instances auf dedizierter Hardware ausgeführt werden, Sie aber keine Transparenz oder Kontrolle über die Instance-Platzierung benötigen und Sie keine Softwarelizenzen pro Socket oder pro Core verwenden müssen, können Sie stattdessen die Verwendung von Dedicated Instances in Betracht ziehen. Dedicated Instances und Dedicated Hosts können beide verwendet werden, um EC2 Amazon-Instances auf dedizierten physischen Servern zu starten.
Es gibt keine leistungsbezogenen, sicherheitsrelevanten oder physischen Unterschiede zwischen Dedicated Instances und Instances auf Dedicated Hosts. Es gibt jedoch einige wichtige Unterschiede zwischen beiden. Die folgende Tabelle hebt einige der wichtigsten Unterschiede zwischen Dedicated Hosts und Dedicated Instances hervor:

	Dedicated Host	Dedicated Instance
Dedizierter physischer Server	Physischer Server mit Instance-Kapazität, die vollständig für Ihre Nutzung bereitgestellt wird.	Physischer Server, der für ein einzelnes Kundenkonto bereitgestellt wird.

	Dedicated Host	Dedicated Instance
Instance-Kapazität sfreigabe	Kann die Instance-Kapazität mit anderen Konten teilen.	Nicht unterstützt
Fakturierung	Abrechnung pro Host	Abrechnung pro Instance
Sichtbarkeit von Sockets, Kernen und Host-ID	Zeigt die Anzahl der Sockets und physischen Kerne	Keine Sichtbarkeit
Host- und Instance-Affinität	Gestattet Ihnen, Ihre Instances im Laufe der Zeit durchgängig auf demselben physischen Server bereitzustellen	Nicht unterstützt
Zielgerichtete Instance-Platzierung	Bietet zusätzliche Sichtbarkeit und Kontrolle darüber, wie Instances auf einem physischen Server platziert werden.	Nicht unterstützt
Automatis che Instance-Wiederher stellung	Unterstützt. Weitere Informationen finden Sie unter Wiederherstellung von Amazon EC2 Dedicated Host.	Unterstützt
Bring Your Own License (BYOL)	Unterstützt	Teilweise Unterstützung*
Kapazität sreservie rungen	Nicht unterstützt	Unterstützt

* Microsoft SQL Server mit Lizenzmobilität über Software Assurance und Windows Virtual Desktop Access (VDA)-Lizenzen können mit Dedicated Instance verwendet werden.

Weitere Informationen über Dedicated Instances finden Sie unter Amazon-EC2-Dedicated-Instances.

Dedicated Hosts-Einschränkungen

Bevor Sie Dedicated Hosts zuordnen, beachten Sie die folgenden Begrenzungen und Einschränkungen:

- Um RHEL und SUSE Linux auf Dedicated Hosts ausführen zu können, müssen Sie Ihre eigenen mitbringen. AMIs Sie können RHEL und SUSE Linux AMIs , die von Dedicated Hosts angeboten werden AWS oder auf AWS Marketplace Dedicated Hosts verfügbar sind, nicht verwenden. Weitere Informationen zum Erstellen Ihres eigenen AMI finden Sie unter Bringen Sie Ihre eigenen Softwarelizenzen zu Amazon EC2 Dedicated Hosts.

  Diese Einschränkung gilt nicht für Hosts, die für Instances mit hohem Arbeitsspeicher (`u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal`, und `u-24tb1.metal`) zugewiesen sind. RHEL und SUSE Linux AMIs , die von AWS oder auf angeboten werden, AWS Marketplace können mit diesen Hosts verwendet werden.
- Es gibt eine Begrenzung für die Anzahl der laufenden Dedicated Hosts pro Instance-Familie pro AWS -Konto pro Region. Kontingente gelten nur für laufende Instances. Wenn Ihre Instance aussteht, stoppt oder angehalten wird, wird sie nicht auf Ihr Kontingent angerechnet. Um die Kontingente für Ihr Konto einzusehen oder eine Kontingenterhöhung anzufordern, können Sie die Service-Quotas-Konsole verwenden.
- Amazon EC2 Auto Scaling Scaling-Gruppen werden unterstützt, wenn eine Startvorlage verwendet wird, die eine Host-Ressourcengruppe spezifiziert. Weitere Informationen finden Sie unter Erstellen einer Startvorlage mit erweiterten Einstellungen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.
- Amazon RDS-Instances werden nicht unterstützt.
- Das AWS kostenlose Nutzungskontingent ist für Dedicated Hosts nicht verfügbar.
- Die Instance-Platzierungskontrolle bezieht sich auf die Verwaltung von Instance-Starts auf Dedicated Hosts. Sie können Dedicated Hosts nicht in Placement-Gruppen starten.
- Wenn Sie einen Host für einen virtualisierten Instance-Typ zuweisen, können Sie den Instance-Typ nicht in einen `.metal`-Instance-Typ ändern, nachdem der Host zugewiesen wurde. Wenn Sie beispielsweise einen Host für den `m5.large`-Instance-Typ zuweisen, können Sie den Instance-Typ nicht in `m5.metal` ändern.

  Ebenso können Sie, wenn Sie einen Host für einen `.metal`-Instance-Typ zuweisen, den Instance-Typ nicht in einen virtualisierten Instance-Typ ändern, nachdem der Host zugewiesen wurde.

Wenn Sie beispielsweise einen Host für den `m5.metal`-Instance-Typ zuweisen, können Sie den Instance-Typ nicht in `m5.large` ändern.

Inhalt

- Preise und Abrechnung EC2 für Amazon Dedicated Host
- Kapazitätskonfigurationen EC2 für Amazon Dedicated Host-Instances
- Burstable T3-Instances auf Amazon EC2 Dedicated Hosts
- Bringen Sie Ihre eigenen Softwarelizenzen zu Amazon EC2 Dedicated Hosts
- Automatische Platzierung und Host-Affinität EC2 für Amazon Dedicated Host
- Weisen Sie Ihrem Konto einen Amazon EC2 Dedicated Host zu
- Starten Sie EC2 Amazon-Instances auf einem Amazon EC2 Dedicated Host
- Starten Sie EC2 Amazon-Instances in einer Host-Ressourcengruppe
- Ändern Sie die Einstellung für die automatische Platzierung für einen vorhandenen Amazon EC2 Dedicated Host
- Unterstützte Instance-Typen für einen vorhandenen Amazon EC2 Dedicated Host ändern
- Ändern Sie die Tenancy und Affinität von Amazon EC2 Dedicated Host für eine Amazon-Instance EC2
- Einen Amazon EC2 Dedicated Host veröffentlichen
- Migrieren Sie zu Nitro-basierten Amazon EC2 Dedicated Hosts
- Dedicated-Host-Reservierungen für Abrechnungsrabatte bei Dedicated Hosts erwerben
- Kontoübergreifendes Amazon EC2 Dedicated Host-Sharing
- Amazon EC2 Dedicated Hosts auf AWS Outposts
- Wiederherstellung von Amazon EC2 Dedicated Host
- Host-Wartung für Amazon EC2 Dedicated Host
- Überwachen Sie den Status Ihrer Amazon EC2 Dedicated Hosts
- Verfolgen Sie Änderungen der Amazon EC2 Dedicated Host-Konfiguration mit AWS Config

Preise und Abrechnung EC2 für Amazon Dedicated Host

Der Preis für eine Dedicated Host variiert in Abhängigkeit von der Zahlungsoption.

Zahlungsoptionen

- On-Demand Dedicated Hosts
- Dedicated Host Reservations
- Savings Plans
- Preise für Windows Server auf Dedicated Hosts

On-Demand Dedicated Hosts

Die On-Demand-Abrechnung wird automatisch aktiviert, wenn Sie Ihrem Konto einen Dedicated Host zuweisen.

Der On-Demand-Preis für einen Dedicated Host variiert abhängig von Instance-Familie und Region. Sie zahlen pro Sekunde (mit einem Minimum von 60 Sekunden) für den aktiven Dedicated Host, unabhängig von der Menge oder der Größe der Instances, die Sie darauf starten möchten. Weitere Informationen zu On-Demand-Preisen finden Sie unter Amazon EC2 Dedicated Hosts On-Demand-Preise.

Sie können einen On-Demand Dedicated Host jederzeit freigeben, sodass keine Gebühren mehr dafür anfallen. Weitere Informationen über die Freigabe eines Dedicated Host finden Sie unter Einen Amazon EC2 Dedicated Host veröffentlichen.

Dedicated Host Reservations

Dedicated Host-Reservierungen bietet einen Abrechnungsrabatt im Vergleich zur Ausführung von On-Demand-Dedicated Hosts. Reservierungen sind in drei Zahlungsoptionen verfügbar:

- Keine Vorauszahlung:— Reservierungen vom Typ "Keine Vorauszahlung" bieten Ihnen einen Rabatt auf Ihre Dedicated Host-Nutzung in einem bestimmten Zeitraum und erfordern keine Vorauszahlung. Verfügbar mit einer Laufzeit von einem Jahr und drei Jahren. Nur einige Instance-Familien unterstützen die dreijährige Laufzeit für „Keine Vorabreservierungen“.
- Teilweise Vorauszahlung:— Ein Teil der Reservierung muss im Voraus bezahlt werden und die restlichen Stunden während der Laufzeit werden zu einem ermäßigten Satz abgerechnet. Verfügbar mit einer Laufzeit von einem Jahr und drei Jahren.
- Komplette Vorauszahlung:— Bietet den günstigsten effektiven Preis. Ist verfügbar mit einer Laufzeit von einem Jahr und drei Jahren und deckt die gesamten Kosten für die Laufzeit im Voraus ab, ohne weitere, künftig anfallende Kosten.

Sie müssen über aktive Dedicated Hosts in Ihrem Konto verfügen, bevor Sie Reservierungen kaufen können. Jede Reservierung kann einen oder mehrere Hosts abdecken, die dieselbe Instance-Familie in einer einzelnen Availability Zone unterstützen. Reservierungen werden auf die Instance-Familie auf dem Host angewendet, nicht auf die Instance-Größe. Falls Sie über drei Dedicated Hosts mit verschiedenen Instance-Größen (`m4.xlarge`, `m4.medium` und `m4.large`) verfügen, können Sie eine einzelne `m4`-Reservierung all diesen Dedicated Hosts zuordnen. Die Instance-Familie und Availability Zone müssen mit denen der Dedicated Hosts übereinstimmen, denen Sie sie zuordnen möchten.

Wenn eine Reservierung einem Dedicated Host zugeordnet wird, kann der Dedicated Host erstellt freigestellt werden, wenn die Laufzeit der Reservierung vorüber ist.

Weitere Informationen zu den Reservierungspreisen finden Sie unter Amazon EC2 Dedicated Hosts-Preise.

Savings Plans

Savings Plans sind ein flexibles Preismodell, das erhebliche Einsparungen gegenüber On-Demand-Instances bietet. Mit Savings Plans verpflichten Sie sich zu einer konstanten Nutzung (in USD pro Stunde) für eine Laufzeit von einem oder drei Jahren. Dadurch erhalten Sie die Flexibilität, die Dedicated Hosts zu nutzen, die Ihren Anforderungen am besten entsprechen. Zugleich können Sie weiterhin Geld sparen, statt sich auf eine bestimmte Dedicated Host festzulegen. Weitere Informationen finden Sie im AWS Savings Plans User Guide.

> **Note**
>
> Savings Plans werden mit `u-6tb1.metal`-, `u-9tb1.metal`-, `u-12tb1.metal`-, `u-18tb1.metal`- und `u-24tb1.metal`-Dedicated-Hosts nicht unterstützt.

Preise für Windows Server auf Dedicated Hosts

Vorbehaltlich der Microsoft-Lizenzbedingungen können Sie Ihre vorhandenen Windows Server- und SQL Server-Lizenzen zu Dedicated Hosts mitbringen. Wenn Sie Ihre eigenen Lizenzen mitbringen, fallen keine zusätzlichen Kosten für die Softwarenutzung an.

Darüber hinaus können Sie auch Windows Server AMIs von Amazon verwenden, um die neuesten Versionen von Windows Server auf Dedicated Hosts auszuführen. Dies kommt häufig in Szenarien vor, in denen Sie über vorhandene SQL Server-Lizenzen verfügen, die zur Ausführung auf Dedicated Hosts berechtigt sind, aber Windows Server zur Ausführung der SQL Server-Workload benötigen.

Von Amazon AMIs bereitgestellte Windows Server werden nur auf Instance-Typen der aktuellen Generation unterstützt. Weitere Informationen finden Sie unter Amazon EC2 Dedicated Hosts — Preise.

Kapazitätskonfigurationen EC2 für Amazon Dedicated Host-Instances

Dedicated Hosts unterstützen verschiedene Konfigurationen (physische Kerne, Sockets und VCPUs), mit denen Sie Instances verschiedener Familien und Größen ausführen können.

Wenn Sie Ihrem Konto einen Dedicated Host zuweisen, können Sie eine Konfiguration auswählen, die entweder einen einzelnen Instance-Typ oder mehrere Instance-Typen innerhalb derselben Instance-Familie unterstützt. Die Anzahl der Instances, die Sie auf einem Host ausführen können, hängt von der ausgewählten Konfiguration ab.

Inhalt

- Unterstützung für einzelne Instance-Typen
- Unterstützung mehrerer Instance-Typen

Unterstützung für einzelne Instance-Typen

Sie können einen Dedicated Host zuweisen, der nur einen Instance-Typ unterstützt. Bei dieser Konfiguration muss jede Instance, die Sie auf dem Dedicated Host starten, vom gleichen Instance-Typ sein, den Sie bei der Zuweisung des Hosts angeben.

Sie können beispielsweise einen Host zuweisen, der nur den `m5.4xlarge`-Instance-Typ unterstützt. In diesem Fall können Sie nur `m5.4xlarge`-Instances auf diesem Host ausführen.

Die Anzahl der Instances, die Sie auf dem Host starten können, hängt von der Anzahl der vom Host bereitgestellten physischen Kerne und der Anzahl der vom angegebenen Instance-Typ verbrauchten Kerne ab. Wenn Sie beispielsweise einen Host für `m5.4xlarge`-Instances zuweisen, stellt der Host 48 physische Kerne bereit und jede `m5.4xlarge`-Instance verbraucht 8 physische Kerne. Dies bedeutet, dass Sie bis zu 6 Instances auf diesem Host starten können (48 physische Kerne / 8 Kerne pro Instance = 6 Instances).

Unterstützung mehrerer Instance-Typen

Sie können einen Dedicated Host zuweisen, der mehrere Instance-Typen innerhalb derselben Instance-Familie unterstützt. Auf diese Weise können Sie verschiedene Instance-Typen auf demselben Host ausführen, sofern sie sich in derselben Instance-Familie befinden und der Host über ausreichend Instance-Kapazität verfügt.

Sie können beispielsweise einen Host zuweisen, der verschiedene R5-Instance-Typen innerhalb der Instance-Familie unterstützt. In diesem Fall können Sie auf diesem Host bestimmte Kombinationen von R5-Instance-Typen, wie z. B. `r5.large`, `r5.xlarge`, `r5.2xlarge` und `r5.4xlarge`, starten, bis zur physischen Kernkapazität des Hosts.

Die folgenden Instance-Familien unterstützen Dedicated Hosts mit Unterstützung mehrerer Instance-Typen:

- Allzweck: A1 | M5 | M5n | M6i | M7i | T3
- Für Datenverarbeitung optimiert: C5 | C5n | C6i | C7i
- Arbeitsspeicheroptimiert: R5 | R5n | R6i | R7i

Die Anzahl der Instances, die Sie auf dem Host ausführen können, hängt von der Anzahl der vom Host bereitgestellten physischen Kerne und der Anzahl der von jedem Instance-Typ, den Sie auf dem Host ausführen, verbrauchten Kerne ab. Wenn Sie beispielsweise einen R5-Host zuweisen, der 48 physische Kerne bereitstellt, und Sie zwei `r5.2xlarge`-Instances (4 Kerne x 2 Instances) und drei `r5.4xlarge`-Instances (8 Kerne x 3 Instances) ausführen, verbrauchen diese Instances insgesamt 32 Kerne. Sie können eine beliebige Kombination von R5-Instances ausführen, solange diese die verbleibenden 16 Kerne nicht überschreiten.

Für jede Instance-Familie gibt es jedoch ein Limit für die Anzahl der Instances, die für jeden Instance-Typ ausgeführt werden können. Beispielsweise unterstützt ein R5 Dedicated Host maximal 2 `r5.8xlarge`-Instances, die 32 der physischen Kerne nutzen. In diesem Fall können dann zusätzliche R5-Instances kleinerer Größe verwendet werden, um den Host auf die Kernkapazität zu füllen. Informationen zur unterstützten Anzahl von Instance-Typen für jede Instance-Familie finden Sie unter Konfigurationstabelle für Dedicated Hosts.

Die folgende Tabelle zeigt Beispielkombinationen von Instance-Typen:

Instance-Familie	Beispiel für Instance-Typenkombinationen	
R5	• Beispiel 1: 4 x `r5.4xlarge` + 4 x `r5.2xlarge` • Beispiel 2: 1 x `r5.12xlarge` + 1 x `r5.4xlarge` + 1 x `r5.2xlarge` + 5 x `r5.xlarge` + 2 x `r5.large`	
C5		

Instance-Familie	Beispiel für Instance-Typenkombinationen
	• Beispiel 1: 1 x `c5.9xlarge` + 2 x `c5.4xlarge` + 1 x `c5.xlarge` • Beispiel 2: 4 x `c5.4xlarge` + 1 x `c5.xlarge` + 2 x `c5.large`
M5	• Beispiel 1: 4 x `m5.4xlarge` + 4 x `m5.2xlarge` • Beispiel 2: 1 x `m5.12xlarge` + 1 x `m5.4xlarge` + 1 x `m5.2xlarge` + 5 x `m5.xlarge` + 2 x `m5.large`

Überlegungen

Beachten Sie beim Arbeiten mit Dedicated Hosts, die mehrere Instance-Typen unterstützen, Folgendes:

- Die Verwendung mehrerer Instance-Typen auf demselben Host ist nur innerhalb derselben Instance-Familie möglich.
- Wenn Instance-Typen gemischt werden, empfehlen wir zur Maximierung der Hostauslastung, zuerst größere Instance-Typen und dann kleinere Instance-Typen zu starten.
  - Je nach Kombination und Startreihenfolge der Instance-Typen auf einem Dedicated Host ist es möglicherweise physisch nicht möglich, die Auslastung des Hosts zu maximieren. Beim Mischen von Instance-Typen auf einem Host ist möglicherweise ein Teil der Kapazität auf dem Host verfügbar, aber nicht nutzbar. Beispielsweise könnten Sie sehen, dass 16 v auf einem r5n-Host CPUs verfügbar ist, Sie aber möglicherweise keine 4xlarge-Instance auf dem Host starten können, obwohl r5n.4xlarge auf 16 v ausgeführt wird. CPUs

> **Note**
>
> Wenn Sie einen A1 Dedicated Host für mehrere Instance-Typen aktivieren, können Sie auf diesem Host nur eine Mischung aus `a1.xlarge`- und `a1.2xlarge`-Instances starten. Wenn Sie eine `a1.medium`- oder `a1.large`-Instance auf diesem Host starten, sind Sie darauf beschränkt, nur weitere Instances desselben Instance-Typs auf dem Host zu starten. Eine

einzelne `a1.4xlarge`-Instance verbraucht die gesamte Kapazität auf dem Host. Wenn Sie einen Host für `a1.medium`- oder `a1.large`-Instances benötigen, empfehlen wir, diesen Instance-Typen separate Hosts zuzuweisen.

Burstable T3-Instances auf Amazon EC2 Dedicated Hosts

Dedicated Hosts unterstützen T3-Instances mit burstable Leistung. T3-Instances bieten eine kosteneffiziente Möglichkeit, Ihre berechtigte BYOL-Lizenzsoftware auf dedizierter Hardware zu verwenden. Der geringere vCPU-Footprint von T3-Instances ermöglicht es Ihnen, Ihre Workloads auf weniger Hosts zu konsolidieren und Ihre Lizenzauslastung pro Kern zu maximieren.

T3-Dedicated-Hosts eignen sich am besten für die Ausführung von BYOL-Software mit geringer bis mittlerer CPU-Auslastung. Dies umfasst berechtigte Softwarelizenzen pro Socket, pro Kern oder pro VM (z. B. Windows Server, Windows Desktop, SQL Server, SUSE Enterprise Linux Server, Red Hat Enterprise Linux und Oracle Database). Beispiele für Workloads, die für T3-Dedicated-Hosts geeignet sind, sind kleine und mittlere Datenbanken, virtuelle Desktops, Entwicklungs- und Testumgebungen, Code-Repositorys und Produktprototypen. T3-Dedicated-Hosts werden nicht für Workloads mit anhaltender hoher CPU-Auslastung oder für Workloads empfohlen, bei denen gleichzeitig korrelierte CPU-Bursts auftreten.

T3-Instances auf Dedicated Hosts verwenden dasselbe Kreditmodell wie T3-Instances auf gemeinsam genutzter Tenancy-Hardware. Sie unterstützen jedoch nur den `standard`-Kredit-Modus; sie unterstützen nicht den `unlimited`-Kredit-Modus. Im `standard`-Modus verdienen, verbrauchen und sammeln T3-Instances auf Dedicated Hosts Guthaben auf dieselbe Weise wie spitzenlastfähige Instances auf gemeinsam genutzter Tenancy-Hardware. Sie bieten eine Basis-CPU-Leistung mit der Möglichkeit, über das Basisniveau zu steigen. Um die Basisleistung zu übersteigen, gibt die Instance Guthaben aus, die sie in ihrem CPU-Guthaben-Konto angesammelt hat. Wenn die aufgelaufenen Gutschriften erschöpft sind, wird die CPU-Auslastung auf die Basisebene gesenkt. Weitere Informationen zum `standard`-Modus finden Sie unter Funktionsweise der Standard-Instances mit Spitzenlastleistung.

T3 Dedicated Hosts unterstützen alle Funktionen von Amazon EC2 Dedicated Hosts, einschließlich mehrerer Instance-Größen auf einem einzigen Host, Host-Ressourcengruppen und BYOL.

Unterstützte T3-Instance-Größen und -konfigurationen

T3-Dedicated-Hosts führen universelle burstable T3-Instances aus, die CPU-Ressourcen des Hosts gemeinsam nutzen, indem sie eine Basis-CPU-Leistung und die Möglichkeit bieten, bei Bedarf auf ein

höheres Niveau zu steigen. Dadurch können T3-Dedicated-Hosts mit 48 Kernen bis zu 192 Instances pro Host unterstützen. Um die Ressourcen des Hosts effizient zu nutzen und die beste Instance-Leistung zu erzielen, berechnet der EC2 Amazon-Instance-Platzierungsalgorithmus automatisch die unterstützte Anzahl von Instances und Instance-Größenkombinationen, die auf dem Host gestartet werden können.

T3-Dedicated-Hosts unterstützen mehrere Instance-Typen auf demselben Host. Alle T3-Instance-Größen werden auf Dedicated Hosts unterstützt. Sie können verschiedene Kombinationen von T3-Instances bis zum CPU-Limit des Hosts ausführen.

In der folgenden Tabelle werden die unterstützten Instance-Typen aufgeführt, die Leistung jedes Instance-Typs zusammengefasst und die maximale Anzahl von Instances jeder Größe angegeben, die gestartet werden können.

Insta Typ	v CPUs	Arbeitsspeicher (GiB)	Basis-CPU-Auslastung pro vCPU	Netzwerk-Burst-Bandbreite (Gbit/s)	Amazon-EBS-Burst-Bandbreite (Mbit/s)	Maximale Anzahl von Instances pro Dedicated Host
t3.na	2	0.5	5 %	5	Bis zu 2 085	192
t3.m	2	1	10 %	5	Bis zu 2 085	192
t3.sn	2	2	20 %	5	Bis zu 2 085	192
t3.m	2	4	20 %	5	Bis zu 2 085	192
t3.la	2	8	30 %	5	2.780	96
t3.xla	4	16	40%	5	2.780	48
t3.2x e	8	32	40%	5	2.780	24

Überwachung der CPU-Auslastung für T3-Dedicated-Hosts

Sie können die `DedicatedHostCPUUtilization` CloudWatch Amazon-Metrik verwenden, um die vCPU-Auslastung eines Dedicated Hosts zu überwachen. Die Metrik ist im `EC2`-Namespace und der

`Per-Host-Metrics`-Dimension verfügbar. Weitere Informationen finden Sie unter Dedicated-Host-Metriken.

Bringen Sie Ihre eigenen Softwarelizenzen zu Amazon EC2 Dedicated Hosts

Dedicated Hosts gestatten Ihnen, Ihre vorhandenen Lizenzen pro Socket, pro Kern oder pro VM-Software zu verwenden. Wenn Sie BYOL verwenden, sind Sie für die Verwaltung Ihrer eigenen Lizenzen verantwortlich. Amazon EC2 bietet jedoch Funktionen, die Ihnen dabei helfen, die Lizenzbestimmungen einzuhalten, z. B. Instance-Affinität und gezielte Platzierung.

Dies sind die allgemeinen Schritte, die Sie befolgen müssen, um Ihr eigenes volumenlizenziertes Maschinenimage auf Amazon zu importieren EC2.

1. Prüfen Sie, ob die Lizenzbedingungen, die die Nutzung Ihrer Computer-Images regeln, die Nutzung in einer virtualisierten Cloud-Umgebung erlauben. Weitere Informationen über die Microsoft-Lizenzierung finden Sie unter Amazon Web Services- und Microsoft-Lizenzierung.
2. Nachdem Sie sich vergewissert haben, dass Ihr Maschinen-Image in Amazon verwendet werden kann EC2, importieren Sie es mit VM Import/Export. Informationen zum Importieren Ihres Maschinen-Images finden Sie im Import/Export VM-Benutzerhandbuch.
3. Nach dem Importieren Ihres Machine Image können Sie Instances davon auf aktiven Dedicated Hosts in Ihrem Konto starten.
4. Wenn Sie diese Instances ausführen, müssen Sie je nach Betriebssystem diese Instances auf Ihrem eigenen KMS-Server aktivieren (Beispiel: Windows Server oder Windows SQL Server). Sie können Ihr importiertes Windows-AMI nicht über den Amazon Windows KMS-Server aktivieren.

> **Note**
>
> Um zu verfolgen, wie Ihre Bilder verwendet werden AWS, aktivieren Sie die Host-Aufzeichnung in AWS Config. Sie können AWS Config damit Konfigurationsänderungen auf einem Dedicated Host aufzeichnen und die Ausgabe als Datenquelle für Lizenzberichte verwenden. Weitere Informationen finden Sie unter Verfolgen Sie Änderungen der Amazon EC2 Dedicated Host-Konfiguration mit AWS Config.

Automatische Platzierung und Host-Affinität EC2 für Amazon Dedicated Host

Die Platzierungssteuerung für Dedicated Hosts erfolgt sowohl auf Instance- als auch auf Hostebene.

Automatische Platzierung

Die automatische Platzierung ist auf Host-Ebene konfiguriert. Mit ihr können Sie steuern, ob gestartete Instances auf einem bestimmten Host oder auf einem beliebigen verfügbaren Host mit passender Konfiguration gestartet werden.

Wenn die automatische Platzierung eines Dedicated Host deaktiviert ist, akzeptiert er nur Host-Tenancy-Instance-Starts, die seine eindeutige Host-ID angeben. Dies ist die Standardeinstellung für neue Dedicated Hosts.

Wenn die automatische Platzierung für einen Dedicated Host aktiviert ist, akzeptiert er alle nicht zielgerichteten, Host-Tenancy-Instances, die seiner Instancetypkonfiguration entsprechen.

Beim Starten einer Instance müssen Sie Ihre Tenancy konfigurieren. Wenn eine Instance auf einem Dedicated Host gestartet wird, ohne eine spezifische `HostId` anzugeben, kann sie auf jedem beliebigen Dedicated Host gestartet werden, für den automatische Platzierung aktiviert ist, und der für den Instance-Typ geeignet ist.

Host-Affinität

Host-Affinität wird auf Instance-Ebene konfiguriert. Sie schafft eine Start-Beziehung zwischen einer Instance und einem Dedicated Host.

Wenn die Affinität auf `Host` festgelegt ist, wird eine Instance, die auf einem spezifischen Host gestartet wurde, immer auf demselben Host neu gestartet, wenn sie einmal angehalten wurde. Dies gilt für gezielte und nicht gezielte Starts.

Wenn die Affinität auf `Default` gesetzt ist, und Sie den Neustart der Instance anhalten, kann sie auf jedem verfügbaren Host gestartet werden. Es wird jedoch versucht, sie auf dem letzten Dedicated Host zu starten, auf dem sie ausgeführt wurde (auf Best Effort-Basis).

Weisen Sie Ihrem Konto einen Amazon EC2 Dedicated Host zu

Um einen Dedicated Host zu nutzen, müssen Sie ihn zunächst in Ihrem Konto zuweisen. Nachdem den Dedicated Host zugewiesen haben, wird die Dedicated Host-Kapazität sofort in Ihrem Konto verfügbar gemacht und Sie können mit dem Starten von Instances über den Dedicated Host beginnen.

Wenn Sie Ihrem Konto einen Dedicated Host zuweisen, können Sie eine Konfiguration auswählen, die entweder einen einzelnen Instance-Typ oder mehrere Instance-Typen innerhalb derselben

Instance-Familie unterstützt. Die Anzahl der Instances, die Sie auf dem Host ausführen können, hängt von der ausgewählten Konfiguration ab. Weitere Informationen finden Sie unter Kapazitätskonfigurationen EC2 für Amazon Dedicated Host-Instances.

Console

So weisen Sie ein Dedicated Host zu

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts und dann Allocate Dedicated Host (Dedicated Host zuweisen) aus.
3. Wählen Sie für Instance (Instance-Familie) die Instance-Familie für die Dedicated Host aus.
4. Geben Sie an, ob der Dedicated Host mehrere Instance-Größen innerhalb der ausgewählten Instance-Familie oder nur einen bestimmten Instance-Typ unterstützt. Führen Sie eine der folgenden Aufgaben aus.

   - Um den Dedicated Host so zu konfigurieren, dass mehrere Instance-Typen in der ausgewählten Instance-Familie unterstützt werden, wählen Sie für Support multiple instance types (Mehrere Instance-Typen unterstützen) die Option Enable (Aktivieren) aus. Wenn Sie diese Option aktivieren, können Sie verschiedene Instance-Größen aus derselben Instance-Familie auf dem Dedicated Host starten. Wenn Sie die Instance-Familie `m5` und diese Option auswählen, können Sie beispielsweise `m5.xlarge`- und `m5.4xlarge`-Instances auf dem Dedicated Host starten.
   - Um das Dedicated Host so zu konfigurieren, dass ein einzelner Instance-Typ innerhalb der ausgewählten Instance-Familie unterstützt wird, deaktivieren Sie Support multiple instance types (Mehrere Instance-Typen unterstützen) und wählen Sie dann für Instance type (Instance-Typ) den zu unterstützenden Instance-Typ. Damit können Sie einen einzelnen Instance-Typ auf dem Dedicated Host starten. Wenn Sie diese Option wählen und `m5.4xlarge` als unterstützten Instance-Typ angeben, können Sie beispielsweise nur `m5.4xlarge`-Instances auf dem Dedicated Host starten.
5. Wählen Sie für Availability Zone die Availability Zone aus, in der der Dedicated Host zugewiesen werden soll.
6. Damit der Dedicated Host nicht zielgerichtete Instance-Starts akzeptiert, die seinem Instance-Typ entsprechen, wählen Sie für Instance auto-placement (Automatische Instance-Platzierung) Enable (Aktiveren) aus. Weitere Informationen zur automatischen Platzierung finden Sie unter Automatische Platzierung und Host-Affinität EC2 für Amazon Dedicated Host.

7. Zur Aktivierung der Host-Wiederherstellung für den Dedicated Host wählen Sie für Host recovery (Host-Wiederherstellung) Enable (Aktivieren) aus. Weitere Informationen finden Sie unter Wiederherstellung von Amazon EC2 Dedicated Host.
8. Geben Sie für Quantity (Menge) die Anzahl der zuzuordnenden Dedicated Hosts ein.
9. (Optional) Wählen Sie Add new Tags (Neuen Tags (Markierungen) hinzufügen) aus. Geben Sie einen Tag (Markierung)-Schlüssel und einen Tag (Markierung)-Wert ein.
10. Wählen Sie Allocate aus.

AWS CLI

So weisen Sie ein Dedicated Host zu

Verwenden Sie den allocate-hosts-Befehl. Im folgenden Beispiel wird einen Dedicated Host zugewiesen, der mehrere Instance-Typen aus der `m5`-Instance-Familie in der Availability Zone `us-east-1a` unterstützt. Es wird auch die Host-Wiederherstellung ermöglicht und die automatische Platzierung deaktiviert.

```
aws ec2 allocate-hosts \
    --instance-family "m5" \
    --availability-zone "us-east-1a" \
    --auto-placement "off" \
    --host-recovery "on" \
    --quantity 1
```

Das folgende Beispiel weist einen Dedicated Host zu, der nicht zielgerichtete Instance-Starts in der angegebenen Availability Zone unterstützt. Darüber hinaus werden die Host-Wiederherstellung und die automatische Platzierung aktiviert.

```
aws ec2 allocate-hosts \
    --instance-type "m5.large" \
    --availability-zone "eu-west-1a" \
    --auto-placement "on" \
    --host-recovery "on" \
    --quantity 1
```

PowerShell

So weisen Sie ein Dedicated Host zu

Verwenden Sie das cmdlet New-EC2Host. Im folgenden Beispiel wird einen Dedicated Host zugewiesen, der mehrere Instance-Typen aus der m5-Instance-Familie in der Availability Zone us-east-1a unterstützt. Für den Host ist außerdem die Host-Wiederherstellung aktiviert und die automatische Platzierung deaktiviert.

```
New-EC2Host `
    -InstanceFamily m5 `
    -AvailabilityZone us-east-1a `
    -AutoPlacement Off `
    -HostRecovery On `
    -Quantity 1
```

Das folgende Beispiel weist einen Dedicated Host zu, der nicht zielgerichtete Instance-Starts in der angegebenen Availability Zone unterstützt und die Host-Wiederherstellung ermöglicht.

```
New-EC2Host `
    -InstanceType m5.large `
    -AvailabilityZone eu-west-1a `
    -AutoPlacement On `
    -HostRecovery On `
    -Quantity 1
```

Starten Sie EC2 Amazon-Instances auf einem Amazon EC2 Dedicated Host

Nach dem Zuordnen eines Dedicated Host können Sie Instances darauf starten. Sie können keine Instances mit host-Tenancy starten, wenn Sie nicht Dedicated Hosts aktiviert haben und über genügend Kapazität für den von Ihnen gestarteten Instance-Typ verfügen.

Überlegungen

- Von Amazon AMIs bereitgestellte SQL Server, SUSE und RHEL EC2 können nicht mit Dedicated Hosts verwendet werden.
- Für Dedicated Hosts, die mehrere Instance-Größen unterstützen, wird empfohlen, zuerst die größeren Instance-Größen zu starten und dann die verbleibende Instance-Kapazität nach Bedarf mit den kleineren Instance-Größen zu füllen.
- Beachten Sie vor dem Start Ihrer Instances die Einschränkungen. Weitere Informationen finden Sie unter Dedicated Hosts-Einschränkungen.

Console

So starten Sie eine Instances auf einem spezifischen Dedicated Host über die Dedicated Hosts-Seite

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie auf der Seite Dedicated Hosts einen Host aus. Wählen Sie dann Actions (Aktionen) und Launch Instance(s) onto Host (Instance(s) auf Host starten) aus.
4. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) ein AMI aus der Liste aus.
5. Wählen Sie im Bereich Instance type (Instance-Typ) den zu startenden Instance-Typ aus.

   > **Note**
   >
   > Wenn der Dedicated Host nur einen einzelnen Instance-Typ unterstützt, ist der unterstützte Instance-Typ standardmäßig ausgewählt und kann nicht geändert werden.
   > Wenn der Dedicated Host mehrere Instance-Typen unterstützt, müssen Sie einen Instance-Typ innerhalb der unterstützten Instance-Familie basierend auf der verfügbaren Instance-Kapazität des Dedicated Host auswählen. Es wird empfohlen, zuerst die größeren Instance-Größen zu starten und dann die verbleibende Instance-Kapazität nach Bedarf mit den kleineren Instance-Größen zu füllen.
6. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das der Instance zugeordnet werden soll.
7. Wählen Sie im Bereich Erweiterte Details unter Tenancy-Affinität eins der folgenden aus:

   - Aus – Host-Affinität deaktiviert. Die Instance wird im angegebenen Host gestartet, es ist aber nicht garantiert, dass sie nach dem Anhalten wieder in demselben Dedicated Host gestartet wird.
   - Eine Dedicated-Host-ID – Host-Affinität aktiviert. Falls die Instance angehalten wird, wird sie immer wieder in diesem spezifischen Host neu gestartet, wenn Kapazität vorhanden ist. Wenn der Host über keine Kapazität verfügt, kann die Instance nicht neu gestartet werden. Sie müssen Affinität zu einem anderen Host herstellen.

Weitere Informationen zur Affinität finden Sie unter Automatische Platzierung und Host-Affinität EC2 für Amazon Dedicated Host.

> **Note**
>
> Die Optionen Tenancy und Host sind abhängig von dem ausgewählten Host vorkonfiguriert.

8. Konfigurieren Sie die verbleibenden Instance-Optionen nach Bedarf. Weitere Informationen finden Sie unter Referenz für EC2 Amazon-Instance-Konfigurationsparameter.
9. Wählen Sie Launch Instance (Instance starten) aus.

So starten Sie eine Instance auf einem Dedicated Host unter Verwendung des Launch Instance Wizard

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Launch Instance (Instance starten) aus.
3. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) ein AMI aus der Liste aus.
4. Wählen Sie im Bereich Instance type (Instance-Typ) den zu startenden Instance-Typ aus.
5. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das der Instance zugeordnet werden soll.
6. Führen Sie im Bereich Advanced details (Erweiterte Details) folgende Schritte aus:
   a. Wählen Sie unter Tenancy die Option Dedicated Host aus.
   b. Wählen Sie unter Target host by (Ziel-Host durch) die Option Host ID (Host-ID) aus.
   c. Wählen Sie unter Target host ID (Ziel-Host-ID) den Host aus, auf dem die Instance gestartet werden soll.
   d. Wählen Sie unter Tenancy-Affinität eins der folgenden aus:
      - Aus – Host-Affinität deaktiviert. Die Instance wird im angegebenen Host gestartet, es ist aber nicht garantiert, dass sie nach dem Anhalten wieder in demselben Dedicated Host gestartet wird.

- Eine Dedicated-Host-ID – Host-Affinität aktiviert. Falls die Instance angehalten wird, wird sie immer wieder in diesem spezifischen Host neu gestartet, wenn Kapazität vorhanden ist. Wenn der Host über keine Kapazität verfügt, kann die Instance nicht neu gestartet werden. Sie müssen Affinität zu einem anderen Host herstellen.

Weitere Informationen zur Affinität finden Sie unter Automatische Platzierung und Host-Affinität EC2 für Amazon Dedicated Host.

7. Konfigurieren Sie die verbleibenden Instance-Optionen nach Bedarf. Weitere Informationen finden Sie unter Referenz für EC2 Amazon-Instance-Konfigurationsparameter.
8. Wählen Sie Launch Instance (Instance starten) aus.

AWS CLI

So starten Sie eine Instance in einem Dedicated Host

Verwenden Sie den Befehl run-instances und geben Sie die Instance-Affinität, Tenancy und den Host in der Option `--placement` an.

Um auf einem bestimmten Dedicated Host mit Host-Affinität zu starten (die Instance wird immer auf demselben Host neu gestartet, wenn sie gestoppt wird):

```
--placement Affinity=host,Tenancy=host,HostId=h-07879acf49EXAMPLE
```

Um auf einem bestimmten Dedicated Host ohne Host-Affinität zu starten (die Instance kann auf jedem verfügbaren Host neu gestartet werden):

```
--placement Tenancy=host,HostId=h-07879acf49EXAMPLE
```

So starten Sie auf einem beliebigen verfügbaren Dedicated Host mit aktivierter Auto-Platzierung und passendem Instance-Typ:

```
--placement Tenancy=host
```

PowerShell

So starten Sie eine Instance in einem Dedicated Host

Verwenden Sie das New-EC2InstanceCmdlet und geben Sie die Instanzaffinität, den Tenancy und den Host im Parameter an. `-Placement`

So starten Sie auf einem bestimmten Dedicated Host mit Host-Affinität (die Instanz wird immer auf demselben Host neu gestartet, wenn sie gestoppt wird):

```
-Placement_Affinity host `
-Placement_Tenancy host `
-Placement_HostId h-07879acf49EXAMPLE
```

Um auf einem bestimmten Dedicated Host ohne Host-Affinität zu starten (die Instance kann auf jedem verfügbaren Host neu gestartet werden):

```
-Placement_Tenancy host `
-Placement_HostId h-07879acf49EXAMPLE
```

So starten Sie auf einem beliebigen verfügbaren Dedicated Host mit aktivierter Auto-Platzierung und passendem Instance-Typ:

```
-Placement_Tenancy host
```

Starten Sie EC2 Amazon-Instances in einer Host-Ressourcengruppe

Dedicated Hosts sind ebenfalls integriert AWS License Manager. Mit License Manager können Sie eine Hostressourcengruppe erstellen, bei der es sich um eine Sammlung von Dedicated Hosts handelt, die als einzelne Entity verwaltet werden. Beim Erstellen einer Hostressourcengruppe geben Sie die Einstellungen für die Hostverwaltung an, z. B. automatische Zuweisung und automatische Freigabe für die Dedicated Hosts. Auf diese Weise können Sie Instances auf Dedicated Hosts starten, ohne diese Hosts manuell zuzuweisen und zu verwalten. Weitere Informationen finden Sie unter Hostressourcengruppen im AWS License Manager Benutzerhandbuch.

Wenn Sie eine Instance in einer Host-Ressourcengruppe starten, die über einen Dedicated Host mit verfügbarer Instance-Kapazität verfügt, EC2 startet Amazon die Instance auf diesem Host. Wenn die Host-Ressourcengruppe keinen Host mit verfügbarer Instance-Kapazität hat, weist Amazon EC2 automatisch einen neuen Host in der Host-Ressourcengruppe zu und startet dann die Instance auf diesem Host. Weitere Informationen finden Sie unter Hostressourcengruppen im AWS License Manager Benutzerhandbuch.

Voraussetzungen und Einschränkungen

- Sie müssen dem AMI eine core- oder socket-basierte Lizenzkonfiguration zuordnen.
- Sie können SQL Server, SUSE oder RHEL, die von Amazon AMIs bereitgestellt werden, nicht EC2 mit Dedicated Hosts verwenden.
- Sie können nicht auf einen bestimmten Host abzielen, indem Sie eine Host-ID auswählen, und Sie können die Instance-Affinität beim Starten einer Instance in eine Hostressourcengruppe nicht aktivieren.

Console

So starten Sie eine Instance in einer Hostressourcengruppe

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Launch Instance (Instance starten) aus.
3. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) ein AMI aus der Liste aus.
4. Wählen Sie im Bereich Instance type (Instance-Typ) den zu startenden Instance-Typ aus.
5. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das der Instance zugeordnet werden soll.
6. Führen Sie im Bereich Advanced details (Erweiterte Details) folgende Schritte aus:
   a. Wählen Sie unter Tenancy die Option Dedicated Host aus.
   b. Wählen Sie unter Target host by (Ziel-Host durch) die Option Host resource group (Host-Ressourcengruppe) aus.
   c. Wählen Sie unter Tenancy host resource group (Tenancy-Host-Ressourcengruppe) die Host-Ressourcengruppe aus, in der die Instance gestartet werden soll.
   d. Führen Sie unter Tenancy affinity (Tenancy-Affinität) einen der folgenden Schritte aus:
      - Wählen Sie Off (Aus). Die Instance wird auf dem angegebenen Host gestartet, es ist aber nicht garantiert, dass sie nach dem Anhalten wieder auf demselben Dedicated Host gestartet wird.
      - Wählen Sie die ID des Dedicated Host aus. Falls die Instance angehalten wird, wird sie immer wieder auf diesem spezifischen Host neu gestartet.

Weitere Informationen zur Affinität finden Sie unter Automatische Platzierung und Host-Affinität EC2 für Amazon Dedicated Host.

7. Konfigurieren Sie die verbleibenden Instance-Optionen nach Bedarf. Weitere Informationen finden Sie unter Referenz für EC2 Amazon-Instance-Konfigurationsparameter.
8. Wählen Sie Launch Instance (Instance starten) aus.

AWS CLI

So starten Sie eine Instance in einer Hostressourcengruppe

Verwenden Sie den Befehl run-instances. Lassen Sie in der Option `--placement` den Tenancy weg und geben Sie den ARN der Host-Ressourcengruppe an.

```
--placement HostResourceGroupArn=arn:aws:resource-groups:us-
east-2:123456789012:group/my-resource-group
```

PowerShell

So starten Sie eine Instance in einer Hostressourcengruppe

Verwenden Sie das cmdlet New-EC2Instance. Lassen Sie im Parameter `-Placement` den Tenancy weg und geben Sie den ARN der Host-Ressourcengruppe an.

```
-Placement_HostResourceGroupArn arn:aws:resource-groups:us-
east-2:123456789012:group/my-resource-group
```

Ändern Sie die Einstellung für die automatische Platzierung für einen vorhandenen Amazon EC2 Dedicated Host

Sie können die Einstellungen für die automatische Platzierung eines Dedicated Hosts ändern, nachdem Sie ihn Ihrem AWS Konto zugewiesen haben.

Console

So ändern Sie die automatische Platzierung eines Dedicated Host

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie einen Host und Actions (Aktionen), Modify host (Host ändern) aus.
4. Wählen Sie bei Instance auto-placement (Automatische Platzierung der Instance) die Option Enable (Aktivieren) aus, um die automatische Platzierung zu aktivieren oder deaktivieren Sie Enable (Aktivieren), um die automatische Platzierung zu deaktivieren. Weitere Informationen finden Sie unter Automatische Platzierung und Host-Affinität EC2 für Amazon Dedicated Host.
5. Wählen Sie Save (Speichern) aus.

AWS CLI

So ändern Sie die automatische Platzierung eines Dedicated Host

Verwenden Sie den modify-hosts-Befehl.

```
aws ec2 modify-hosts \
    --auto-placement on \
    --host-ids h-012a3456b7890cdef
```

PowerShell

So ändern Sie die automatische Platzierung eines Dedicated Host

Verwenden Sie das cmdlet Edit-EC2Host.

```
Edit-EC2Host `
    -AutoPlacement 1 `
    -HostId h-012a3456b7890cdef
```

Unterstützte Instance-Typen für einen vorhandenen Amazon EC2 Dedicated Host ändern

Sie können einen Dedicated Host bearbeiten, um die von ihm unterstützten Instance-Typen zu ändern. Wenn er derzeit einen einzelnen Instance-Typ unterstützt, können Sie ihn so ändern, dass er mehrere Instance-Typen innerhalb der Instance-Familie unterstützt. Wenn er derzeit mehrere Instance-Typen unterstützt, können Sie ihn so ändern, dass er nur einen bestimmten Instance-Typ unterstützt.

Um einen Dedicated Host zum Support mehrerer Instance-Typen zu ändern, müssen Sie zunächst alle laufenden Instances auf dem Host stoppen. Die Änderung dauert ca. 10 Minuten. Der Dedicated Host wechselt in den Status `pending`, während die Änderung durchgeführt wird. Sie können keine gestoppten Instances starten oder neue Instances auf dem Dedicated Host starten, während er sich im Status `pending` befinden.

Um ein Dedicated Host, das mehrere Instance-Typen unterstützt, so zu ändern, dass es nur einen einzigen Instance-Typ unterstützt, muss der Host entweder keine ausgeführten Instances haben oder die ausgeführten Instances müssen von dem Instance-Typ sein, den der Host unterstützen soll. Um beispielsweise einen Host für mehrere Instance-Typen der `m5`-Instance-Familie so zu ändern, dass er nur `m5.large`-Instances unterstützt, darf der Dedicated Host entweder keine laufenden Instances haben oder es dürfen nur `m5.large`-Instances darauf laufen.

Wenn Sie einen Host für einen virtualisierten Instance-Typ zuweisen, können Sie den Instance-Typ nicht in einen `.metal`-Instance-Typ ändern, nachdem der Host zugewiesen wurde. Wenn Sie beispielsweise einen Host für den `m5.large`-Instance-Typ zuweisen, können Sie den Instance-Typ nicht in `m5.metal` ändern. Ebenso können Sie, wenn Sie einen Host für einen `.metal`-Instance-Typ zuweisen, den Instance-Typ nicht in einen virtualisierten Instance-Typ ändern, nachdem der Host zugewiesen wurde. Wenn Sie beispielsweise einen Host für den `m5.metal`-Instance-Typ zuweisen, können Sie den Instance-Typ nicht in `m5.large` ändern.

Console

SO ändern Sie die unterstützten Instance-Typen für einen Dedicated Host

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Host (Dedizierter Host) aus.
3. Wählen Sie den zu ändernden Dedicated Host und Actions (Aktionen), Modify host (Host ändern) aus.
4. Führen Sie je nach der aktuellen Konfiguration des Dedicated Host einen der folgenden Schritte aus:

   - Wenn der Dedicated Host derzeit einen bestimmten Instance-Typ unterstützt, ist Support multiple instance types (Unterstützung mehrerer Instance-Typen) nicht aktiviert und Instance type (Instance-Typ) führt den unterstützten Instance-Typ auf. Um den Host so zu ändern, dass er mehrere Typen in der aktuellen Instance-Familie unterstützt, wählen Sie für Support multiple instance types (Unterstützung mehrerer Instance-Typen) die Option Enable (Aktivieren) aus.

Sie müssen zunächst alle Instances stoppen, die auf dem Host laufen, bevor Sie ihn so ändern, dass er mehrere Instance-Typen unterstützt.

- Wenn Dedicated Host derzeit mehrere Instance-Typen in einer Instance-Familie unterstützt, wird Enabled (Aktiviert) für Support multiple instance types (Mehrere Instance-Typen unterstützen) ausgewählt. Um den Host so zu ändern, dass er einen bestimmten Instance-Typ unterstützt, löschen Sie bei Support multiple instance types (Unterstützung mehrerer Instance-Typen) die Option Enable (Aktivieren) und wählen dann bei Instance type (Instance-Typ) den spezifischen zu unterstützenden Instance-Typ aus.

  Sie können die vom Dedicated Host unterstützte Instance-Familie nicht ändern.

5. Wählen Sie Save (Speichern) aus.

AWS CLI

SO ändern Sie die unterstützten Instance-Typen für einen Dedicated Host

Verwenden Sie den modify-hosts-Befehl.

Im folgenden Beispiel wird ein Dedicated Host für die Unterstützung mehrerer Instance-Typen innerhalb der `m5`-Instance-Familie geändert.

```
aws ec2 modify-hosts \
    --instance-family m5 \
    --host-ids h-012a3456b7890cdef
```

Im folgenden Beispiel wird ein Dedicated Host so geändert, dass nur `m5.xlarge`-Instances unterstützt werden.

```
aws ec2 modify-hosts \
    --instance-type m5.xlarge \
    --instance-family --host-ids h-012a3456b7890cdef
```

PowerShell

SO ändern Sie die unterstützten Instance-Typen für einen Dedicated Host

Verwenden Sie das cmdlet Edit-EC2Host.

Im folgenden Beispiel wird ein Dedicated Host für die Unterstützung mehrerer Instance-Typen innerhalb der m5-Instance-Familie geändert.

```
Edit-EC2Host `
    -InstanceFamily m5 `
    -HostId h-012a3456b7890cdef
```

Im folgenden Beispiel wird ein Dedicated Host so geändert, dass nur `m5.xlarge`-Instances unterstützt werden.

```
Edit-EC2Host `
    -InstanceType m5.xlarge `
    -HostId h-012a3456b7890cdef
```

Ändern Sie die Tenancy und Affinität von Amazon EC2 Dedicated Host für eine Amazon-Instance EC2

Die Tenancy einer Instance kann geändert werden, nachdem sie gestartet wurde. Sie können die Affinität für Ihre Instance auch ändern, um einen bestimmten Host als Ziel festzulegen, oder das Starten auf einem beliebigen verfügbaren Dedicated Host mit passenden Attributen in Ihrem Konto zulassen. Um entweder die Instance-Tenancy oder die Affinität der Instance zu ändern, muss sich die Instance im Status `stopped` befinden.

Welche Konvertierungen unterstützt werden, hängt von den Betriebssystemdetails Ihrer Instance sowie davon ab, ob SQL Server installiert ist. Weitere Informationen zu den für Ihre Instance verfügbaren Tenancy-Konvertierungspfaden finden Sie im License Manager-Benutzerhandbuch unter Tenancy-Konvertierung.

> **Note**
>
> Bei T3-Instances muss die Instance auf einem Dedicated Host gestartet werden, um eine Tenancy vom Typ `host` zu verwenden. Bei T3-Instances kann die Tenancy nicht von `host` in `dedicated` oder `default` geändert werden. Wenn Sie versuchen, eine dieser nicht unterstützten Tenancy-Änderungen vorzunehmen, wird der `InvalidRequest`-Fehlercode angezeigt.

Console

So ändern Sie Instance-Tenancy oder die Affinität

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Instances und die Instances aus, die zu ändern sind.
3. Wählen Sie Instance state (Instance-Status), Stop (Anhalten).
4. Wählen Sie bei ausgewählter Instance Aktionen, Instance-Einstellungen und Instance-Platzierung ändern.
5. Konfigurieren Sie auf der Seite Instance-Platzierung ändern Folgendes:

   - Tenancy:— Wählen Sie eine der folgenden Optionen:
     - Run a dedicated hardware instance (Eine dedizierte Hardware-Instance ausführen) — Startet die Instance als eine Dedicated Instance. Weitere Informationen finden Sie unter Amazon-EC2-Dedicated-Instances.
     - Launch the instance on a Dedicated Host (Starten der Instance auf einem) — Startet die Instance auf einem Dedicated Host mit konfigurierbarer Affinität.
   - Affinity (Affinität):— Wählen Sie eine der folgenden Optionen:
     - This instance can run on any one of my hosts (Diese Instance kann auf allen meinen Hosts ausgeführt werden) – Die Instance startet auf einem beliebigen, in Ihrem Konto verfügbaren Dedicated Host, der ihren Instance-Typ unterstützt.
     - This instance can only run on the selected host (Diese Instance kann nur auf dem ausgewählten Host gestartet werden) – Die Instance kann nur auf dem Dedicated Host ausgeführt werden, der als Target Host (Ziel-Host) bestimmt wurde.
   - Target Host (Ziel-Host) — Wählen Sie den Dedicated Host aus, auf dem die Instance ausgeführt werden muss. Falls kein Ziel-Host aufgelistet ist, verfügen Sie möglicherweise über keine verfügbaren, kompatiblen Dedicated Hosts in Ihrem Konto.

   Weitere Informationen finden Sie unter Automatische Platzierung und Host-Affinität EC2 für Amazon Dedicated Host.
6. Wählen Sie Save (Speichern) aus.

AWS CLI

So ändern Sie Instance-Tenancy oder die Affinität

Verwenden Sie den Befehl modify-instance-placement. Das folgende Beispiel ändert die Affinität der angegebenen Instance von `default` in `host` und gebt den Dedicated Host an, zu dem die Instance eine Affinität hat.

```
aws ec2 modify-instance-placement \
    --instance-id i-1234567890abcdef0 \
    --affinity host \
    --tenancy host \
    --host-id h-012a3456b7890cdef
```

PowerShell

So ändern Sie Instance-Tenancy oder die Affinität

Verwenden Sie das cmdlet Edit-EC2InstancePlacement. Das folgende Beispiel ändert die Affinität der angegebenen Instance von `default` in `host` und gebt den Dedicated Host an, zu dem die Instance eine Affinität hat.

```
Edit-EC2InstancePlacement `
    -InstanceId i-1234567890abcdef0 `
    -Affinity host `
    -Tenancy host `
    -HostId h-012a3456b7890cdef
```

Einen Amazon EC2 Dedicated Host veröffentlichen

Falls Sie keinen Dedicated Host mehr benötigen, können Sie die in dem Host ausgeführten Instances anhalten, sie in einem anderen Host starten und dann den Host freigeben.

Sämtliche auf dem Dedicated Host ausgeführten Instances müssen angehalten werden, bevor Sie den Host freigeben können. Diese Instances können auf andere Dedicated Hosts in Ihrem Konto migriert werden, damit Sie deren Nutzung fortsetzen können. Diese Schritte gelten nur für On-Demand Dedicated Hosts.

Console

So veröffentlichen Sie ein Dedicated Host

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.

3. Wählen Sie auf der Seite Dedicated Hosts den freizugebenden Dedicated Host aus.
4. Wählen Sie Actions (Aktionen), Release host (Host veröffentlichen).
5. Wählen Sie zur Bestätigung Release (Freigeben) aus.

AWS CLI

So veröffentlichen Sie ein Dedicated Host

Verwenden Sie den release-hosts.

```
aws ec2 release-hosts --host-ids h-012a3456b7890cdef
```

PowerShell

So veröffentlichen Sie ein Dedicated Host

Verwenden Sie das cmdlet Remove-EC2Host.

```
Remove-EC2Host -HostId h-012a3456b7890cdef
```

Nachdem Sie einen Dedicated Host freigegeben haben, können Sie denselben Host oder dieselbe Host-ID nicht mehr wiederverwenden. Es werden Ihnen keine On-Demand-Abrechnungstarife mehr berechnet. Der Status des Dedicated Host wird in `released` geändert, und Sie können keine Instances mehr auf diesem Host starten.

> **Note**
>
> Falls Sie vor kurzem Dedicated Hosts freigegeben haben, kann es etwas dauern, bis diese nicht mehr zu Ihrem Limit hinzugezählt werden. Während dieser Zeit können `LimitExceeded`-Fehler auftreten, wenn Sie versuchen, neue Dedicated Hosts zuzuordnen. Wenn das der Fall ist, versuchen Sie nach ein paar Minuten noch einmal, neue Hosts zuzuordnen.

Die Instances, die angehalten wurden, sind immer noch zur Verwendung verfügbar und werden auf der Seite Instances aufgeführt. Sie behalten ihre `host`-Tenancy-Einstellung.

Migrieren Sie zu Nitro-basierten Amazon EC2 Dedicated Hosts

Das Nitro-System ist eine von AWS entwickelte Sammlung von Hardware- und Softwarekomponenten, die eine hohe Leistung, Verfügbarkeit und Sicherheit ermöglichen. Dedicated Hosts auf Nitro-Basis bieten im Vergleich zu Xen-basierten Dedicated Hosts ein besseres Preis-Leistungs-Verhältnis. Wenn Sie XEN-basierte Dedicated Hosts in Ihrem Konto haben, empfehlen wir Ihnen, Ihre Workloads auf Nitro-basierte Dedicated Hosts zu migrieren. Weitere Informationen finden Sie unter AWS Nitro System.

Um von einem Xen-basierten Dedicated Host zu einem Dedicated Host auf Nitro-Basis zu migrieren, müssen Sie die Xen-basierten Instances auf Ihrem Dedicated Host zu Nitro-basierten Instance-Typen migrieren, einen neuen Dedicated Host auf Nitro-Basis zuweisen und dann Ihre migrierten Nitro-basierten Instances auf Ihren neuen Dedicated Host auf Nitro-Basis verschieben.

Dieses Thema enthält detaillierte Schritte für die Migration von XEN-basierten Dedicated Hosts zu Dedicated Hosts auf Nitro-Basis.

Schritte zur Migration

- Schritt 1: Identifizierung Ihrer Xen-basierten Dedicated Hosts
- Schritt 2: Xen-basierte Instances zu Instance-Typen auf Nitro-Basis migrieren
- Schritt 3: Zuweisung eines Dedicated Host auf Nitro-Basis
- Schritt 4: Verschiebung von migrierten Instances auf einen neuen Dedicated Host auf Nitro-Basis
- Schritt 5: Freigabe ungenutzter XEN-basierten Dedicated Host

Schritt 1: Identifizierung Ihrer Xen-basierten Dedicated Hosts

Die folgenden Dedicated Hosts basieren auf XEN und können zu Dedicated Hosts auf Nitro-Basis migriert werden.

- Allgemeine Zwecke: M3 | M4
- Für Datenverarbeitung optimiert: C3 | C4
- Arbeitsspeicheroptimiert: R3 | R4 | X1 | X1e
- Speicheroptimiert: D2 | H1 | I2 | I3
- Beschleunigte Datenverarbeitung: F1 | G3 | P2 | P3

So überprüfen Sie, ob Ihr Konto Xen-basierte Dedicated Hosts enthält

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Verwenden Sie im Suchfeld den Filter Instance-Familien, um nach den oben genannten XEN-basierten Dedicated Hosts zu suchen. Zum Beispiel Instance-Familie = m3.

Schritt 2: Xen-basierte Instances zu Instance-Typen auf Nitro-Basis migrieren

Instances, die auf Xen-basierten Dedicated Hosts ausgeführt werden, sind ebenfalls XEN-basiert. Sie müssen diese Instances zu Instance-Typen auf Nitro-Basis migrieren, bevor Sie sie auf Dedicated Hosts auf Nitro-Basis verschieben können.

> **Important**
>
> Bevor Sie mit der Migration Ihrer Instances beginnen, empfehlen wir Ihnen, Ihre Daten zu sichern. Weitere Informationen finden Sie unter Amazon EBS-Snapshots mit mehreren Volumes aus einer Amazon-Instance erstellen. EC2

So finden Sie Instances, die in Ihren XEN-basierten Dedicated Hosts ausgeführt werden

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie den XEN-basierten Host aus, den Sie migrieren möchten, und wählen Sie dann die Registerkarte Ausgeführte Instances aus. Die Registerkarte listet alle Instances auf, die in dem ausgewählten Host ausgeführt werden.

Informationen zur Migration von Linux-Instances finden Sie unter Änderungen des EC2 Amazon-Instanztyps.

Informationen zur Migration von Windows-Instances finden Sie unter Eine EC2-Windows-Instance zu einem Nitro-basierten Instance-Typ migrieren.

> **Note**
>
> Stellen Sie sicher, dass Sie Ihre Instances zu einem Instance-Typ migrieren, der dem Dedicated Host auf Nitro-Basis entspricht, zu dem Sie migrieren möchten. Wenn Sie

beispielsweise beabsichtigen, zu einem M7i Dedicated Host zu migrieren, stellen Sie sicher, dass Sie Ihre Instances auf einen M7i-Instance-Typ migrieren.

Schritt 3: Zuweisung eines Dedicated Host auf Nitro-Basis

So suchen Sie unterstützte Dedicated Hosts auf Nitro-Basis

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instance-Typen aus.
3. Wenden Sie die folgenden Filter an:
   - Hypervisor = Nitro
   - Unterstützung für Dedicated Host = wahr

Nachdem Sie einen geeigneten Instance-Typ auf Nitro-Basis gefunden haben, weisen Sie einen neuen Dedicated Host zu.

Schritt 4: Verschiebung von migrierten Instances auf einen neuen Dedicated Host auf Nitro-Basis

Nachdem Sie den Dedicated Host auf Nitro-Basis zugewiesen haben und dieser den `available`-Status erreicht hat, können Sie die Instances, die Sie zuvor auf Instance-Typen auf Nitro-Basis migriert haben, auf den neuen Dedicated Host verschieben.

So verschieben Sie Ihre Instances auf einen neuen Dedicated Host auf Nitro-Basis

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die migrierte Instance und dann Aktionen, Instance-Einstellungen und Instance-Platzierung ändern.
4. Wählen Sie für Ziel-Dedicated-Host den neuen Dedicated Host auf Nitro-Basis aus und klicken Sie dann auf Speichern.
5. Starten Sie die Instance neu. Wählen Sie die Instance und dann Instance-Status, Instance starten aus.

Schritt 5: Freigabe ungenutzter XEN-basierten Dedicated Host

Nachdem Sie Ihre Workloads vom XEN-basierten Dedicated Host auf den neuen Dedicated Host auf Nitro-Basis migriert haben, können Sie den XEN-basierten Dedicated Host freigeben, falls Sie ihn nicht mehr benötigen.

Dedicated-Host-Reservierungen für Abrechnungsrabatte bei Dedicated Hosts erwerben

Dedicated-Host-Reservierungen bieten im Vergleich mit den Preisen für On-Demand-Dedicated-Hosts einen Rabatt von bis zu 70 Prozent. Sie müssen über aktive Dedicated Hosts in Ihrem Konto verfügen, bevor Sie Dedicated-Host-Reservierungen erwerben können. Weitere Informationen finden Sie unter Dedicated Host Reservations.

Console

So kaufen Sie Reservierungen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Dedicated Hosts, Dedicated Host-Reservierungen, Purchase Dedicated Host-Reservierung (Dedicated Host-Reservierung erwerben).
3. Gehen Sie auf dem Bildschirm Angebote suchen wie folgt vor:
   a. Wählen Sie unter Instance-Familie die Instance-Familie des Dedicated Hosts aus, für den Sie die Dedicated-Host-Reservierung erwerben möchten.
   b. Wählen und konfigurieren Sie unter Zahlungsoption Ihre bevorzugte Zahlungsoption.
4. Wählen Sie Weiter aus.
5. Wählen Sie die Dedicated Hosts, die der Reservierung zugeordnet werden sollen, und wählen Sie dann Weiter aus.
6. (Optional) Weisen Sie der Dedicated-Host-Reservierung Tags zu.
7. Überprüfen Sie Ihre Bestellung und klicken Sie auf Bestellen.

AWS CLI

So kaufen Sie Reservierungen

1. Verwenden Sie den describe-host-reservation-offeringsBefehl, um die verfügbaren Angebote aufzulisten, die Ihren Anforderungen entsprechen. Das folgende Beispiele listet die Angebote auf, die Instances in der Instance-Familie `m4` unterstützen und eine einjährige Laufzeit haben.

   Die Laufzeit wird in Sekunden angegeben. Eine einjährige Laufzeit umfasst 31 536 000 Sekunden und eine dreijährige Laufzeit 94 608 000 Sekunden.

   ```
   aws ec2 describe-host-reservation-offerings \
       --filter Name=instance-family,Values=m4 \
       --max-duration 31536000
   ```

   Die Befehle geben eine Liste mit Angeboten zurück, die Ihren Kriterien entsprechen. Notieren Sie die ID des Angebots, das Sie erwerben möchten.

2. Verwenden Sie den purchase-host-reservationBefehl, um das Angebot zu erwerben und die `offeringId` im vorherigen Schritt angegebenen Informationen bereitzustellen. Im folgenden Beispiel wird die angegebene Reservierung gekauft und sie einem bestimmten Dedicated Host zugeordnet, der dem AWS Konto bereits zugewiesen ist. Außerdem wird ein Tag mit dem Schlüssel `purpose` und dem Wert von zugewiesen`production`.

   ```
   aws ec2 purchase-host-reservation \
       --offering-id hro-03f707bf363b6b324 \
       --host-id-set h-013abcd2a00cbd123 \
       --tag-specifications 'ResourceType=host-
   reservation,Tags={Key=purpose,Value=production}'
   ```

PowerShell

So kaufen Sie Reservierungen

1. Verwenden Sie das Get-EC2HostReservationOfferingCmdlet, um die verfügbaren Angebote aufzulisten, die Ihren Anforderungen entsprechen. Die folgenden Beispiele listen die Angebote auf, die Instances in der Instance-Familie `m5` unterstützen und eine einjährige Laufzeit haben.

Die Laufzeit wird in Sekunden angegeben. Eine einjährige Laufzeit umfasst 31 536 000 Sekunden und eine dreijährige Laufzeit 94 608 000 Sekunden.

```
$filter = @{Name="instance-family"; Values="m5"}
Get-EC2HostReservationOffering `
    -Filter $filter `
    -MaxDuration 31536000
```

Die Befehle geben eine Liste mit Angeboten zurück, die Ihren Kriterien entsprechen. Notieren Sie die ID des Angebots, das Sie erwerben möchten.

2. Verwenden Sie das New-EC2HostReservationCmdlet, um das Angebot zu erwerben, und geben Sie die im vorherigen Schritt angegebene Angebots-ID ein. Im folgenden Beispiel wird die angegebene Reservierung gekauft und sie einem bestimmten Dedicated Host zugeordnet, der AWS dem Konto bereits zugewiesen ist.

```
New-EC2HostReservation `
    -OfferingId hro-03f707bf363b6b324 `
    -HostIdSet h-013abcd2a00cbd123
```

Kontoübergreifendes Amazon EC2 Dedicated Host-Sharing

Dedicated Host Sharing ermöglicht es Besitzern von Dedicated Hosts, ihre Dedicated Hosts mit anderen AWS Konten oder innerhalb einer AWS Organisation zu teilen. Auf diese Weise können Sie Dedicated Hosts zentral erstellen und verwalten und den Dedicated Host für mehrere AWS Konten oder innerhalb Ihrer AWS Organisation gemeinsam nutzen.

Bei diesem Modell teilt sich das AWS Konto, dem der Dedicated Host gehört (Eigentümer), ihn mit anderen AWS Konten (Verbrauchern). Konsumenten können beim Starten der für sie freigegebenen Instances auf Dedicated Hosts so vorgehen, wie sie dies beim Starten von Instances auf Dedicated Hosts tun würden, die sie in ihrem eigenen Konto zuweisen. Der Besitzer ist für die Verwaltung des Dedicated Host und der Instances, die von ihm darin gestartet werden, verantwortlich. Besitzer können Instances, die Konsumenten auf freigegebenen Dedicated Hosts starten, nicht ändern. Konsumenten sind für die Verwaltung der Instances verantwortlich, die sie in den für sie freigegebenen Dedicated Hosts starten. Konsumenten können sich keine Instances anzeigen lassen oder ändern, die anderen Konsumenten oder dem Besitzer des Dedicated Host gehören, und sie können keine Dedicated Hosts ändern, die für sie freigegeben sind.

Ein Dedicated Host-Besitzer kann einen Dedicated Host freigeben für:

- Bestimmte AWS Konten innerhalb oder außerhalb der AWS Organisation
- Eine Organisationseinheit innerhalb ihrer AWS Organisation
- Es ist die gesamte AWS Organisation

Inhalt

- Voraussetzungen für die Freigabe von Dedicated Hosts
- Einschränkungen für die Freigabe von Dedicated Hosts
- Zugehörige Services
- Freigeben in mehreren Availability Zones
- Berechtigungen für freigegebene Dedicated Host
- Fakturierung und Messung
- Dedicated Host-Limits
- Hostwiederherstellung und Dedicated Host-Freigabe
- Einen Amazon EC2 Dedicated Host für mehrere AWS Konten teilen
- Hebt die Freigabe eines Dedicated Hosts auf, der mit anderen Konten gemeinsam genutzt wurde AWS
- Geteilte Amazon EC2 Dedicated Hosts in Ihrem AWS Konto anzeigen

Voraussetzungen für die Freigabe von Dedicated Hosts

- Um einen Dedicated Host zu teilen, musst du ihn in deinem AWS Konto besitzen. Sie können keinen Dedicated Host freigeben, der für Sie freigegeben wurde.
- Um einen Dedicated Host mit deiner AWS Organisation oder einer Organisationseinheit in deiner AWS Organisation zu teilen, musst du das Teilen mit aktivieren AWS Organizations. Weitere Informationen finden Sie unter Freigabe für AWS Organizations aktivieren im AWS RAM - Benutzerhandbuch.

Einschränkungen für die Freigabe von Dedicated Hosts

Sie können Dedicated Hosts nicht freigeben, die für die folgenden Instance-Typen zugewiesen wurden: `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` und `u-24tb1.metal`.

Zugehörige Services

AWS Resource Access Manager

Die gemeinsame Nutzung von Dedicated Hosts ist in AWS Resource Access Manager (AWS RAM) integriert. AWS RAM ist ein Dienst, mit dem Sie Ihre AWS Ressourcen mit einem beliebigen AWS Konto oder über dieses teilen können AWS Organizations. Mit können Sie Ressourcen AWS RAM, die Ihnen gehören, gemeinsam nutzen, indem Sie eine gemeinsame Nutzung erstellen. Eine Ressourcenfreigabe legt die freizugebenden Ressourcen und die Konsumenten fest, für die sie freigegeben werden sollen. Bei Verbrauchern kann es sich um einzelne AWS Konten, Organisationseinheiten oder eine gesamte Organisation handeln AWS Organizations.

Weitere Informationen zu AWS RAM finden Sie im AWS RAM Benutzerhandbuch.

Freigeben in mehreren Availability Zones

Um sicherzustellen, dass Ressourcen auf die Availability Zones einer Region verteilt sind, ordnen wir Availability Zones einzeln Namen für jedes Konto zu. Dies könnte zu in mehreren Konten unterschiedlich benannten Availability Zones führen. Beispielsweise hat die Availability Zone `us-east-1a` für Ihr AWS Konto möglicherweise nicht denselben Standort wie `us-east-1a` für ein anderes AWS Konto.

Um den Ort Ihrer Dedicated Hosts relativ zu Ihren Konten zu bestimmen, verwenden Sie die Availability-Zone-ID (AZ-ID). Die Availability Zone ID ist eine eindeutige und konsistente Kennung für eine Availability Zone für alle AWS Konten. Beispielsweise ist `use1-az1` eine Availability-Zone-ID für die `us-east-1`-Region und ist derselbe Speicherort in jedem AWS -Konto.

Um die Availability Zone IDs für die Availability Zones in Ihrem Konto anzuzeigen

1. Öffnen Sie die AWS RAM Konsole zu https://console.aws.amazon.com/ram/Hause.
2. Die Availability Zone IDs für die aktuelle Region wird im Bereich „Ihre AZ-ID“ auf der rechten Seite des Bildschirms angezeigt.

Berechtigungen für freigegebene Dedicated Host

Berechtigungen für Besitzer

Besitzer sind verantwortlich für die Verwaltung ihrer freigegebenen Dedicated Hosts und der Instances, die sie auf ihnen starten. Besitzer können sich alle Instances anzeigen lassen, die auf dem freigegebenen Dedicated Host ausgeführt werden, dazu gehören auch die von Konsumenten

gestarteten. Besitzer können jedoch keine Maßnahmen für ausgeführte Instances ergreifen, die von Konsumenten gestartet wurden.

Berechtigungen für Konsumenten

Konsumenten sind für die Verwaltung der Instances verantwortlich, die sie in dem für sie freigegebenen Dedicated Host starten. Konsumenten können den freigegebenen Dedicated Host keinesfalls ändern und können keine Instances anzeigen oder bearbeiten, die von anderen Konsumenten oder dem Dedicated Host-Besitzer gestartet wurden.

Fakturierung und Messung

Für die Freigabe von Dedicated Hosts fallen keine zusätzlichen Gebühren an.

Besitzern werden die Dedicated Hosts in Rechnung gestellt, die sie freigeben. Konsumenten werden keine Instances in Rechnung gestellt, die sie auf freigegebenen Dedicated Hosts starten.

Dedicated Host-Reservierungen bieten weiterhin Abrechnungsrabatte für freigegebene Dedicated Hosts. Nur Dedicated Host-Besitzer können Dedicated Host-Reservierungen für freigegebene Dedicated Hosts kaufen, die sie besitzen.

Dedicated Host-Limits

Freigegebene Dedicated Hosts werden nur auf die Dedicated Hosts-Limits des Besitzers angerechnet. Die Dedicated Hosts-Limits von Konsumenten sind nicht von Dedicated Hosts betroffen, die ihnen freigegeben wurden. Ebenso werden Instances, die Konsumenten auf freigegebenen Dedicated Hosts starten, nicht auf ihre Instance-Limits angerechnet.

Hostwiederherstellung und Dedicated Host-Freigabe

Die Hostwiederherstellung stellt Instances wieder her, die vom Dedicated Host-Besitzer und den Konsumenten gestartet wurden, für die er freigegeben wurde. Der Ersatz-Dedicated Host wird dem Konto des Besitzers zugeordnet. Er wird zu den gleichen Ressourcenfreigaben wie der ursprüngliche Dedicated Host hinzugefügt und den gleichen Konsumenten freigegeben.

Weitere Informationen finden Sie unter Wiederherstellung von Amazon EC2 Dedicated Host.

Einen Amazon EC2 Dedicated Host für mehrere AWS Konten teilen

Gibt ein Besitzer einen Dedicated Host frei, können Konsumenten Instances auf dem Host starten. Konsumenten können so viele Instances auf dem freigegebenen Host starten, wie es die verfügbare Kapazität zulässt.

> **Important**
>
> Beachten Sie, dass Sie dafür verantwortlich sind, sicherzustellen, dass Sie über die entsprechenden Lizenzrechte verfügen, um BYOL-Lizenzen auf Ihren Dedicated Hosts freizugeben.

Wenn Sie einen Dedicated Host freigeben, bei dem die automatische Platzierung aktiviert ist, beachten Sie Folgendes, da dies zu einer unbeabsichtigten Dedicated Host-Nutzung führen könnte:

- Wenn Konsumenten Instances mit Dedicated Host-Tenancy starten und über keine Kapazität auf einem Dedicated Host verfügen, den sie in ihrem Konto besitzen, wird die Instance automatisch auf dem freigegebenen Dedicated Host gestartet.

Um einen Dedicated Host freigeben zu können, müssen Sie ihn einer Ressourcenfreigabe hinzufügen. Eine gemeinsame Nutzung von Ressourcen ist eine AWS RAM Ressource, mit der Sie Ihre Ressourcen AWS kontenübergreifend teilen können. Eine Ressourcenfreigabe gibt die freizugebenden Ressourcen und die Konsumenten an, für die sie freigegeben werden. Sie können den Dedicated Host zu einer vorhandenen Ressource oder zu einer neuen Ressourcenfreigabe hinzufügen.

Wenn du Teil einer Organisation bist AWS Organizations und das Teilen innerhalb deiner Organisation aktiviert ist, erhalten Verbraucher in deiner Organisation automatisch Zugriff auf den gemeinsam genutzten Dedicated Host. Andernfalls erhalten Konsumenten eine Einladung zur Teilnahme an der Ressourcenfreigabe und nach Annahme der Einladung wird ihnen Zugriff auf den freigegebenen Dedicated Host gewährt.

> **Note**
>
> Nach der Freigabe eines Dedicated Host kann es einige Minuten dauern, bis Konsumenten darauf zugreifen können.

Console

Um einen Dedicated Host, den Sie besitzen, über die EC2 Amazon-Konsole zu teilen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie den Dedicated Host aus, der freigegeben werden soll, und wählen Sie Aktionen, Host freigeben aus.
4. Wählen Sie die Ressourcenfreigabe aus, der der Dedicated Host hinzugefügt werden soll, aus und wählen Sie dann Freigeben aus.

   Es kann einige Minuten dauern, bis Konsumenten Zugriff auf den freigegebenen Host gewährt wird.

Um einen Dedicated Host, den Sie besitzen, über die AWS RAM Konsole gemeinsam zu nutzen

Weitere Informationen finden Sie unter Erstellen einer Ressourcenfreigabe im AWS RAM - Benutzerhandbuch.

AWS CLI

So können Sie einen Dedicated Host in Ihrem Besitz freigeben

Verwenden Sie den Befehl create-resource-share.

```
aws ram create-resource-share \
    --name my-resource-share \
    --resource-arns arn:aws:ec2:us-east-2:123456789012:dedicated-
host/h-07879acf49EXAMPLE
```

PowerShell

So können Sie einen Dedicated Host in Ihrem Besitz freigeben

Verwenden Sie das Cmdlet New- RAMResource Share.

```
New-RAMResourceShare `
    -Name my-resource-share `
    -ResourceArn arn:aws:ec2:us-east-2:123456789012:dedicated-
host/h-07879acf49EXAMPLE
```

Hebt die Freigabe eines Dedicated Hosts auf, der mit anderen Konten gemeinsam genutzt wurde AWS

Der Dedicated Host-Besitzer kann die Freigabe eines freigegebenen Dedicated Host jederzeit aufheben. Wenn Sie die Freigabe eines freigegebenen Dedicated Host aufheben, gelten die folgenden Regeln:

- Verbraucher, für die der Dedicated Host freigegeben wurde, können darauf keine neuen Instances mehr starten.
- Instances im Besitz von Konsumenten, die zum Zeitpunkt der Freigabe auf dem Dedicated Host ausgeführt wurden, werden weiterhin ausgeführt, sind jedoch für die Ausmusterung vorgesehen. Konsumenten erhalten für die Instances Benachrichtigungen über die Ausmusterung und haben zwei Wochen Zeit, um entsprechende Maßnahmen zu ergreifen. Wird der Dedicated Host dem Konsumenten jedoch innerhalb der Ausmusterungsbenachrichtigungszeitraums erneut freigegeben, erfolgt ein Abbruch der Instance-Ausmusterungen.

Um die Freigabe eines freigegebenen Dedicated Host in Ihrem Besitz aufheben zu können, müssen Sie ihn aus der Ressourcenfreigabe entfernen.

Console

So heben Sie die Freigabe eines Dedicated Host in Ihrem Besitz auf

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie den Dedicated Host aus, dessen Freigabe aufgehoben werden soll, und wählen Sie dann die Registerkarte Freigabe aus.
4. Auf der Registerkarte Freigabe werden die Ressourcenfreigaben aufgelistet, zu denen der Dedicated Host hinzugefügt wurde. Wählen Sie die Ressourcenfreigabe aus, aus der der Dedicated Host entfernt werden soll, und wählen Sie Host aus Ressourcenfreigabe entfernen aus.

Um die Freigabe eines gemeinsam genutzten Dedicated Hosts, den Sie besitzen, mithilfe der AWS RAM Konsole rückgängig zu machen

Weitere Informationen finden Sie unter Aktualisieren einer Ressourcenfreigabe im AWS RAM - Benutzerhandbuch.

AWS CLI

So heben Sie die Freigabe eines Dedicated Host in Ihrem Besitz auf

Verwenden Sie den Befehl disassociate-resource-share.

```
aws ram disassociate-resource-share \
    --resource-share-arn arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
 --resource-arns arn:aws:ec2:us-east-2:123456789012:dedicated-host/h-07879acf49EXAMPLE
```

PowerShell

So heben Sie die Freigabe eines Dedicated Host in Ihrem Besitz auf

Verwenden Sie das Cmdlet Disconnect- RAMResource Share.

```
Disconnect-RAMResourceShare `
    -ResourceShareArn "arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE" `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:dedicated-host/h-07879acf49EXAMPLE"
```

Geteilte Amazon EC2 Dedicated Hosts in Ihrem AWS Konto anzeigen

Sie können Dedicated Hosts, die Sie für andere Konten freigeben, und Dedicated Hosts, die für Sie freigegeben sind, anzeigen. Wenn Sie der Eigentümer des Dedicated Host sind, können Sie alle Instances anzeigen, die auf dem Host ausgeführt werden, einschließlich der von Verbrauchern gestarteten Instances. Wenn der Dedicated Host für Sie freigegeben wird, können Sie nur die Instances anzeigen, die Sie auf dem freigegebenen Host gestartet haben, und nicht die Instances, die von anderen Verbrauchern gestartet wurden.

Besitzer und Konsumenten können freigegebene Dedicated Hosts mit einer der folgenden Methoden identifizieren.

Console

So identifizieren Sie einen freigegebenen Dedicated Host

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Dedicated Hosts aus. Im Bildschirm werden die Dedicated Hosts in Ihrem Besitz und Dedicated Hosts, die für Sie freigegeben werden, aufgelistet.
3. In der Spalte Owner (Besitzer) wird die AWS -Konto-ID des Dedicated Host-Besitzers angezeigt.
4. Um die auf den Hosts ausgeführten Instances anzuzeigen, wählen Sie die Registerkarte Instances aus.

AWS CLI

So identifizieren Sie einen freigegebenen Dedicated Host

Verwenden Sie den Befehl describe-hosts. Der Befehl gibt die Dedicated Hosts zurück, die Sie besitzen und die Dedicated Hosts, die für Sie freigegeben sind. Der Wert von `Owner` ist die Konto-ID des Besitzers des Dedicated Host. Die `Instances`-Liste beschreibt die Instances, die auf dem Host ausgeführt werden.

```
aws ec2 describe-hosts --filter "Name=state,Values=available"
```

PowerShell

So identifizieren Sie einen freigegebenen Dedicated Host

Verwenden Sie das EC2host Cmdlet Get-. Das cmdlet gibt die Dedicated Hosts zurück, die Sie besitzen und die Dedicated Hosts, die für Sie freigegeben sind. Der Wert von `Owner` in der Antwort ist die Konto-ID des Besitzers des Dedicated Host. Die `Instances`-Liste beschreibt die Instances, die auf dem Host ausgeführt werden.

```
Get-EC2Host -Filter @{Name="state"; Values="available"}
```

Amazon EC2 Dedicated Hosts auf AWS Outposts

AWS Outposts ist ein vollständig verwalteter Service, der AWS Infrastruktur APIs, Dienste und Tools auf Ihre Räumlichkeiten ausdehnt. Durch den lokalen Zugriff auf die AWS verwaltete Infrastruktur AWS Outposts können Sie Anwendungen vor Ort mit denselben Programmierschnittstellen wie in AWS Regionen erstellen und ausführen und gleichzeitig lokale Rechen- und Speicherressourcen für geringere Latenz und lokale Datenverarbeitungsanforderungen nutzen.

Ein Outpost ist ein Pool von AWS Rechen- und Speicherkapazität, der am Standort eines Kunden bereitgestellt wird. AWS betreibt, überwacht und verwaltet diese Kapazität als Teil einer AWS Region.

Sie können Dedicated Hosts auf Outposts zuweisen, die Sie in Ihrem Konto besitzen. Dies erleichtert es Ihnen, Ihre vorhandenen Softwarelizenzen und Workloads, die einen dedizierten physischen Server erfordern, nach AWS Outposts zu bringen. Sie können auch auf bestimmte Hardwareressourcen auf einem Outpost ausrichten, um die Latenz zwischen Ihren Workloads zu minimieren.

Dedicated Hosts ermöglichen es Ihnen, Ihre in Frage kommenden Softwarelizenzen bei Amazon zu verwenden EC2, sodass Sie die Flexibilität und Kosteneffizienz nutzen können, die Sie mit Ihren eigenen Lizenzen gewohnt sind. Andere Softwarelizenzen, die an virtuelle Maschinen, Sockets oder physische Kerne gebunden sind, können vorbehaltlich ihrer Lizenzbedingungen auch auf Dedicated Hosts verwendet werden. Während Outposts schon immer eine Einzelmandanten-Umgebung waren, die für BYOL-Workloads in Frage kommen, können Sie mit Dedicated Hosts die erforderlichen Lizenzen auf einen einzelnen Host im Gegensatz zur gesamten Outpost-Bereitstellung beschränken.

Darüber hinaus bietet Ihnen die Verwendung von Dedicated Hosts in einem Outpost eine größere Flexibilität bei der Instance-Typ-Bereitstellung und eine detailliertere Kontrolle über die Platzierung von Instances. Sie können beispielsweise auf einen bestimmten Host zielen und Host-Affinität verwenden, um sicherzustellen, dass die Instance immer auf diesem Host ausgeführt wird oder Sie können die automatische Platzierung verwenden, um eine Instance auf jedem verfügbaren Host zu starten, der über übereinstimmende Konfigurationen und verfügbare Kapazität verfügt.

Inhalt

- Voraussetzungen
- Unterstützte Features
- Überlegungen
- Ordnen Sie einen Amazon EC2 Dedicated Host zu AWS Outposts

Voraussetzungen

Sie müssen einen Outpost an Ihrem Standort installiert haben. Weitere Informationen finden Sie unter Outpost erstellen und die Kapazität dafür bestellen im AWS Outposts -Benutzerhandbuch.

Unterstützte Features

- Die folgenden Instance-Familien werden unterstützt: `C5`, `M5`, `R5`, `C5d`, `M5d`, `R5d`, `G4dn` und `i3en`.

- Dedicated Hosts on Outposts können so konfiguriert werden, dass sie mehrere Instance-Größen unterstützen. Unterstützung für mehrere Instance-Größen ist für die folgenden Instance-Familien verfügbar: `C5`, `M5`, `R5`, `C5d`, `M5d` und `R5d`. Weitere Informationen finden Sie unter Kapazitätskonfigurationen EC2 für Amazon Dedicated Host-Instances.
- Dedicated Hosts on Outposts unterstützen die automatische Platzierung und gezielte Instance-Starts. Weitere Informationen finden Sie unter Automatische Platzierung und Host-Affinität EC2 für Amazon Dedicated Host.
- Dedicated Hosts auf Outposts unterstützen Host-Affinität. Weitere Informationen finden Sie unter Automatische Platzierung und Host-Affinität EC2 für Amazon Dedicated Host.
- Dedizierte Hosts auf Outposts unterstützen das Teilen mit AWS RAM. Weitere Informationen finden Sie unter Kontoübergreifendes Amazon EC2 Dedicated Host-Sharing.

Überlegungen

- Dedicated-Host-Reservierungen werden auf Outposts nicht unterstützt.
- Hosten Ressourcengruppen und AWS License Manager werden auf Outposts nicht unterstützt.
- Dedicated Hosts auf Outposts unterstützen keine Burstable T3-Instances.
- Dedicated Hosts auf Outposts unterstützen keine Host-Wiederherstellung.
- Die vereinfachte automatische Wiederherstellung wird für Instances mit Dedicated-Host-Tenancy auf Outposts nicht unterstützt.

Ordnen Sie einen Amazon EC2 Dedicated Host zu AWS Outposts

Sie weisen Dedicated Hosts auf Outposts auf die gleiche Weise zu und verwenden sie wie bei Dedicated Hosts in einer AWS -Region.

Voraussetzungen

Erstellen Sie ein Subnetz auf dem Outpost. Weitere Informationen finden Sie unter Erstellen eines Subnetzes im AWS Outposts -Benutzerhandbuch.

Verwenden Sie eine der folgenden Methoden, um einen Dedicated Host für einen Outpost zuzuweisen:

Console

Um einem Außenposten mithilfe der Konsole einen Dedicated Host zuzuweisen AWS Outposts

1. Öffnen Sie die AWS Outposts Konsole unter. https://console.aws.amazon.com/outposts/
2. Wählen Sie im Navigationsbereich Outposts aus. Wählen Sie den Outpost aus und wählen Sie dann Actions (Aktionen), Allocate Dedicated Host (Dedicated Host zuweisen).
3. Konfigurieren Sie den Dedicated Host nach Bedarf. Weitere Informationen finden Sie unter Weisen Sie Ihrem Konto einen Amazon EC2 Dedicated Host zu.

> **Note**
>
> Availability Zone (Verfügbarkeitszone) und Outpost ARN (Outpost-ARN) sollte mit der Availability Zone und dem ARN des ausgewählten Outposts vorausgefüllt werden.

4. Wählen Sie Allocate aus.

So weisen Sie einem Outpost mithilfe der Amazon-Konsole einen Dedicated Host zu EC2

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts und dann Allocate Dedicated Host (Dedicated Host zuweisen) aus.
3. Als Availability Zon (Verfügbarkeitszone) wählen Sie die Availability Zone aus, die dem Outpost zugewiesen ist.
4. Als Outpost ARN (Outpost-ARN) geben Sie den ARN des Outposts ein.
5. Um auf bestimmte Hardwareressourcen auf dem Outpost auszurichten, wählen Sie für Gezielt auf spezifische Hardwareressourcen auf Outpost ausrichten die Option Aktivieren aus. Wählen Sie für jede Hardwareressource, die Sie als Ziel verwenden möchten, Ressourcen-ID hinzufügen aus, und geben Sie dann die ID der Hardwareressource ein.

> **Note**
>
> Der Wert, den Sie für Menge angeben, muss der Anzahl der von IDs Ihnen angegebenen Anlagen entsprechen. Wenn Sie beispielsweise 3 Anlagen angeben IDs, muss auch Menge den Wert 3 haben.

6. Konfigurieren Sie die verbleibenden Dedicated-Host-Einstellungen nach Bedarf. Weitere Informationen finden Sie unter Weisen Sie Ihrem Konto einen Amazon EC2 Dedicated Host zu.
7. Wählen Sie Allocate aus.

AWS CLI

So weisen Sie einen Dedicated Host auf einem Outpost zu

Verwenden Sie den allocate-hosts-Befehl. Geben Sie bei `--availability-zone` die Availability Zone an, die dem Outpost zugewiesen ist. Geben Sie bei `--outpost-arn` den ARN des Ouposts an. Geben Sie optional für `--asset-ids` die IDs Outpost-Hardwareressourcen an, auf die Sie abzielen möchten.

```
aws ec2 allocate-hosts \
    --availability-zone "us-east-1a" \
    --outpost-arn "arn:aws:outposts:us-east-1a:111122223333:outpost/
op-4fe3dc21baEXAMPLE" \
    --asset-ids asset_id \
    --instance-family "m5" \
    --auto-placement "off" \
    --quantity 1
```

PowerShell

So weisen Sie einen Dedicated Host auf einem Outpost zu

Verwenden Sie das cmdlet New-EC2Host. Geben Sie die Availability Zone an, die dem Outpost zugewiesen ist. Geben Sie optional für die IDs Outpost-Hardwareressourcen an`-AssetId`, auf die Sie abzielen möchten.

```
New-EC2Host `
    -AvailabilityZone "us-east-1a" `
    -OutpostArn "arn:aws:outposts:us-east-1a:111122223333:outpost/
op-4fe3dc21baEXAMPLE" `
    -AssetId asset_id `
    -InstanceFamily "m5" `
    -AutoPlacement "off" `
    -Quantity 1
```

So starten Sie eine Instance in einem Dedicated Host auf einem Outpost

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus. Wählen Sie den Dedicated Host aus, den Sie im vorherigen Schritt zugewiesen haben, und wählen Sie Actions (Aktionen), Launch instance onto host (Instance auf Host launchen).
3. Konfigurieren Sie die Instance nach Bedarf und launchen Sie dann die Instance. Weitere Informationen finden Sie unter Starten Sie EC2 Amazon-Instances auf einem Amazon EC2 Dedicated Host.

Wiederherstellung von Amazon EC2 Dedicated Host

Die automatische Wiederherstellung des Dedicated Hosts startet Ihre Instances auf einem neuen Ersatzhost neu, wenn bestimmte problematische Bedingungen auf Ihrem Dedicated Host erkannt werden. Die Host-Wiederherstellung reduziert den Bedarf an manuellen Eingriffen und verringert die Betriebsbelastung, wenn ein unerwarteter Ausfall des Dedicated Hosts im Zusammenhang mit Systemstrom- oder Netzwerkkonnektivitätsereignissen auftritt. Andere Dedicated-Host-Probleme erfordern manuelle Eingriffe, um sie zu beheben.

Inhalt

- So funktioniert Amazon EC2 Dedicated Host-Wiederherstellung
- Unterstützte Instance-Typen
- Preisgestaltung
- Amazon EC2 Dedicated Host-Wiederherstellung verwalten
- Sehen Sie sich die Host-Wiederherstellungseinstellungen für Ihren Amazon EC2 Dedicated Host an
- Manuelles Wiederherstellen von Instances, die von Amazon EC2 Dedicated Host Recovery nicht unterstützt werden

So funktioniert Amazon EC2 Dedicated Host-Wiederherstellung

Dedicated Hosts und der Wiederherstellungsprozess von Hostressourcengruppen verwenden Zustandsprüfungen auf Hostebene, um die Verfügbarkeit von Dedicated Hosts zu bewerten und zugrunde liegende Systemfehler zu erkennen. Die Art des Dedicated-Host-Fehlers bestimmt, ob die automatische Wiederherstellung des Dedicated Hosts möglich ist. Zu den Problemen, die zu Prüfungen auf Hostebene führen können, zählen:

- Verlust der Netzwerkverbindung
- Systemstromausfall
- Hardware- oder Softwareprobleme auf dem physischen Host

> **Important**
>
> Die automatische Wiederherstellung eines Dedicated Hosts findet nicht statt, wenn der Host für die Außerbetriebnahme vorgesehen ist.

Automatische Wiederherstellung für Dedicated Hosts

Wenn auf Ihrem Dedicated Host ein Ausfall der Systemleistung oder der Netzwerkverbindung festgestellt wird, wird die auto Wiederherstellung des Dedicated Hosts eingeleitet und Amazon weist EC2 automatisch einen Ersatz-Dedicated Host in derselben Availability Zone wie der ursprüngliche Dedicated Host zu. Dieser Dedicated Host erhält eine neue Host-ID, hat aber dieselben Attribute wie der ursprüngliche Dedicated Host, einschließlich:

- Availability Zone
- Instance-Typ
- Tags (Markierungen)
- Einstellungen zur automatischen Platzierung
- Reservation (Reservierung)

Nachdem der ersatzmäßige Dedicated Host zugeordnet wurde, werden die Instances auf dem ersatzmäßigen Dedicated Host wiederhergestellt. Die wiederhergestellten Instances haben dieselben Attribute wie der ursprüngliche Host, einschließlich:

- Instance-ID
- Private IP-Adressen
- Elastic IP-Adressen
- EBS-Volume-Anhänge
- Alle Instance-Metadaten

Darüber hinaus automatisiert die integrierte Integration mit AWS License Manager die Nachverfolgung und Verwaltung Ihrer Lizenzen.

> **Note**
>
> AWS Die License Manager-Integration wird nur in Regionen unterstützt, in denen AWS License Manager verfügbar ist.

Wenn zwischen den Instances und dem nicht funktionierenden Dedicated Host eine Affinitätsbeziehung besteht, richten die wiederhergestellten Instances eine Host-Affinität mit dem ersatzmäßigen Dedicated Host ein.

Wenn alle Instances auf dem ersatzmäßigen Dedicated Host wiederhergestellt wurden, wird der beeinträchtigte Dedicated Host freigegeben und der ersatzmäßige Dedicated Host kann verwendet werden.

Wenn die Host-Wiederherstellung eingeleitet wird, wird der AWS Kontoinhaber per E-Mail und durch ein AWS Health Dashboard Ereignis benachrichtigt. Nachdem die Host-Wiederherstellung erfolgreich durchgeführt wurde, wird eine zweite Benachrichtigung gesendet.

Wenn Sie AWS License Manager verwenden, um Ihre Lizenzen nachzuverfolgen, weist AWS License Manager neue Lizenzen für den Ersatz-Dedicated Host auf der Grundlage der Lizenzkonfigurationslimits zu. Wenn die Lizenzkonfiguration feste Grenzwerte hat, die durch die Host-Wiederherstellung überschritten werden, ist der Wiederherstellungsprozess nicht zulässig und Sie werden über eine Amazon SNS SNS-Benachrichtigung über den Fehler bei der Host-Wiederherstellung informiert (sofern die Benachrichtigungseinstellungen für AWS License Manager konfiguriert wurden). Gelten für die Lizenzkonfiguration weiche Limits, die aufgrund der Host-Wiederherstellung überschritten werden, kann der Wiederherstellungsprozess fortgesetzt werden und Sie werden per Amazon SNS-Benachrichtigung über die Limit-Überschreitung informiert. Weitere Informationen finden Sie unter Verwenden von Lizenzkonfigurationen und Einstellungen in License Manager im AWS -License-Manager-Benutzerhandbuch.

Status der Host-Wiederherstellung

Wird ein Dedicated Host-Ausfall entdeckt, wechselt der beeinträchtigte Dedicated Host in den Status „`under-assessment`“ und die betroffenen Instances in den Status „`impaired`“. Sie können keine Instances auf dem gestörten Dedicated Host starten, während er sich im Status `under-assessment` befindet.

Nachdem der ersatzmäßige Dedicated Host zugeordnet wurde, wechselt er in den Status `pending`. Er bleibt in diesem Status, bis die Host-Wiederherstellung abgeschlossen ist. Sie können keine Instances auf den Ersatz-Dedicated Host starten, während er sich im Status `pending` befindet. Wiederhergestellte Instances auf dem ersatzmäßigen Dedicated Host verbleiben während der Wiederherstellung im Status `impaired`.

Nach Abschluss der Host-Wiederherstellung wechselt der ersatzmäßige Dedicated Host in den Status `available` und die wiederhergestellten Instances erhalten wieder den Status `running`. Sie können Instances auf dem ersatzmäßigen Dedicated Host starten, sobald dieser wieder den Status `available` hat. Der ursprüngliche, beeinträchtigte Dedicated Host wird dauerhaft freigegeben und wechselt in den Status `released-permanent-failure`.

Verfügt der beeinträchtigte Dedicated Host über Instances, die keine Host-Wiederherstellung unterstützen, beispielsweise solche mit Instance-Speicher-Root-Volumes, wird der Dedicated Host nicht freigegeben. Stattdessen wird er für die Ausmusterung gekennzeichnet und erhält den Status `permanent-failure`.

Szenarien ohne automatische Wiederherstellung für Dedicated Hosts

Die automatische Wiederherstellung eines Dedicated Hosts findet nicht statt, wenn der Host für die Außerbetriebnahme vorgesehen ist. Sie erhalten im Rahmen eines CloudWatch Amazon-Events eine Benachrichtigung zur Kündigung, und die E-Mail-Adresse des AWS Kontoinhabers erhält eine Nachricht über den Ausfall des Dedicated Hosts. AWS Health Dashboard Führen Sie die in der Benachrichtigung über die Außerbetriebnahme beschriebenen Abhilfemaßnahmen innerhalb der angegebenen Zeitspanne durch, um die Instances auf dem außerbetriebgenommenen Host manuell wiederherzustellen.

Angehaltene Instances werden auf dem Dedicated Host nicht wiederhergestellt. Wenn Sie versuchen, eine angehaltene Instance zu starten, die auf den beeinträchtigten Dedicated Host ausgerichtet ist, schlägt der Start fehl. Wir empfehlen, die angehaltene Instance so zu ändern, dass sie auf einen anderen Dedicated Host ausgerichtet ist oder so, dass sie auf einem verfügbaren Dedicated Host mit passender Konfiguration und aktivierter automatischer Platzierung gestartet wird.

Instances mit Instance-Speicher werden auf dem Ersatz-Dedicated Host nicht wiederhergestellt. Im Rahmen einer Korrekturmaßnahme wird der beeinträchtigte Dedicated Host für die Ausmusterung gekennzeichnet und Sie erhalten eine entsprechende Benachrichtigung, wenn die Host-Wiederherstellung abgeschlossen ist. Befolgen Sie die Korrekturmaßnahmen aus der Benachrichtigung innerhalb des angegebenen Zeitraums, um die verbliebenen Instances auf dem beeinträchtigten Dedicated Host wiederherzustellen.

Unterstützte Instance-Typen

Host-Wiederherstellung wird für die folgenden Instance-Familien unterstützt: A1 | C3 | C4 | C5 | C5n | C6a | C6g | C6i | Inf1 | G3 | G5g | M3 | M4 | M5 | M5n | M5zn | M6a | M6g | M6i | Mac1 | Mac2 | Mac2-m1ultra | Mac2-m2 | Mac2-m2pro | P2 | P3 | R3 | R4 | R5 | R5b | R5n | R6g | R6i | T3 | X1 | X1e | X2iezn | u-6tb1 | u-9tb1 | u-12tb1 | u-18tb1 | u-24tb1.

Informationen zum Wiederherstellen nicht unterstützter Instances finden Sie unter Manuelles Wiederherstellen von Instances, die von Amazon EC2 Dedicated Host Recovery nicht unterstützt werden.

> **Note**
>
> Die automatische Wiederherstellung von unterstützten Metal-Instance-Typen für Dedicated Hosts dauert länger als die von Nicht-Metal-Instance-Typen zum Erkennen und Wiederherstellen.

Preisgestaltung

Für die Host-Wiederherstellung fallen keine weiteren Kosten an. Es gelten die üblichen Dedicated Host-Gebühren. Weitere Informationen finden Sie unter Amazon EC2 Dedicated Hosts — Preise.

Sobald die Host-Wiederherstellung gestartet wurde, fallen keine Gebühren mehr für den beeinträchtigten Dedicated Host an. Kosten für den ersatzmäßigen Dedicated Host fallen erst an, wenn er den Status `available` hat.

Wenn der beeinträchtigte Dedicated Host nach Bedarf abgerechnet wurde, wird der ersatzmäßige Dedicated Host ebenso abgerechnet. Verfügte der beeinträchtigte Dedicated Host über einen aktiven Dedicated Host-Reservierung, wird er an den ersatzmäßigen Dedicated Host weitergegeben.

Amazon EC2 Dedicated Host-Wiederherstellung verwalten

Die automatische Wiederherstellung des Dedicated Hosts startet Ihre Instances auf einem neuen Ersatzhost neu, wenn bestimmte problematische Bedingungen auf Ihrem Dedicated Host erkannt werden. Sie können die Host-Wiederherstellung zum Zeitpunkt der Dedicated-Host-Zuordnung oder hinterher aktivieren.

Verwenden Sie die folgenden Verfahren, um die Host-Wiederherstellung bei der Host-Zuweisung zu aktivieren.

Console

So aktivieren Sie die Host-Wiederherstellung bei der Zuweisung

Wenn Sie über die EC2 Amazon-Konsole einen Dedicated Host zuweisen, wählen Sie für Host-Wiederherstellung die Option Enable. Weitere Informationen finden Sie unter Weisen Sie Ihrem Konto einen Amazon EC2 Dedicated Host zu.

AWS CLI

So aktivieren Sie die Host-Wiederherstellung bei der Zuweisung

Verwenden Sie den allocate-hosts-Befehl.

```
aws ec2 allocate-hosts \
    --instance-type m5.large \
    --availability-zone eu-west-1a \
    --auto-placement on \
    --host-recovery on \
    --quantity 1
```

PowerShell

So aktivieren Sie die Host-Wiederherstellung bei der Zuweisung

Verwenden Sie das cmdlet New-EC2Host.

```
New-EC2Host `
    -InstanceType m5.large `
    -AvailabilityZone eu-west-1a `
    -AutoPlacement on `
    -HostRecovery on `
    -Quantity 1
```

Verwenden Sie die folgenden Verfahren, um die Host-Wiederherstellung für einen Dedicated Host zu verwalten.

Console

So aktivieren Sie die Host-Wiederherstellung nach der Zuweisung

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie den Dedicated Host aus.
4. Wählen Sie Aktionen und anschließend Host ändern aus.
5. Wählen oder deaktivieren Sie für die Host-Wiederherstellung die Option Aktivieren.
6. Wählen Sie Speichern.

AWS CLI

So aktivieren Sie die Host-Wiederherstellung nach der Zuweisung

Verwenden Sie den modify-hosts-Befehl.

```
aws ec2 modify-hosts \
    --host-recovery on \
    --host-ids h-012a3456b7890cdef
```

So deaktivieren Sie die Host-Wiederherstellung nach der Zuweisung

Verwenden Sie den Befehl modify-hosts und geben Sie den Parameter `host-recovery` mit einem Wert von `off` an.

```
aws ec2 modify-hosts \
    --host-recovery off \
    --host-ids h-012a3456b7890cdef
```

PowerShell

So aktivieren Sie die Host-Wiederherstellung nach der Zuweisung

Verwenden Sie das cmdlet Edit-host.

```
Edit-EC2Host `
    -HostRecovery on `
    -HostId h-012a3456b7890cdef
```

So deaktivieren Sie die Host-Wiederherstellung nach der Zuweisung

Verwenden Sie das cmdlet Edit-EC2Host.

```
Edit-EC2Host `
```

```
    -HostRecovery off `
    -HostId h-012a3456b7890cdef
```

Sehen Sie sich die Host-Wiederherstellungseinstellungen für Ihren Amazon EC2 Dedicated Host an

Sie können die Konfiguration der Host-Wiederherstellung für einen Dedicated Host jederzeit anzeigen.

Console

So zeigen Sie die Host-Wiederherstellungskonfiguration für Dedicated Host an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie den Dedicated Host aus und überprüfen Sie auf der Registerkarte Description (Beschreibung) das Feld Host Recovery (Host-Wiederherstellung).

AWS CLI

So zeigen Sie die Host-Wiederherstellungskonfiguration für Dedicated Host an

Verwenden Sie den Befehl describe-hosts.

```
aws ec2 describe-hosts \
    --host-ids h-012a3456b7890cdef \
    --query Hosts[].HostRecovery
```

Es folgt eine Beispielausgabe.

```
on
```

PowerShell

So zeigen Sie die Host-Wiederherstellungskonfiguration für Dedicated Host an

Verwenden Sie das cmdlet Get-EC2Host.

```
(Get-EC2Host -HostId h-012a3456b7890cdef).Hosts | Select HostRecovery
```

Es folgt eine Beispielausgabe.

```
HostRecovery
------------
on
```

Manuelles Wiederherstellen von Instances, die von Amazon EC2 Dedicated Host Recovery nicht unterstützt werden

Die Host-Wiederherstellung unterstützt nicht die Wiederherstellung von Instances, die Instance-Speicher-Volumes verwenden. Befolgen Sie die unten stehende Anleitung, um manuell die Instances wiederherzustellen, die nicht automatisch wiederhergestellt werden konnten.

> **Warning**
>
> Alle Daten, die auf Instance-Speicher-Volumes gespeichert sind, gehen verloren, wenn eine Instance angehalten, in den Ruhezustand versetzt oder beendet wird. Dies gilt auch für Instance-Speicher-Volumes, die an eine Instance mit einem EBS-Root-Volume angehängt sind. Wenn Sie Daten von Instance-Speicher-Volumes schützen möchten, sichern Sie diese auf einem persistenten Speicher, ehe die Instance angehalten oder beendet wird.

Manuelles Wiederherstellen von EBS-gestützten Instances

EBS-gestützte Instances, die nicht automatisch wiederhergestellt werden, sollten Sie manuell anhalten und starten, damit sie auf einem neuen Dedicated Host wiederhergestellt werden. Weitere Informationen zum Anhalten Ihrer Instance und zu den Änderungen an der Instance-Konfiguration nach dem Anhalten finden Sie unter Stoppen und starten Sie EC2 Amazon-Instances.

Instances mit Instance-Speicher-Root-Volumes manuell wiederherstellen

Bei Instances mit Instance-Speicher-Root-Volumes, die nicht automatisch wiederhergestellt werden konnten, sollten Sie wie folgt vorgehen:

1. Starten Sie eine Ersatz-Instance auf einem neuen Dedicated Host über Ihr neuestes AMI.
2. Migrieren Sie alle notwendigen Daten zur Ersatz-Instance.
3. Beenden Sie die Original-Instance auf dem beeinträchtigten Dedicated Host.

Host-Wartung für Amazon EC2 Dedicated Host

Bei der Host-Wartung migrieren wir für den seltenen Fall, dass ein Dedicated Host beeinträchtigt wird, die unterstützten Instances, die darauf ausgeführt werden, automatisch zu einem funktionsfähigen Dedicated Host als Ersatz. Dies trägt dazu bei, die Ausfallzeiten für Ihren Workload zu minimieren und die Verwaltung Ihrer Dedicated Hosts zu vereinfachen. Die Host-Wartung wird auch für geplante und routinemäßige EC2 Amazon-Wartungsarbeiten durchgeführt.

Amazon EC2 unterstützt zwei Arten der Host-Wartung:

- Wartung des Live-Migrations-Hosts – Instances werden innerhalb von 24 Stunden automatisch auf den Ersatz-Host migriert, ohne sie anzuhalten und neu zu starten.
- Host-Wartung auf Basis eines Neustarts – Instances werden für geplante Instance-Neustart-Ereignisse eingeplant, bei denen sie automatisch angehalten und auf dem Ersatz-Host neu gestartet werden.

Inhalt

- Host-Wartung im Vergleich zur Host-Wiederherstellung
- Überlegungen
- Zugehörige Services
- Preisgestaltung
- So funktioniert die Host-Wartung für Amazon EC2 Dedicated Hosts
- Konfiguration der Host-Wartungseinstellungen für einen Amazon EC2 Dedicated Host

Host-Wartung im Vergleich zur Host-Wiederherstellung

Die folgende Tabelle zeigt die Hauptunterschiede zwischen Host-Wiederherstellung und Host-Wartung.

	Host-Wiederherstellung	Host-Wartung
Instance-Erreichbarkeit	Unerreichbar	Erreichbar
Dedicated-Host-Zustand	`under-assessment`	`permanent-failure`
Host-Ressourcengruppe	Unterstützt	Nicht unterstützt

Weitere Informationen zur Host-Wiederherstellung finden Sie unter Host-Wiederherstellung.

Überlegungen

- Die Host-Wartung ist in allen Ländern verfügbar AWS-Regionen, mit Ausnahme der Regionen China und AWS GovCloud (US) Regions.
- Die Host-Wartung wird in AWS Outposts AWS Local Zones und AWS Wavelength Zones nicht unterstützt.
- Die Host-Wartung kann für Hosts, die sich bereits in einer Host-Ressourcengruppe befinden, nicht aktiviert oder deaktiviert werden. Hosts, die einer Host-Ressourcengruppe hinzugefügt wurden, behalten ihre Host-Wartungseinstellung bei. Weitere Informationen finden Sie unter Host-Ressourcengruppen.
- Die Host-Wartung wird bei den folgenden Instance-Typen nicht unterstützt, da sie Instance-Speicher Root-Volumes haben: C1, C3, D2, I2, M1, M2, M3, R3, and X1.

Zugehörige Services

Dedicated Host ist in AWS License Manager integriert — Verfolgt Lizenzen auf Ihren Amazon EC2 Dedicated Hosts (wird nur in Regionen unterstützt, in denen AWS License Manager verfügbar ist). Weitere Informationen finden Sie im AWS License-Manager-Benutzerhandbuch.

Sie müssen über ausreichend Lizenzen AWS-Konto für Ihren neuen Dedicated Host verfügen. Die Ihrem beeinträchtigten Host zugeordneten Lizenzen werden freigegeben, wenn der Host nach Abschluss des geplanten Wartungsvorgangs freigegeben wird.

Preisgestaltung

Für die Host-Wartung fallen keine zusätzlichen Gebühren an. Es fallen jedoch die üblichen Dedicated-Host-Gebühren an. Weitere Informationen finden Sie unter Amazon EC2 Dedicated Hosts — Preise.

Sobald die Host-Wartung eingeleitet wird, wird Ihnen der beeinträchtigte Dedicated Host nicht mehr in Rechnung gestellt. Kosten für den ersatzmäßigen Dedicated Host fallen erst an, wenn er den Status `available` hat.

Wenn der beeinträchtigte Dedicated Host nach Bedarf abgerechnet wurde, wird der ersatzmäßige Dedicated Host genauso abgerechnet. Wenn der beeinträchtigte Dedicated Host über eine aktive Dedicated-Host-Reservierung verfügt, wird diese auf den neuen Dedicated Host übertragen.

So funktioniert die Host-Wartung für Amazon EC2 Dedicated Hosts

Wenn eine Beeinträchtigung in einem Dedicated Host festgestellt wird, der für die Host-Wartung aktiviert ist, weisen wir Ihrem Konto automatisch einen Dedicated Host zu. Dieser Dedicated Host erhält eine neue Host-ID, hat aber dieselben Attribute wie der ursprüngliche Dedicated Host, einschließlich:

- Einstellungen zur automatischen Platzierung
- Availability Zone
- Dedicated-Host-Reservierungszuordnung
- Host-Affinität
- Einstellungen für die Host-Wartung
- Einstellungen für die Host-Wiederherstellung
- Instance-Typ
- Tags (Markierungen)

Sobald der Ersatz-Host zugewiesen wurde, migrieren wir die Instances entweder mithilfe der Live-Migrations-Host-Wartung oder der Host-Wartung auf Basis eines Neustarts, abhängig von der Instance.

Sobald auf dem beeinträchtigten Host keine Instances mehr ausgeführt werden, wird er dauerhaft von Ihrem Konto entfernt.

Wartung des Hosts für die Live-Migration

Instances, die Live-Migration-Host-Wartung unterstützen, werden innerhalb von 24 Stunden automatisch auf den Ersatz-Host migriert, ohne dass sie angehalten und neu gestartet werden müssen. Die migrierten Instances behalten ihre vorhandenen Attribute bei, darunter:

- Instance-ID
- Instance-Metadaten
- Anhänge von Amazon-EBS-Volumes
- Elastic IP-Adressen und private IP-Adressen
- Speicher-, CPU- und Netzwerkstatus

Bei einigen größeren Instances kann es während der Migration zu leichten Leistungseinbußen kommen.

Nachdem die Instances automatisch auf den Ersatzhost migriert wurden, senden wir Ihnen E-Mail- und AWS Health Dashboard-Benachrichtigungen. Zu den Benachrichtigungen gehören die IDs heruntergestuften Hosts und die Ersatzhosts, Informationen zu den Instances, die mithilfe der Live-Hostwartung für die Migration automatisch migriert wurden, sowie Informationen über die verbleibenden Instanzen.

Host-Wartung auf Basis eines Neustarts

Für Instances, für die eine Host-Wartung auf Basis eines Neustarts erforderlich ist, werden beispielsweise geplante Neustart-Ereignisse für 14 Tage ab dem Datum der Benachrichtigung geplant. Sie können vor dem geplanten Ereignis weiterhin auf Ihre Instances in dem beeinträchtigten Dedicated Host zugreifen.

Sie können Neustart-Ereignisse auf ein Datum verschieben, das innerhalb von 7 Tagen nach Datum und Uhrzeit des ursprünglichen Ereignisses liegt. Weitere Informationen finden Sie unter Planen Sie ein geplantes Ereignis für eine Instanz neu EC2 .

Amazon reserviert EC2 automatisch Kapazität auf dem Ersatzhost für diese Instances. In dieser reservierten Kapazität können Sie keine Instances ausführen.

Die EC2 Amazon-Konsole zeigt die reservierte Kapazität als genutzte Kapazität an. Es könnte den Anschein haben, dass die Instances sowohl auf dem heruntergestuften Host als auch in dem Ersatz-Host ausgeführt werden. Die Instances werden jedoch weiterhin nur in dem heruntergestuften Host ausgeführt, bis sie angehalten oder in die reservierte Kapazität zu dem Ersatz-Host migriert werden.

Am Tag und zur Uhrzeit des geplanten Ereignisses werden die Instances automatisch gestoppt und mit der reservierten Kapazität in dem Ersatz-Host neu gestartet. Die migrierten Instances behalten ihre vorhandenen Attribute bei, darunter:

- Instance-ID
- Instance-Metadaten
- Anhänge von Amazon-EBS-Volumes
- Elastic IP-Adressen und private IP-Adressen

Da die Instances jedoch während der Migration gestoppt und neu gestartet werden, behalten sie ihren Speicher-, CPU- und Netzwerkstatus nicht bei.

Sie können diese Instances auch jederzeit vor dem geplanten Ereignis manuell beenden und neu starten, um sie zu den Ersatz-Host oder einen anderen Host zu migrieren. Möglicherweise müssen Sie die Host-Affinität Ihrer Instance ändern, um sie auf einem anderen Host neu zu starten. Wenn Sie eine Instance vor dem geplanten Ereignis beenden, wird die reservierte Kapazität in dem Ersatz-Host freigegeben und kann wieder verwendet werden.

Status der Host-Wartung

Wenn ein Host herabgestuft wird, wechselt er in den Status `permanent-failure`. Sie können keine Instances in einem Dedicated Host im Status `permanent-failure` starten.

Sobald der Ersatz-Host zugewiesen wurde, verbleibt er im Status `pending`, bis die Instances, die die Live-Migration-Host-Wartung unterstützen, automatisch vom beeinträchtigten Host migriert wurden und bis die geplanten Ereignisse für die verbleibenden Instances geplant wurden. Nachdem diese Aufgaben abgeschlossen sind, wechselt der Ersatz-Host in den Status `available`.

Sobald der Ersatz-Host in den Status `available` wechselt, können Sie ihn genauso verwenden wie jeden Host in Ihrem Konto. Ein Teil der Instance-Kapazität auf dem Ersatz-Host ist jedoch für die Instances reserviert, für die eine Host-Migration auf Basis eines Neustarts erforderlich ist. In dieser reservierten Kapazität können Sie keine neuen Instances starten.

Sobald auf dem heruntergestuften Host keine Instances mehr ausgeführt werden, wechselt er in den Status `released, permanent-failure` und wird dauerhaft aus Ihrem Konto entfernt. Beachten Sie, dass der Host und seine Ressourcen für kurze Zeit in der Konsole sichtbar bleiben.

Automatische Migration

Einige Instances können nicht automatisch zu den Ersatz-Host migriert werden.

Instances mit EBS-Backed Root-Volumes

Für diese Instances planen wir Ereignisse zur Außerbetriebnahme von Instances für 28 Tage ab dem Datum der Benachrichtigung. Am Tag und zur Uhrzeit des geplanten Ereignisses werden die Instances dauerhaft beendet. Wir empfehlen, dass Sie die Instance in dem Ersatz-Host oder in einem anderen Host manuell beenden und neu starten. Möglicherweise müssen Sie die Host-Affinität Ihrer Instance ändern, um sie in einem anderen Host neu zu starten.

Instances mit einem Instance-Speicher-gestützten Root-Volume

Für diese Instances planen wir Ereignisse zur Außerbetriebnahme von Instances für 28 Tage ab dem Datum der Benachrichtigung. Am Tag und zur Uhrzeit des geplanten Ereignisses werden die

Instances dauerhaft beendet. Wir empfehlen, dass Sie Ersatz-Instances manuell in dem Ersatz-Host starten und dann die erforderlichen Daten vor dem geplanten Ereignis zu die Ersatz-Instances migrieren.

Die folgenden Instances verfügen über Instance-Speicher-Root-Volumes: C1, C3, D2, I2, M1, M2, M3, R3 und X1.

Sie können vor dem geplanten Ereignis weiterhin auf Ihre Instances in dem beeinträchtigten Dedicated Host zugreifen.

Konfiguration der Host-Wartungseinstellungen für einen Amazon EC2 Dedicated Host

Aktivieren Sie die Host-Wartung, um sicherzustellen, dass Ihre in einem Dedicated Host ausgeführte Instances während eines geplanten Wartungsereignisses automatisch auf einem neuen Dedicated Host wiederhergestellt werden.

Wenn Sie die Host-Wartung deaktivieren, erhalten Sie eine E-Mail-Benachrichtigung, um den beeinträchtigten Host zu entfernen und Ihre Instances innerhalb von 28 Tagen manuell auf einen anderen Host zu migrieren. Wenn Sie über eine Dedicated-Host-Reservierung verfügen, wird ein Ersatz-Host zugewiesen. Nach 28 Tagen werden die auf dem beeinträchtigten Host ausgeführten Instances beendet und der Host wird automatisch freigegeben.

Console

So aktivieren Sie die Host-Wartung für Ihren Dedicated Host

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie Dedicated Host > Aktionen > Host ändern aus.
4. Wählen Sie die Option ein im Feld Host-Wartung aus.

So deaktivieren Sie die Host-Wartung für Ihren Dedicated Host

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie Dedicated Host > Aktionen > Host ändern aus.
4. Wählen Sie die Option aus im Feld Host-Wartung aus.

AWS CLI

So aktivieren Sie die Host-Wartung für Ihren Dedicated Host

Verwenden Sie den modify-hosts-Befehl.

```
aws ec2 modify-hosts \
    --host-maintenance on \
    --host-ids h-0d123456bbf78910d
```

So deaktivieren Sie die Host-Wartung für Ihren Dedicated Host

Verwenden Sie den modify-hosts-Befehl.

```
aws ec2 modify-hosts \
    --host-maintenance off \
    --host-ids h-0d123456bbf78910d
```

PowerShell

So aktivieren Sie die Host-Wartung für Ihren Dedicated Host

Verwenden Sie das cmdlet Edit-EC2Host.

```
Edit-EC2Host `
    -HostMaintenance on `
    -HostId h-0d123456bbf78910d
```

So deaktivieren Sie die Host-Wartung für Ihren Dedicated Host

Verwenden Sie das cmdlet Edit-EC2Host.

```
Edit-EC2Host `
    -HostMaintenance off `
    -HostId h-0d123456bbf78910d
```

Überwachen Sie den Status Ihrer Amazon EC2 Dedicated Hosts

Amazon überwacht EC2 ständig den Status Ihrer Dedicated Hosts. Updates werden auf der EC2 Amazon-Konsole kommuniziert. Sie können Informationen zu einem Dedicated Host mit den folgenden Methoden anzeigen.

Console

So zeigen Sie den Status eines Dedicated Host an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Suchen Sie den Dedicated Host in der Liste und sehen Sie sich den Wert in der Spalte State (Status) an.

AWS CLI

So zeigen Sie den Status eines Dedicated Host an

Verwenden Sie den Befehl describe-hosts.

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

PowerShell

So zeigen Sie den Status eines Dedicated Host an

Verwenden Sie das cmdlet Get-EC2Host.

```
Get-EC2Host -HostId h-012a3456b7890cdef
```

Die folgende Tabelle erklärt die möglichen Dedicated Host-Statuswerte.

Status	Beschreibung
`available`	AWS hat kein Problem mit dem Dedicated Host festgestellt. Es sind keine Wartungen oder Reparaturen geplant. Instances können auf diesem Dedicated Host gestartet werden.
`released`	Der Dedicated Host wurde freigegeben. Die Host-ID wird nicht mehr verwendet. Freigegebene Hosts können nicht wiederverwendet werden.
`under-assessment`	AWS untersucht ein mögliches Problem mit dem Dedicated Host. Wenn Maßnahmen ergriffen werden müssen, werden Sie per E-Mail AWS-

Status	Beschreibung
	Managementkonsole oder per E-Mail benachrichtigt. In diesem Status können keine Instances auf dem Dedicated Host gestartet werden.
`pending`	Der Dedicated Host kann nicht für den Start neuer Instances verwendet werden. Er wird entweder geändert, um mehrere Instance-Typen zu unterstützen oder es wird eine Host-Wiederherstellung durchgeführt.
`permanent-failure`	Ein unwiederbringlicher Fehler ist aufgetreten. Sie erhalten einen Bereinigungshinweis über Ihre Instances und per E-Mail. Ihre Instances werden möglicherweise weiter ausgeführt. Wenn Sie alle Instances auf einem Dedicated Host mit diesem Status beenden oder beenden, wird der AWS Host außer Betrieb genommen. AWS startet Instanzen in diesem Status nicht neu. In diesem Status können keine Instances auf dem Dedicated Hosts gestartet werden.
`released-permanent-failure`	AWS gibt Dedicated Hosts, die ausgefallen sind und auf denen keine laufenden Instances mehr laufen, dauerhaft frei. Die Dedicated Host-ID steht nicht mehr zur Nutzung zur Verfügung.

Verfolgen Sie Änderungen der Amazon EC2 Dedicated Host-Konfiguration mit AWS Config

Sie können AWS Config es verwenden, um Konfigurationsänderungen für Dedicated Hosts und für Instances aufzuzeichnen, die auf Dedicated Hosts gestartet, gestoppt oder beendet werden. Sie können dann die von AWS Config erfassten Informationen als Datenquelle für die Lizenzberichterstellung verwenden.

AWS Config zeichnet Konfigurationsinformationen für Dedicated Hosts und Instances einzeln auf und verknüpft diese Informationen anhand von Beziehungen. Es gibt drei Berichtsbedingungen.

- AWS Config Aufzeichnungsstatus — Wenn aktiviert, AWS Config werden ein oder mehrere AWS Ressourcentypen aufgezeichnet, zu denen Dedicated Hosts und Dedicated Instances gehören können. Um die erforderlichen Informationen für die Lizenzberichterstattung zu erfassen, prüfen Sie, dass Hosts und Instances mit den folgenden Feldern aufgenommen werden.
- Host recording status (Hostaufnahmestatus):— Bei Enabled (Aktiviert) werden die Konfigurationsinformationen für Dedicated Hosts aufgenommen.

- Instance recording status (Instance-Erfassungsstatus) – Bei Enabled (Aktiviert) werden die Konfigurationsinformationen für Dedicated Instances erfasst.

Falls mindestens eine dieser drei Bedingungen deaktiviert ist, ist das Symbol auf der Schaltfläche Edit Config Recording (Konfigurationsaufnahme bearbeiten) rot. Um den vollständigen Nutzen dieses Tools zu erhalten, müssen Sie gewährleisten, dass alle drei Aufnahmemethoden aktiviert sind. Wenn alle drei aktiviert sind, ist das Symbol grün. Zum Bearbeiten der Einstellungen wählen Sie Edit Config Recording (Konfigurationsaufnahme bearbeiten). Sie werden zur AWS Config Einrichtungsseite in der AWS Config Konsole weitergeleitet, auf der Sie die Aufzeichnung für Ihre Hosts, Instances AWS Config und andere unterstützte Ressourcentypen einrichten und starten können. Weitere Informationen finden Sie im AWS Config Entwicklerhandbuch AWS Config unter Einrichtung mithilfe der Konsole.

> **Note**
>
> AWS Config zeichnet Ihre Ressourcen auf, nachdem sie erkannt wurden. Dies kann mehrere Minuten dauern.

Nach AWS Config Beginn der Aufzeichnung von Konfigurationsänderungen an Ihren Hosts und Instances können Sie den Konfigurationsverlauf aller Hosts abrufen, die Sie zugewiesen oder freigegeben haben, sowie aller Instances, die Sie gestartet, gestoppt oder beendet haben. Beispiel: Sie können an jedem beliebigen Punkt im Konfigurationsverlauf eines Dedicated Host neben der Anzahl der Sockets und Kerne im Host auch nachsehen, wie viele Instances auf dem Host gestartet werden. Sie können für all diese Instances die ID des zugehörigen Amazon Machine Image (AMI) nachsehen. Sie können diese Informationen verwenden, um einen Bericht über die Lizenzierung Ihrer eigenen servergebundenen Software zu erstellen, die auf Socket- oder Kernbasis lizenziert ist.

Sie können die Konfigurationsverläufe auf eine der folgenden Arten anzeigen:

- Mithilfe der AWS Config Konsole. Für jede aufgenommene Ressource können Sie eine Timeline-Seite anzeigen, die einen Verlauf der Konfigurationsdetails bietet. Wählen Sie zum Anzeigen dieser Seite das graue Symbol in der Spalte Config Timeline (Konfig.-Timeline) der Seite Dedicated Hosts. Weitere Informationen finden Sie im AWS Config Entwicklerhandbuch unter Konfigurationsdetails in der AWS Config Konsole anzeigen.
- Durch das Ausführen von AWS CLI Befehlen. Zunächst können Sie den list-discovered-resourcesBefehl verwenden, um eine Liste aller Hosts und Instanzen abzurufen. Anschließend

können Sie den get-resource-config-historyBefehl verwenden, um die Konfigurationsdetails eines Hosts oder einer Instanz für ein bestimmtes Zeitintervall abzurufen.

- Indem Sie die AWS Config API in Ihren Anwendungen verwenden. Zunächst können Sie die ListDiscoveredResourcesAktion verwenden, um eine Liste aller Hosts und Instanzen abzurufen. Anschließend können Sie die GetResourceConfigHistoryAktion verwenden, um die Konfigurationsdetails eines Hosts oder einer Instanz für ein bestimmtes Zeitintervall abzurufen.

Um beispielsweise eine Liste all Ihrer Dedicated Hosts von abzurufen AWS Config, führen Sie einen CLI-Befehl wie den folgenden aus.

```
aws configservice list-discovered-resources --resource-type AWS::EC2::Host
```

Um den Konfigurationsverlauf eines Dedicated Hosts von abzurufen AWS Config, führen Sie einen CLI-Befehl wie den folgenden aus.

```
aws configservice get-resource-config-history \
    --resource-type AWS::EC2::Instance \
    --resource-id i-1234567890abcdef0
```

Um AWS Config Einstellungen mit der Konsole zu verwalten

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Seite Dedicated Hosts die Option Edit Config Recording (Konfigurationsaufnahme bearbeiten).
3. Folgen Sie in der AWS Config Konsole den angegebenen Schritten, um die Aufnahme zu aktivieren. Weitere Informationen finden Sie unter Einrichtung AWS Config über die Konsole.

Weitere Informationen finden Sie unter Konfigurationsdetails in der AWS Config Konsole anzeigen.

Zur Aktivierung AWS Config über die Befehlszeile oder API

- AWS CLI: Konfigurationsdetails (AWS CLI) im AWS Config Entwicklerhandbuch anzeigen.
- EC2 Amazon-API: GetResourceConfigHistory.

Amazon-EC2-Dedicated-Instances

EC2-Instances werden standardmäßig auf gemeinsam genutzter Tenancy-Hardware ausgeführt. Das bedeutet, dass mehrere AWS-Konten dieselbe physische Hardware gemeinsam nutzen können.

Dedicated Instances sind EC2-Instances, die auf Hardware ausgeführt werden, die für ein einzelnes AWS-Konto bestimmt ist. Dedicated Instances, die zu verschiedenen AWS-Konten gehören, sind auf einer Hardwareebene physisch isoliert, selbst wenn diese Konten mit einem einzelnen Zahlerkonto verknüpft sind. Dedicated Instances können jedoch Hardware mit anderen Instances desselben AWS-Kontos teilen, die keine Dedicated Instances sind.

Dedizierte Instances bieten weder Transparenz noch Kontrolle über die Platzierung von Instances und unterstützen keine Host-Affinität. Wenn Sie eine Dedicated Instance beenden und starten, läuft sie möglicherweise nicht auf demselben Host. Ebenso können Sie nicht auf einen bestimmten Host abzielen, auf dem eine Instance gestartet oder ausgeführt werden soll. Darüber hinaus bieten Dedicated Instances eingeschränkte Unterstützung für Bring Your Own License (BYOL).

Wenn Sie Transparenz und Kontrolle über die Platzierung von Instances und einen umfassenderen BYOL-Support benötigen, sollten Sie überlegen, stattdessen einen Dedicated Host zu verwenden. Dedicated Hosts und Dedicated Instances können beide zum Starten von Amazon-EC2-Instances auf physischen Servern verwendet werden. Es gibt keine leistungsbezogenen, sicherheitsrelevanten oder physischen Unterschiede zwischen Dedicated Instances und Instances auf Dedicated Hosts. Es gibt jedoch einige wichtige Unterschiede zwischen beiden. Die folgende Tabelle hebt einige der wichtigsten Unterschiede zwischen Dedicated Hosts und Dedicated Instances hervor:

	Dedicated Host	Dedicated Instance
Dedizierter physischer Server	Physischer Server mit Instance-Kapazität, die vollständig für Ihre Nutzung bereitgestellt wird.	Physischer Server, der für ein einzelnes Kundenkonto bereitgestellt wird.
Instance-Kapazität sfreigabe	Kann die Instance-Kapazität mit anderen Konten teilen.	Nicht unterstützt
Fakturierung	Abrechnung pro Host	Abrechnung pro Instance
Sichtbarkeit von Sockets,	Zeigt die Anzahl der Sockets und physischen Kerne	Keine Sichtbarkeit

	Dedicated Host	Dedicated Instance
Kernen und Host-ID		
Host- und Instance-Affinität	Gestattet Ihnen, Ihre Instances im Laufe der Zeit durchgängig auf demselben physischen Server bereitzustellen	Nicht unterstützt
Zielgerichtete Instance-Platzierung	Bietet zusätzliche Sichtbarkeit und Kontrolle darüber, wie Instances auf einem physischen Server platziert werden.	Nicht unterstützt
Automatische Instance-Wiederherstellung	Unterstützt. Weitere Informationen finden Sie unter Wiederherstellung von Amazon EC2 Dedicated Host.	Unterstützt
Bring Your Own License (BYOL)	Unterstützt	Teilweise Unterstützung*
Capacity Reservations	Nicht unterstützt	Unterstützt

* Microsoft SQL Server mit Lizenzmobilität über Software Assurance und Windows Virtual Desktop Access (VDA)-Lizenzen können mit Dedicated Instance verwendet werden.

Weitere Informationen finden Sie unter EC2 Dedizierte Amazon-Hosts.

Inhalt

- Grundlagen von Dedicated Instance
- Unterstützte Features
- Dedicated Instances-Einschränkungen
- Preise für Dedicated Instances

- Dedicated Instances in eine VPC mit Standard-Tenancy starten
- Die Tenancy einer EC2-Instance ändern
- Ändern der Instance-Tenancy einer VPC

Grundlagen von Dedicated Instance

Eine VPC kann eine Tenancy von `default` oder `dedicated` haben. Ihre VPCs haben standardmäßig eine `default`-Tenancy und Instances, die in einer `default`-Tenancy-VPC gestartet werden, haben eine `default`-Tenancy. Starten Sie Dedicated Instances wie folgt:

- Erstellen Sie eine VPC mit einer Tenancy `dedicated`, sodass alle Instances in der VPC als Dedicated Instances ausgeführt werden. Weitere Informationen finden Sie unter Dedicated Instances in eine VPC mit Standard-Tenancy starten.
- Erstellen Sie eine VPC mit der Tenancy `default` und geben Sie manuell die Tenancy `dedicated` für die Instances an, die als Dedicated Instances ausgeführt werden sollen. Weitere Informationen finden Sie unter Dedicated Instances in eine VPC mit Standard-Tenancy starten.

Unterstützte Features

Dedicated Instances unterstützen die folgenden Features und AWS-Service-Integrationen:

Feature

- Reserved Instances
- Auto Scaling
- Automatische Wiederherstellung
- Dedicated Spot Instances
- Burstable Performance Instances

Reserved Instances

Um Kapazität für Ihre Dedicated Instances zu reservieren, können Sie Dedicated-Reserved-Instances oder Kapazitätsreservierungen erwerben. Weitere Informationen finden Sie unter Überblick über Reserved Instances für Amazon EC2 und Reservieren Sie Rechenkapazität mit Kapazitätsreservierungen EC2 auf Abruf.

Wenn Sie eine Dedicated Reserved Instance kaufen, erwerben Sie die Kapazität zum Starten einer Dedicated Instance in einer VPC zu deutlich reduzierten Nutzungsgebühren. Der Preisunterschied in der nutzungsabhängigen Gebühr gilt nur, wenn Sie eine Instance mit Dedicated Tenancy starten. Wenn Sie eine Reserved Instance mit Standard-Tenancy erwerben, gilt sie nur für eine aktive Instance mit `default`-Tenancy; sie gilt nicht für eine aktive Instance mit `dedicated`-Tenancy.

Darüber hinaus können Sie die Tenancy einer Reserved Instance nach dem Kauf nicht mit dem Änderungsverfahren ändern. Sie können jedoch auch eine Convertible Reserved Instance gegen eine neue Convertible Reserved Instance mit einer anderen Tenancy austauschen.

Auto Scaling

Mit Amazon EC2 Auto Scaling können Sie Dedicated Instances starten. Weitere Informationen finden Sie unter Erstellen einer Startvorlage mit erweiterten Einstellungen im Amazon EC2 Auto Scaling-Benutzerhandbuch.

Automatische Wiederherstellung

Sie können automatische Wiederherstellung für eine Dedicated Instance konfigurieren, wenn die Instance aufgrund eines zugrunde liegenden Hardware-Ausfalls oder eines Problems, das eine Beteiligung von AWS für eine Reparatur erforderlich macht, beeinträchtigt wird. Weitere Informationen finden Sie unter Automatische Instance-Wiederherstellung.

Dedicated Spot Instances

Sie können eine Dedicated Spot-Instance ausführen, indem Sie beim Erstellen einer Spot-Instance-Anfrage die Tenancy `dedicated` angeben. Weitere Informationen finden Sie unter Auf Einzel-Tenant-Hardware starten.

Burstable Performance Instances

Sie können die Vorteile der Ausführung auf Dedicated-Tenancy-Hardware mit nutze the section called “Burstable Performance Instances”. T3 Dedicated Instances werden standardmäßig im unbegrenzten Modus gestartet und sie stellen eine CPU-Basisleistung mit der Fähigkeit bereit, die CPU-Leistung je nach Erfordernis Ihrer Workload itslast zu steigern. Die T3-Basisleistung und die Steigerbarkeit unterliegen dem CPU-Guthaben. Aufgrund der Steigerbarkeit der T3-Instance-Typen empfehlen wir, zu überwachen, wie Ihre T3-Instances die CPU-Ressourcen der dedizierten Hardware für die beste Leistung verwenden. T3 Dedicated Instances sind für Kunden mit unterschiedlichen Workloads gedacht, die ein zufälliges CPU-Verhalten aufweisen, aber idealerweise eine durchschnittliche CPU-

Auslastung bei oder unterhalb der Basisnutzung haben. Weitere Informationen finden Sie unter the section called “Die wichtigsten Konzepte”.

Amazon EC2 verfügt über Systeme zur Identifizierung und Korrektur von Leistungsschwankungen. Es ist jedoch immer noch möglich, dass es zu kurzfristigen Schwankungen kommt, wenn Sie mehrere T3 Dedicated Instances starten, die korrelierte CPU-Auslastungsmuster aufweisen. Für diese anspruchsvolleren oder korrelierten Workloads empfehlen wir die Verwendung von M5 oder M5a Dedicated Instances anstelle von T3 Dedicated Instances.

Dedicated Instances-Einschränkungen

Berücksichtigen Sie bei Verwendung von Dedicated Instances Folgendes:

- Einige AWS-Services oder ihre Features funktionieren nicht mit einer VPC, deren Instance-Tenancy auf `dedicated` festgelegt ist. Lesen Sie die Dokumentation zum entsprechenden Service, um zu bestätigen, ob es Einschränkungen gibt.
- Einige Instance-Typen können nicht in einer VPC gestartet werden, deren Instance-Tenancy auf festgelegt ist `dedicated`. Weitere Informationen zu den unterstützten Instance-Typen finden Sie unter Amazon-EC2-Dedicated-Instances.
- Wenn Sie eine Dedicated-Instance-gestützte Amazon EBS starten, wird das EBS-Volume nicht auf einer Single-Tenant-Hardware ausgeführt.

Preise für Dedicated Instances

Die Preise für Dedicated Instances unterscheiden sich von den Preisen für On-Demand-Instances. Weitere Informationen finden Sie unter Amazon-EC2-Dedicated-Instances.

Dedicated Instances in eine VPC mit Standard-Tenancy starten

Beim Erstellen einer VPC haben Sie die Option, eine Instance-Tenancy anzugeben. Wenn Sie eine Instance in einer VPC starten, die eine Instance-Tenancy von `dedicated` hat, wird die Instance als Dedicated Instance auf Hardware ausgeführt, die für Ihre Verwendung bestimmt ist.

Weitere Informationen zum Starten einer Instance mit der Tenancy `host` finden Sie unter Starten Sie EC2 Amazon-Instances auf einem Amazon EC2 Dedicated Host.

Weitere Informationen über VPC-Tenancy-Optionen finden Sie unter Erstellen einer VPC im Amazon-VPC-Benutzerhandbuch.

Voraussetzungen

- Wählen Sie einen unterstützten Instance-Typ. Weitere Informationen finden Sie unter Amazon-EC2-Dedicated-Instances.

Console

So starten Sie eine Dedicated Instance in einer VPC mit einer Standard-Tenancy

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Launch Instance (Instance starten) aus.
3. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) ein AMI aus der Liste aus.
4. Wählen Sie im Bereich Instance type (Instance-Typ) den zu startenden Instance-Typ aus.
5. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das der Instance zugeordnet werden soll.
6. Wählen Sie im Bereich Advanced details (Erweiterte Details) unter Tenancy die Option Dedicated aus.
7. Konfigurieren Sie die verbleibenden Instance-Optionen nach Bedarf. Weitere Informationen finden Sie unter Referenz für EC2 Amazon-Instance-Konfigurationsparameter.
8. Wählen Sie Launch Instance (Instance starten) aus.

AWS CLI

So stellen Sie die Tenancy-Option für eine Instance beim Start ein

Verwenden Sie den Befehl run-instances und schließen Sie `Tenancy` mit der Option `--placement` ein.

```
--placement Tenancy=dedicated
```

PowerShell

So stellen Sie die Tenancy-Option für eine Instance beim Start ein

Verwenden Sie das Cmdlet New-EC2Instance mit dem `-Placement_Tenancy`-Parameter.

```
-Placement_Tenancy dedicated
```

Die Tenancy einer EC2-Instance ändern

Sie können die Tenancy einer angehaltenen Instance nach dem Start ändern. Ihre Änderungen werden wirksam, wenn die Instance das nächste Mal gestartet wird.

Alternativ können Sie die Tenancy Ihrer Virtual Private Cloud (VPC) ändern. Weitere Informationen finden Sie unter the section called “Ändern der Tenancy einer VPC”.

Einschränkungen

- Sie können die Tenancy einer Instance nicht mit der AWS-Managementkonsole ändern.
- Die Instance muss sich im Status `stopped` befinden.
- Welche Konvertierungen unterstützt werden, hängt von den Betriebssystemdetails Ihrer Instance sowie davon ab, ob SQL Server installiert ist. Weitere Informationen zu den für Ihre Instance verfügbaren Tenancy-Konvertierungspfaden finden Sie im License Manager-Benutzerhandbuch unter Tenancy-Konvertierung.
- Bei T3-Instances muss die Instance auf einem Dedicated Host gestartet werden, um eine Tenancy vom Typ `host` zu verwenden. Die Tenancy kann nicht von `host` in `dedicated` oder `default` geändert werden. Wenn Sie versuchen, eine dieser nicht unterstützten Tenancy-Änderungen vorzunehmen, wird der `InvalidRequest`-Fehlercode angezeigt.

AWS CLI

So ändern Sie den Tenancy-Wert einer Instance

Verwenden Sie den-Befehl modify-instance-placement.

```
aws ec2 modify-instance-placement \
    --instance-id i-1234567890abcdef0 \
    --tenancy dedicated
```

PowerShell

So ändern Sie den Tenancy-Wert einer Instance

Verwenden Sie das Cmdlet Edit-EC2InstancePlacement.

```
Edit-EC2InstancePlacement `
    -InstanceId i-1234567890abcdef0 `
    -Tenancy Dedicated
```

Ändern der Instance-Tenancy einer VPC

Die Tenancy der Instance einer Virtual Private Cloud (VPC) kann nach dem Erstellen von `dedicated` in `default` geändert werden. Die Änderung der Instance-Tenancy der VPC hat keine Auswirkungen auf die Tenancy der in der VPC vorhandenen Instances. Beim nächsten Start einer Instance in der VPC hat diese eine Tenancy von `default`, wenn beim Start kein anderer Wert angegeben wird.

Alternativ können Sie auch die Tenancy bestimmter Instances ändern. Weitere Informationen finden Sie unter the section called “Ändern der Tenancy einer Instance”.

Einschränkungen

- Sie können die Instance-Tenancy einer VPC nicht von `default` zu `dedicated` in ändern, nachdem sie erstellt wurde.
- Sie können die Tenancy einer VPC nicht mit der AWS-Managementkonsole ändern.

AWS CLI

So ändern Sie das Attribut für die Instance-Tenancy einer VPC

Verwenden Sie den Befehl modify-vpc-tenancy. Der einzige unterstützte Tenancy-Wert ist `default`.

```
aws ec2 modify-vpc-tenancy \
    --vpc-id vpc-1234567890abcdef0 \
    --instance-tenancy default
```

PowerShell

So ändern Sie das Attribut für die Instance-Tenancy einer VPC

Verwenden Sie das cmdlet Edit-EC2VpcTenancy. Der einzige unterstützte Tenancy-Wert ist `Default`.

```
Edit-EC2VpcTenancy `
    -VpcId vpc-1234567890abcdef0 `
    -InstanceTenancy Default
```

On-Demand-Kapazitätsreservierungen und Kapazitätsblöcke

Mit Kapazitätsreservierungen können Sie Rechenkapazität für EC2 Amazon-Instances in einer bestimmten Availability Zone reservieren. Es gibt zwei Arten von Kapazitätsreservierungen für unterschiedliche Anwendungsfälle.

Arten von Kapazitätsreservierungen

- On-Demand-Kapazitätsreservierungen
- Kapazitätsblöcke für ML

Im Folgenden sind einige häufige Anwendungsfälle für On-Demand-Kapazitätsreservierungen aufgeführt:

- Skalierung von Ereignissen – Erstellen Sie vor Ihren geschäftskritischen Ereignissen bedarfsgesteuerte Kapazitätsreservierungen, um sicherzustellen, dass Sie bei Bedarf skalieren können.
- Regulatorische Anforderungen und Notfallwiederherstellung – Verwenden Sie On-Demand-Kapazitätsreservierungen, um regulatorische Anforderungen für Hochverfügbarkeit zu erfüllen und Kapazität in einer anderen Availability Zone oder Region für die Notfallwiederherstellung zu reservieren.
- Ungenutzte Kapazität gemeinsam nutzen — Verwenden Sie Reservierungen für unterbrechbare Kapazitäten, um ungenutzte Kapazität für andere Workloads innerhalb Ihres Kontos verfügbar zu machen und gleichzeitig die Kontrolle zu behalten, um sie bei Bedarf zurückzugewinnen.

Im Folgenden sind einige häufige Anwendungsfälle für Kapazitätsblöcke für ML aufgeführt:

- Modell-Training und Feinabstimmung für Machine Learning (ML) – Erhalten Sie ununterbrochenen Zugriff auf die GPU-Instances, die Sie für das Training und die Feinabstimmung von ML-Modellen reserviert haben.
- ML-Experimente und Prototypen – Führen Sie Experimente durch und erstellen Sie Prototypen, die kurzfristig GPU-Instances erfordern.

Wann sollte die On-Demand-Kapazitätsreservierung verwendet werden?

Verwenden Sie On-Demand-Kapazitätsreservierungen, wenn Sie strenge Kapazitätsanforderungen haben und Ihre aktuellen oder zukünftigen unternehmenskritischen Workloads eine Kapazitätssicherung erfordern. Mit On-Demand-Kapazitätsreservierungen können Sie sicherstellen, dass Sie immer Zugriff auf die von Ihnen reservierten EC2 Amazon-Kapazitäten haben, solange Sie sie benötigen.

Wann sollten Kapazitätsblöcke für ML verwendet werden?

Verwenden Sie Kapazitätsblöcke für ML, wenn Sie sicherstellen müssen, dass Sie ab einem zukünftigen Datum für einen definierten Zeitraum ununterbrochenen Zugriff auf GPU-Instances haben. Kapazitätsblöcke eignen sich ideal für das Training und die Feinabstimmung von ML-Modellen, für kurze Ausführungen von Experimenten und für die Bewältigung eines vorübergehenden Anstiegs der Inferenznachfrage in der Zukunft. Mit Kapazitätsblöcken können Sie sicherstellen, dass Sie zu einem bestimmten Datum Zugriff auf GPU-Ressourcen haben, um Ihre ML-Workloads auszuführen.

Reservieren Sie Rechenkapazität mit Kapazitätsreservierungen EC2 auf Abruf

Mit Amazon EC2 Capacity Reservations können Sie Rechenkapazität für Ihre EC2 Amazon-Instances in einer bestimmten Availability Zone für einen beliebigen Zeitraum reservieren. Wenn Sie strenge Kapazitätsanforderungen für aktuelle oder future geschäftskritische Workloads haben, die ein gewisses Maß an lang- oder kurzfristiger Kapazitätssicherung erfordern, empfehlen wir Ihnen, eine Kapazitätsreservierung zu erstellen, um sicherzustellen, dass Sie jederzeit Zugriff auf EC2 Amazon-Kapazitäten haben, wenn Sie sie benötigen, und so lange Sie sie benötigen.

Sie können jederzeit eine Kapazitätsreservierung erstellen und wählen, wann sie beginnt. Sie können eine Kapazitätsreservierung zur sofortigen Nutzung oder eine Kapazitätsreservierung für einen zukünftigen Termin beantragen.

- Wenn Sie eine Kapazitätsreservierung zur sofortigen Nutzung anfordern, steht die Kapazitätsreservierung sofort zur Verfügung und es besteht keine zeitliche Bindung. Sie können die Kapazitätsreservierung jederzeit ändern und sie jederzeit stornieren, um die reservierte Kapazität freizugeben und keine Änderungen mehr vorzunehmen.
- Wenn Sie eine zukünftige Kapazitätsreservierung beantragen, geben Sie das zukünftige Datum an, an dem die Kapazitätsreservierung zur Nutzung verfügbar sein soll. Sie müssen auch eine Nutzungsdauer angeben, für die Sie sich verpflichten, die angeforderte Kapazität nach dem angegebenen Datum auf Ihrem Konto zu behalten. Am gewünschten Datum und zur gewünschten

Uhrzeit steht die Kapazitätsreservierung zur Verfügung und die Bindungsdauer beginnt. Während der Bindungsdauer können Sie die Anzahl der Instances oder die Dauer der Zusage nicht unter Ihre ursprüngliche Verpflichtung reduzieren oder die Kapazitätsreservierung stornieren. Nach Ablauf der Bindungsdauer können Sie die Kapazitätsreservierung beliebig ändern oder sie stornieren, wenn Sie sie nicht mehr benötigen.

Kapazitätsreservierungen können nur von Instances mit entsprechenden Attributen verwendet werden. Standardmäßig gleichen Kapazitätsreservierungen automatisch neue und ausgeführte Instances ab, die übereinstimmende Attribute besitzen (Instance-Typ, Plattform, Availability Zone und Tenancy). Dies bedeutet, dass eine Instance mit übereinstimmenden Attributen automatisch in der Kapazitätsreservierung ausgeführt wird. Sie können jedoch auch eine Kapazitätsreservierung für bestimmte Workloads festlegen. Auf diese Weise können Sie explizit steuern, welche Instances in der reservierten Kapazität ausgeführt werden dürfen. Sie können auch festlegen, dass Instances nur in einer Kapazitätsreservierung oder Kapazitätsreservierungs-Ressourcengruppe laufen.

> **Important**
>
> Zukünftige Kapazitätsreservierungen dienen dazu, Sie beim Starten und Absichern inkrementeller Instances zu unterstützen, und nicht zur Deckung vorhandener laufender Instances. Wenn Sie bestehende laufende Instances abdecken müssen, verwenden Sie stattdessen Kapazitätsreservierungen, die sofort beginnen.

Alle unterstützten EC2 Amazon-Instances mit übereinstimmenden Attributen, d. h. Instance-Typ, Plattform, Availability Zone und Tenancy, können im Rahmen einer Kapazitätsreservierung ausgeführt werden. Die EC2 Amazon-Instance kann von Ihnen (nicht verwaltete Instances) oder in Ihrem Namen von einem AWS Service (verwaltete Instances) gestartet werden. Dies gilt insbesondere für offene Kapazitätsreservierungen, die automatisch mit allen laufenden Instances mit übereinstimmenden Attributen abgeglichen werden. Beispielsweise können verwaltete Instances, die in Ihrem Namen von den folgenden Services gestartet wurden, in Kapazitätsreservierungen ausgeführt werden, die Sie erstellen und verwalten.

- Amazon EC2 Auto Scaling
- Amazon ECS
- Amazon EKS
- Amazon EMR

- Amazon SageMaker KI
- AWS Batch
- AWS Elastic Beanstalk
- AWS ParallelCluster
- AWS-Service für parallele Datenverarbeitung (AWS PCS)

Inhalt

- Konzepte für EC2 Amazon-Kapazitätsreservierungen
- Unterschiede zwischen Kapazitätsreservierungen, Reserved Instances und Savings Plans
- Unterstützte Plattformen
- Kontingente
- Einschränkungen
- Preise und Fakturierung für Kapazitätsreservierung
- Erstellen eines Kapazitätsreservierung
- Den Status einer Kapazitätsreservierung anzeigen
- Starten von Instances in einer bestehenden Kapazitätsreservierung
- Eine aktive Kapazitätsreservierung ändern
- Die Einstellungen für die Kapazitätsreservierung Ihrer Instance ändern
- Kapazität zwischen Kapazitätsreservierungen verschieben
- Kapazität aus einer bestehenden Kapazitätsreservierung abspalten
- Abbrechen eines Kapazitätsreservierung
- Kapazitätsreservierungen mit Cluster-Placement-Gruppen verwenden
- Kapazitätsreservierungs-Gruppen
- Kapazitätsreservierungen in Local Zones
- Kapazitätsreservierungen in Wavelength-Zonen
- Kapazitätsreservierungen am AWS Outposts
- Freigegebene Kapazitätsreservierungen
- Kapazitätsreservierungsflotten
- Überwachen Sie die Nutzung von Kapazitätsreservierungen anhand von Kennzahlen CloudWatch

- Unterauslastung der Kapazitätsreservierung überwachen
- Statusänderungen von zukünftigen Kapazitätsreservierungen überwachen
- Reservierungen für unterbrechbare Kapazitäten

Konzepte für EC2 Amazon-Kapazitätsreservierungen

Die folgenden Schlüsselkonzepte gelten für Kapazitätsreservierungen.

Themen

- Startdatum und -zeit
- Enddatum und -zeit
- Bindungsdauer
- Bewertung der Kapazitätsreservierung für die Zukunft
- Attribute von Kapazitätsreservierungen
- Kriterien für den Abgleich mit der Instance

Startdatum und -zeit

Das Startdatum und die Startzeit definieren, wann die Kapazitätsreservierung für die Verwendung zur Verfügung steht. Eine Kapazitätsreservierung kann sofort oder zu einem zukünftigem Zeitpunkt beginnen.

- Wenn Sie sich dafür entscheiden, eine Kapazitätsreservierung sofort zu starten, steht die reservierte Kapazität sofort nach ihrer Erstellung zur Verfügung. Die Abrechnung beginnt, sobald die Kapazitätsreservierung den aktiven Status erreicht hat. Sie müssen keine langfristigen Verpflichtungen eingehen. Sie können die Kapazitätsreservierung jederzeit nach Bedarf ändern und sie jederzeit stornieren, um die reservierte Kapazität freizugeben und keine Änderungen mehr vorzunehmen.
- Wenn Sie sich dafür entscheiden, eine Kapazitätsreservierung zu einem späteren Zeitpunkt zu beginnen, geben Sie ein Datum und eine Uhrzeit in der Zukunft an, zu der Sie die reservierte Kapazität benötigen, sowie eine Bindungsdauer, welches die Mindestdauer ist, für die Sie sich verpflichten, die angeforderte Kapazitätsreservierung in Ihrem Konto zu behalten, nachdem sie bereitgestellt wurde. Am angegebenen zukünftigen Datum wird die Kapazitätsreservierung zur Nutzung verfügbar und die Abrechnung beginnt zu diesem Zeitpunkt, sobald die Kapazitätsreservierung den aktiven Status erreicht hat. Die Bindungsdauer beginnt, sobald die Kapazitätsreservierung in Ihrem Konto bereitgestellt wird. Während dieser Zeit können Sie die

Anzahl der Instances nicht unter die Anzahl der gebundenen Instances senken, kein Enddatum wählen, das vor der Laufzeit der Zusage liegt, oder die Kapazitätsreservierung stornieren. Nach Ablauf der Bindungsdauer steht es Ihnen jedoch frei, die Kapazitätsreservierung in beliebiger Weise zu ändern oder sie zu stornieren, um die reservierte Kapazität freizugeben und keine Gebühren mehr anfallen zu lassen.

Enddatum und -zeit

Das Enddatum und die Endzeit legen fest, wann die Kapazitätsreservierung endet und die reservierte Kapazität von Ihrem Konto freigegeben wird. Sie können eine Kapazitätsreservierung so konfigurieren, dass sie automatisch endet an einem bestimmten Datum und zu einer bestimmten Uhrzeit, oder Sie können sie so konfigurieren, dass sie auf unbestimmte Zeit aktiv bleibt, bis Sie sie manuell stornieren.

Wenn Sie eine Kapazitätsreservierung so konfigurieren, dass sie automatisch endet, läuft die Kapazitätsreservierung innerhalb einer Stunde der angegebenen Uhrzeit ab. Wenn Sie beispielsweise `5/31/2019, 13:30:55` angeben, läuft die Kapazitätsreservierungs-Flotte garantiert zwischen `13:30:55` und `14:30:55` am `5/31/2019` ab.

Nach dem Ende einer Reservierung wird die reservierte Kapazität von Ihrem Konto freigegeben und Sie können Instances nicht mehr zielgerichtet in der Kapazitätsreservierung aufnehmen. In der reservierten Kapazität ausgeführte Instances werden weiterhin ununterbrochen ausgeführt. Wenn Instances, die auf eine Kapazitätsreservierung ausgerichtet sind, beendet werden, können Sie sie erst dann neu starten, wenn Sie ihre Ziel-Präferenz für die Kapazitätsreservierung entfernt oder sie für eine andere Kapazitätsreservierung konfiguriert haben. Weitere Informationen finden Sie unter Die Einstellungen für die Kapazitätsreservierung Ihrer Instance ändern.

Bindungsdauer

Die Bindungsdauer gilt nur für zukünftige Kapazitätsreservierungen.

Die Verpflichtungsdauer ist eine Mindestdauer, für die Sie sich verpflichten, die zukünftige Kapazitätsreservierung nach der Bereitstellung in Ihrem Konto im aktiven Status zu haben. Sie können eine Kapazitätsreservierung mit zukünftigem Datum länger als die Bindungsdauer beibehalten, jedoch nicht kürzer. Während der Bindungsdauer gilt Folgendes:

- Sie können eine Kapazitätsreservierung während der Bindungsdauer nicht stornieren.
- Sie können die Anzahl der Instances nicht unter die Anzahl der gebundenen Instances senken, aber Sie können sie erhöhen.

- Sie können eine Kapazitätsreservierung nicht so konfigurieren, dass sie automatisch an einem Datum oder zu einer Uhrzeit endet, die innerhalb der Verpflichtungsdauer liegt. Sie können das Enddatum und die Endzeit während der Bindungsdauer verlängern.

Amazon EC2 verwendet die von Ihnen angegebene Verpflichtungsdauer, um zu beurteilen, ob die Anfrage unterstützt werden kann. Die Bindungsdauer beträgt mindestens 14 Tage. Bei der Prüfung einer Anfrage EC2 kann Amazon zu dem Schluss kommen, dass eine kürzere Bindungsdauer unterstützt werden kann. In diesem Fall plant Amazon EC2 die zukünftige Kapazitätsreservierung mit der kürzeren Bindungsdauer. Das bedeutet, dass Sie sich verpflichten, die Kapazitätsreservierung für einen kürzeren Zeitraum als ursprünglich angefragt auf Ihrem Konto zu behalten.

Bewertung der Kapazitätsreservierung für die Zukunft

Wenn Sie eine zukünftige Kapazitätsreservierung beantragen, EC2 prüft Amazon die Anfrage, um festzustellen, ob sie auf der Grundlage der Kapazitätsverfügbarkeit und der von Ihnen angegebenen Bindungsdauer unterstützt werden kann. Die Bewertung ist in der Regel innerhalb von 5 Tagen abgeschlossen. Amazon EC2 berücksichtigt bei der Bewertung einer Anfrage mehrere Faktoren, darunter:

- Prognostiziertes Kapazitätsangebot
- Die Bindungsdauer
- Wie früh Sie die Kapazitätsreservierung relativ zu Ihrem Startdatum beantragen
- Die Größe der Anforderung

Sie können eine zukünftige Kapazitätsreservierung zwischen 5 und 120 Tagen im Voraus beantragen. Wir empfehlen jedoch, die Anfrage mindestens 56 Tage (8 Wochen) im Voraus zu stellen, damit wir Ihre Anfrage besser unterstützen können. Die Mindestdauer der Bindung beträgt 14 Tage und die Mindestanzahl an Instanzen beträgt 32 CPUs v.

Die Kapazitätsreservierung verbleibt im `assessing`-Status, solange der Antrag bewertet wird.

Wenn die Anfrage unterstützt werden kann, geht die Kapazitätsreservierung in den `scheduled`-Status über und die Lieferung am gewünschten Datum und zur gewünschten Uhrzeit ist geplant. Solange sich die Kapazitätsreservierung im `scheduled`-Status befindet, bleibt die Gesamtzahl der Instances 0. Eine geplante Kapazitätsreservierung wird zum gewünschten Zeitpunkt `active` und kann genutzt werden.

Wenn eine Anfrage nicht unterstützt werden kann, geht die Kapazitätsreservierung in den `unsupported`-Status über. Nicht unterstützte Kapazitätsreservierungen werden nicht zugestellt.

Sie können eine zukünftige Kapazitätsreservierung stornieren, solange sie sich im `assessing`-Status befindet.

Weitere Informationen finden Sie unter Eine zuküftige Kapazitätsreservierung erstellen.

Attribute von Kapazitätsreservierungen

Wenn Sie eine Kapazitätsreservierung erstellen, müssen Sie die folgenden Attribute angeben:

- Availability Zone
- Instance-Typ
- Plattform (Typ des Betriebssystems)
- Tenancy (`default` oder `dedicated`)

Nur Instances, die diesen Attributen entsprechen, können im Rahmen der Kapazitätsreservierung gestartet oder ausgeführt werden.

Kriterien für den Abgleich mit der Instance

Die Kriterien für den Instance-Abgleich oder die Instance-Eignung bestimmen, welche Instances im Rahmen der Kapazitätsreservierung gestartet und ausgeführt werden dürfen. Eine Kapazitätsreservierung kann eines der folgenden übereinstimmenden Kriterien haben:

- Offen – Die Kapazitätsreservierung gleicht automatisch alle Instances mit entsprechenden Attributen (Instance-Typ, Plattform und Availability Zone) ab. Neue und bestehende Instances, die übereinstimmende Attribute aufweisen, laufen automatisch in der Kapazitätsreservierung, ohne dass eine zusätzliche Konfiguration erforderlich ist.
- Zielgerichtet: Die Kapazitätsreservierung akzeptiert nur Instances, die übereinstimmende Attribute aufweisen (Instance-Typ, Plattform und Availability Zone) und explizit auf die Reservierung ausgerichtet sind. Die Instance muss speziell auf die Kapazitätsreservierung abzielen, um in ihrer reservierten Kapazität zu starten oder zu laufen. Auf diese Weise können Sie explizit steuern, welche Instances in der reservierten Kapazität ausgeführt werden dürfen, und das hilft Ihnen, eine unbeabsichtigte Nutzung reservierter Kapazität zu vermeiden.

Wenn Sie eine Kapazitätsreservierung für die Zukunft beantragen, können Sie nur zielgerichtete Übereinstimmungskriterien angeben. Dadurch wird sichergestellt, dass die durch die Kapazitätsreservierung bereitgestellte Kapazität inkrementell oder zusätzlich zu allen laufenden Instances oder der reservierten Kapazität, die Sie zum Zeitpunkt der Bereitstellung haben, erhöht wird. Nachdem die Kapazitätsreservierung in Ihrem Konto aktiv geworden ist, können Sie die Kriterien für den Abgleich der Instance ändern, sodass sie bei Bedarf geöffnet werden. Beachten Sie jedoch, dass alle passenden Instances automatisch in der Kapazitätsreservierung ausgeführt werden. Dies kann zu einer unbeabsichtigten Kapazitätsnutzung führen und Sie daran hindern, neue Instances für die gesamte angeforderte Instance-Anzahl zu starten.

Unterschiede zwischen Kapazitätsreservierungen, Reserved Instances und Savings Plans

Die folgende Tabelle hebt einige der wichtigsten Unterschiede zwischen Kapazitätsreservierungen, Reserved Instances und Savings Plans hervor:

	Capacity Reservations	Zonengebundene Reserved Instances	Regionsgebundene Reserved Instances	Savings Plans
Laufzeit	Für Kapazitätsreservierungen zur sofortigen Nutzung ist keine Bindung erforderlich. Sie können bei Bedarf erstellt, verändert und storniert werden. Bei zukünftigen Kapazitätsreservierungen geben Sie eine Bindungsdauer an, für die Sie sich verpflichten, die Kapazität in Ihrem Konto zu behalten.	Setzen eine feste ein- oder dreijährige Laufzeit voraus.		

	Capacity Reservations	Zonengebundene Reserved Instances	Regionsgebundene Reserved Instances	Savings Plans
	Nach Ablauf der Bindungsdauer können Sie die Kapazitätsreservierung beliebig ändern oder sie stornieren, wenn Sie sie nicht mehr benötigen.			
Kapazität snutzen	In einer bestimmten Availability Zone reservierte Kapazität.		Keine Kapazität reserviert.	
Fakturierungsrabatt	Kein Fakturierungsrabatt. †	Bietet einen Fakturierungsrabatt.		
Instance-Limits	Es gelten Ihre Limits On-Demand-Instance pro Region.	Der Standardwert ist 20 pro Availability Zone. Sie können eine Erhöhung des Limits anfordern.	Der Standardwert ist 20 pro Region. Sie können eine Erhöhung des Limits anfordern.	Kein Limit.

† Sie können Kapazitätsreservierungen mit Savings Plans oder Regional Reserved Instances kombinieren, um einen Rabatt zu erhalten.

Weitere Informationen finden Sie unter:

- Überblick über Reserved Instances für Amazon EC2
- Savings Plans-Benutzerhandbuch

Unterstützte Plattformen

Sie müssen die Kapazitätsreservierung mit der richtigen Plattform erstellen, um sicherzustellen, dass sie optimal mit Ihren Instances abgestimmt ist. Kapazitätsreservierungen unterstützen die folgenden Werte für `platform`:

- Linux/Unix
- Linux mit SQL Server-Standard
- Linux mit SQL Server Web
- Linux mit SQL Server Enterprise
- SUSE Linux
- Red Hat Enterprise Linux
- RHEL mit SQL Server Standard
- RHEL mit SQL Server Enterprise
- RHEL mit SQL Server Web
- RHEL mit HA
- RHEL mit HA und SQL Server Standard
- RHEL mit HA und SQL Server Enterprise
- Ubuntu Pro
- Windows
- Windows mit SQL Server
- Windows mit SQL Server Web
- Windows mit SQL Server-Standard
- Windows mit SQL Server Enterprise

Um sicherzustellen, dass eine Instance in einer bestimmten Kapazitätsreservierung ausgeführt wird, muss die Plattform der Kapazitätsreservierung mit der Plattform des AMI übereinstimmen, das zum Starten der Instance verwendet wurde. Für Linux ist es wichtig zu überprüfen AMIs, ob die AMI-Plattform den allgemeinen Wert Linux/UNIX oder einen spezifischeren Wert wie SUSE Linux verwendet.

Console

So überprüfen Sie die AMI-Plattform

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich AMIs aus.
3. Wählen Sie das AMI aus.
4. Notieren Sie sich auf der Registerkarte Details den Wert der Plattformdetails.

AWS CLI

So überprüfen Sie die AMI-Plattform

Verwenden Sie den Befehl describe-images und überprüfen Sie den Wert von `PlatformDetails`.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[*].PlatformDetails
```

Es folgt eine Beispielausgabe.

```
[
    "Linux/UNIX"
]
```

PowerShell

So überprüfen Sie die AMI-Plattform

Verwenden Sie das Get-EC2ImageCmdlet und überprüfen Sie den Wert von. `PlatformDetails`

```
Get-EC2Image `
    -ImageId ami-0abcdef1234567890 | `
    Select PlatformDetails
```

Es folgt eine Beispielausgabe.

```
PlatformDetails
```

```
---------------
Linux/UNIX
```

Kontingente

Die Anzahl der Instances, für die Sie Kapazität reservieren dürfen, richtet sich nach dem On-Demand-Instance-Kontingent Ihres Kontos. Sie können Kapazität für so viele Instances reservieren, wie es dieses Kontingent erlaubt, abzüglich der Anzahl der bereits ausgeführten Instances.

Kapazitätsreservierungen im Status `assessing`, `scheduled`, `pending`, `active`, und `delayed` und werden auf Ihr On-Demand-Instance-Kontingent angerechnet.

Einschränkungen

Bevor Sie Kapazitätsreservierungen erstellen, beachten Sie bitte die folgenden Begrenzungen und Einschränkungen.

- Aktive und ungenutzte Kapazitätsreservierungen werden auf On-Demand-Instance-Limits angerechnet.
- Kapazitätsreservierungen können nicht von einem AWS Konto auf ein anderes übertragen werden. Sie können Kapazitätsreservierungen jedoch mit anderen AWS Konten teilen. Weitere Informationen finden Sie unter Freigegebene Kapazitätsreservierungen.
- Zonengebundene Reserved Instance-Fakturierungsrabatte gelten nicht für Kapazitätsreservierungen.
- Kapazitätsreservierungen können in Cluster-Placement-Gruppen erstellt werden. Spread- und Partition-Placement-Gruppen werden nicht für unterstützt.
- Kapazitätsreservierungen kann nicht mit Dedicated Hosts verwendet werden. Kapazitätsreservierungen können nicht mit Dedicated Instances verwendet werden.
- [Windows-Instances] Kapazitätsreservierungen können nicht mit Bring Your Own License (BYOL, Verwendung der eigenen Lizenz) verwendet werden.
- [Red-Hat-Instances] Kapazitätsreservierungen können nicht mit Bring Your Own License (BYOL) verwendet werden.
- Kapazitätsreservierungen stellen nicht sicher, dass eine Instance im Ruhezustand fortgesetzt werden kann, nachdem Sie versucht haben, sie zu starten.
- Sie können zukünftige Kapazitätsreservierungen für eine Instance-Anzahl mit mindestens 32 v CPUs beantragen. Wenn Sie beispielsweise eine zukünftige Kapazitätsreservierung für

`m5.xlarge` Instances beantragen, müssen Sie mindestens 8 Instances anfordern (8 * m5.xlarge = 32 v). CPUs

- Sie können Kapazitätsreservierungen für die Zukunft nur für Instance-Typen der folgenden Serien anfordern: C, G, I, M, R und T.

Preise und Fakturierung für Kapazitätsreservierung

Die Themen in diesem Abschnitt geben einen Überblick über Preise und Abrechnung für Kapazitätsreservierungen.

Themen

- Preisgestaltung
- Fakturierung
- Fakturierungsrabatte
- Anzeigen Ihrer Rechnung

Preisgestaltung

Für Kapazitätsreservierungen wird Ihnen der entsprechende On-Demand-Tarif in Rechnung gestellt, unabhängig davon, ob Sie Instances mit der reservierten Kapazität ausführen oder nicht. Wenn Sie die Reservierung nicht nutzen, wird dies auf Ihrer EC2 Amazon-Rechnung als ungenutzte Reservierung ausgewiesen. Wenn Sie eine Instance ausführen, die den Attributen einer Reservierung entspricht, bezahlen Sie nur für die Instance und nichts für die Reservierung. Es gibt keine Vorab- oder Zusatzgebühren.

Wenn Sie beispielsweise eine Kapazitätsreservierung für zwanzig `m4.large`-Linux-Instances erstellen und fünfzehn `m4.large`-Linux-Instances in derselben Availability Zone ausführen, werden Ihnen fünfzehn aktive Instances und fünf ungenutzte Instances in der Reservierung berechnet.

Fakturierungsrabatte für Savings Plans und regionale Reserved Instances gelten für Kapazitätsreservierungen. Weitere Informationen finden Sie unter Fakturierungsrabatte.

Weitere Informationen finden Sie unter Amazon EC2 – Preise.

Fakturierung

Die Abrechnung beginnt, sobald die Kapazitätsreservierung in Ihrem Konto bereitgestellt wurde, und wird fortgesetzt, solange die Kapazitätsreservierung in Ihrem Konto bereitgestellt bleibt. Für

zukünftige Kapazitätsreservierungen bedeutet dies, dass die Abrechnung erst beginnt, wenn die Kapazitätsreservierung zum gewünschten zukünftigen Datum in Ihrem Konto bereitgestellt wurde.

Kapazitätsreservierungen werden mit sekundengenauer Granularität berechnet. Das bedeutet, dass Ihnen angefangene Stunden in Rechnung gestellt werden. Wenn eine Kapazitätsreservierung beispielsweise 24 Stunden und 15 Minuten lang in Ihrem Konto bereitgestellt bleibt, werden Ihnen 24.25 Reservierungsstunden in Rechnung gestellt.

Das folgende Beispiel zeigt, wie eine Kapazitätsreservierung abgerechnet wird. Die Kapazitätsreservierung wurde für eine m4.large-Linux-Instance mit einem On-Demand-Tarif von 0,10 USD pro Nutzungsstunde erstellt. In diesem Beispiel wird die Kapazitätsreservierung im Konto für fünf Stunden lang bereitgestellt. Die Kapazitätsreservierung wird in der ersten Stunde nicht genutzt, sodass in diesem Fall eine ungenutzte Stunde mit dem standardmäßigen On-Demand-Tarif des Instance-Typs m4.large abgerechnet wird. In der zweiten bis fünften Stunde wird die Kapazitätsreservierung von einer m4.large-Instance belegt. In dieser Zeit fallen für die Kapazitätsreservierung keine Gebühren an, stattdessen wird dem Konto die m4.large-Instance in Rechnung gestellt, die diese Kapazitätsreservierung belegt. In der sechsten Stunde wird die Kapazitätsreservierung storniert und die m4.large-Instance arbeitet normalerweise außerhalb der reservierten Kapazität. Für diese Stunde wird der On-Demand-Tarif des Instance-Typs m4.large berechnet.

Hour	1	2	3	4	5	6	Total cost
Unused Capacity Reservation	$0.10	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.10**
On-demand Instance Usage	$0.00	$0.10	$0.10	$0.10	$0.10	$0.10	**$0.50**
Hourly cost	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.60**

Fakturierungsrabatte

Abrechnungsrabatte für Savings Plans und Regional Reserved Instances gelten für Kapazitätsreservierungen. AWS wendet diese Rabatte automatisch auf Kapazitätsreservierungen mit übereinstimmenden Attributen an. Wenn eine Kapazitätsreservierung von einer Instance verwendet wird, wird der Rabatt auf die Instance angewendet. Rabatte werden vorzugsweise auf die Instance-Nutzung angewendet, bevor ungenutzte Kapazitätsreservierungen abgedeckt werden.

Fakturierungsrabatte für zonengebundene Reserved Instances gelten nicht für Kapazitätsreservierungen.

Weitere Informationen finden Sie unter:

- Überblick über Reserved Instances für Amazon EC2
- Savings Plans-Benutzerhandbuch
- Fakturierungs- und Kaufoptionen

Anzeigen Ihrer Rechnung

Sie können die Preise und Gebühren für das Konto in der AWS Fakturierung und Kostenmanagement -Konsole prüfen.

- Das Dashboard zeigt eine Ausgabenzusammenfassung für Ihr Konto an.
- Erweitern Sie auf der Seite Bills (Rechnungen) unter Details den Bereich Elastic Compute Cloud und die Region, um Fakturierungsdaten zu Ihren Kapazitätsreservierungen abzurufen.

Sie können die Gebühren online anzeigen oder eine CSV-Datei herunterladen. Weitere Informationen finden Sie unter Kapazitätsreservierung-Zeilenposten.

Erstellen eines Kapazitätsreservierung

Sie können jederzeit eine Kapazitätsreservierung erstellen, um sicherzustellen, dass Sie in einer bestimmten Availability Zone über verfügbare Datenverabeitungskapazität verfügen. Eine Kapazitätsreservierung kann sofort oder zu einem zukünftigem Zeitpunkt beginnen. Die Kapazität kann erst genutzt werden, wenn die Kapazitätsreservierung den `active`-Status erreicht hat.

> **Note**
>
> Wenn Sie eine Kapazitätsreservierung mit Kriterien für die `open`-Instance-Übereinstimmung erstellen und zum Zeitpunkt, zu dem die Kapazitätsreservierung aktiv wird, Instances mit übereinstimmenden Attributen laufen, werden diese Instances automatisch in der reservierten Kapazität ausgeführt. Um dies zu vermeiden, verwenden Sie Kriterien für den `targeted`-Instance-Abgleich. Weitere Informationen finden Sie unter Kriterien für den Abgleich mit der Instance.

Ihre Anforderung, eine Kapazitätsreservierung zu erstellen, kann bei Eintreten einer der folgenden Bedingungen fehlschlagen:

- Amazon EC2 verfügt nicht über ausreichende Kapazitäten, um die Anfrage zu bearbeiten. Versuchen Sie es entweder zu einem späteren Zeitpunkt noch einmal, versuchen Sie es mit

einer anderen Availability Zone oder versuchen Sie es mit einer kleineren Anfrage. Wenn Ihre Anwendung in Hinsicht auf Instance-Typen und -Größen flexibel ist, versuchen Sie es mit verschiedenen Instance-Attributen.

- Die angeforderte Menge überschreitet Ihr On-Demand-Instance-Limit für die ausgewählte Instance-Familie. Erhöhen Sie Ihr On-Demand-Instance-Limit für die Instance-Familie und versuchen Sie es erneut. Weitere Informationen finden Sie unter Kontingente für On-Demand-Instances.

Themen

- Kapazitätsreservierung zur sofortigen Nutzung erstellen
- Eine zuküftige Kapazitätsreservierung erstellen

Kapazitätsreservierung zur sofortigen Nutzung erstellen

Sie erstellen eine Kapazitätsreservierung zur sofortigen Nutzung.

Console

So erstellen Sie eine Kapazitätsreservierung

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Kapazitätsreservierungen (Kapazitätsreservierungen) und dann Create Kapazitätsreservierung (Kapazitätsreservierung erstellen) aus.
3. Konfigurieren Sie die folgenden Einstellungen im Abschnitt Instance-Details.
   a. Instance-Typ – Der Instance-Typ, für den die Kapazität reserviert werden soll.
   b. Plattform – Das Betriebssystem für Ihre Instances. Weitere Informationen finden Sie unter Unterstützte Plattformen.
   c. Availability Zone – Die Availability Zone, in der die Kapazität reserviert werden soll.
   d. Tenancy – Die Art der Tenancy, die für die reservierte Kapazität verwendet werden soll. Wählen Sie „Standard“, um Kapazität auf gemeinsam genutzter Hardware zu reservieren, oder „Dediziert“, um Kapazität auf Hardware zu reservieren, die Ihrem Konto zugewiesen ist.
   e. (Optional) ARN der Platzierungsgruppe – Der ARN der Cluster-Placement-Gruppe, in der die Kapazitätsreservierung erstellt werden soll. Weitere Informationen finden Sie unter Kapazitätsreservierungen mit Cluster-Placement-Gruppen verwenden.

f. Gesamtzahl der Instances – Die Anzahl der Instances, für die Kapazität reserviert werden soll. Wenn Sie eine neue Menge angeben, die Ihr verbleibendes On-Demand-Instance-Limit für den ausgewählten Instance-Typ überschreitet, schlägt die Anfrage fehl.

4. Konfigurieren Sie die folgenden Einstellungen im Abschnitt Reservation details (Reservierungsdetails):

   a. Kapazitätsreservierung startet – Wählen Sie Sofort.

   b. Kapazitätsreservierung endet – Wählen Sie eine der folgenden Optionen aus:

      - Manuell – Reservieren Sie die Kapazität, bis Sie sie explizit stornieren.
      - Bestimmter Zeitpunkt – Hebt die Kapazitätsreservierung automatisch zum angegebenen Datum und zur festgelegten Uhrzeit auf.

   c. Instance-Berechtigung – Wählen Sie eine der folgenden Optionen aus:

      - Offen – (Standard) Die Kapazitätsreservierung passt zu jeder Instance, die über übereinstimmende Attribute (Instance-Typ, Plattform, Availability Zone und Tenancy) verfügt. Wenn Sie eine Instance mit passenden Attributen starten, wird sie automatisch in der reservierten Kapazität platziert.
      - Zielgerichtet: Die Kapazitätsreservierung akzeptiert nur Instances, die übereinstimmende Attribute aufweisen (Instance-Typ, Plattform, Availability Zone und Tenancy) und explizit auf die Reservierung ausgerichtet sind.

5. Wählen Sie Erstellen aus.

AWS CLI

So erstellen Sie eine Kapazitätsreservierung

Verwenden Sie den Befehl create-capacity-reservation.

```
aws ec2 create-capacity-reservation \
    --availability-zone az_name \
    --instance-type instance_type \
    --instance-count number_of_instances \
    --instance-platform operating_system \
    --instance-match-criteria open|targeted
```

PowerShell

So erstellen Sie eine Kapazitätsreservierung

Verwenden Sie das cmdlet Add-EC2CapacityReservation.

```
Add-EC2CapacityReservation `
    -AvailabilityZone az_name `
    -InstanceType instance_type `
    -InstanceCount number_of_instances `
    -InstancePlatform operating_system `
    -InstanceMatchCriterion open|targeted
```

Eine zukünftige Kapazitätsreservierung erstellen

Wenn Sie eine zukünftige Kapazitätsreservierung beantragen, geben Sie das zukünftige Datum an, an dem die reservierte Kapazität zur Nutzung verfügbar sein soll.

Nachdem Sie eine Kapazitätsreservierung für die Zukunft beantragt haben, wird die bewertung einer Prüfung unterzogen, um festzustellen, ob sie unterstützt werden kann. Weitere Informationen finden Sie unter Bewertung der Kapazitätsreservierung für die Zukunft.

Überlegungen

- Sie können Kapazitätsreservierungen für die Zukunft für Instance-Typen der folgenden Serien anfordern: C, G, I, M, R und T.
- Sie können zukünftige Kapazitätsreservierungen für eine Instance-Anzahl mit mindestens 32 v CPUs beantragen. Wenn Sie beispielsweise eine zukünftige Kapazitätsreservierung für `m5.xlarge` Instances beantragen, müssen Sie Kapazität für mindestens 8 Instances anfordern (8 * m5.xlarge = 32 v). CPUs
- Sie können eine zukünftige Kapazitätsreservierung zwischen 5 und 120 Tagen im Voraus beantragen. Wir empfehlen jedoch, diese mindestens 56 Tage (8 Wochen) im Voraus zu beantragen, um die Supportfähigkeit zu verbessern.
- Die Bindungsdauer beträgt mindestens 14 Tage.

Console

So erstellen Sie eine Kapazitätsreservierung

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Kapazitätsreservierungen (Kapazitätsreservierungen) und dann Create Kapazitätsreservierung (Kapazitätsreservierung erstellen) aus.
3. Konfigurieren Sie die folgenden Einstellungen im Abschnitt Instance-Details.
   a. Instance-Typ – Der Instance-Typ, für den die Kapazität reserviert werden soll.
   b. Plattform – Das Betriebssystem für Ihre Instances. Weitere Informationen finden Sie unter Unterstützte Plattformen.
   c. Availability Zone – Die Availability Zone, in der die Kapazität reserviert werden soll.
   d. Tenancy – Die Art der Tenancy, die für die reservierte Kapazität verwendet werden soll. Wählen Sie „Standard“, um Kapazität auf gemeinsam genutzter Hardware zu reservieren, oder „Dediziert“, um Kapazität auf Hardware zu reservieren, die Ihrem Konto zugewiesen ist.
   e. Gesamtzahl der Instances – Die Anzahl der Instances, für die Kapazität reserviert werden soll. Wenn Sie eine neue Menge angeben, die Ihr verbleibendes On-Demand-Instance-Limit für den ausgewählten Instance-Typ überschreitet, schlägt die Anfrage fehl.
4. Konfigurieren Sie die folgenden Einstellungen im Abschnitt Reservation details (Reservierungsdetails):
   a. Die Kapazitätsreservierung beginnt – Wählen Sie Zu einem bestimmten Zeitpunkt.
   b. Startdatum – Geben Sie das Datum und die Uhrzeit an, zu der die Kapazitätsreservierung verfügbar sein muss. Weitere Informationen finden Sie unter Startdatum und -zeit.
   c. Verpflichtungsdauer – Geben Sie die Mindestdauer an, für die Sie sich verpflichten, die Kapazitätsreservierung auch nach deren Lieferung beizubehalten. Weitere Informationen finden Sie unter Bindungsdauer.
   d. Kapazitätsreservierung endet – Wählen Sie eine der folgenden Optionen aus:
      - Manuell – Reservieren Sie die Kapazität, bis Sie sie explizit stornieren.
      - Bestimmter Zeitpunkt – Hebt die Kapazitätsreservierung automatisch zum angegebenen Datum und zur festgelegten Uhrzeit auf.
5. Wählen Sie Erstellen aus.

AWS CLI

So erstellen Sie eine Kapazitätsreservierung

Verwenden Sie den Befehl create-capacity-reservation.

```
aws ec2 create-capacity-reservation \
    --availability-zone az_name \
    --instance-type instance_type \
    --instance-count number_of_instances \
    --instance-platform operating_system \
    --instance-match-criteria targeted \
    --delivery-preference incremental \
    --commitment-duration commitment_in_seconds \
    --start-date YYYY-MMDDThh:mm:ss.sssZ
```

PowerShell

So erstellen Sie eine Kapazitätsreservierung

Verwenden Sie das cmdlet Add-EC2CapacityReservation.

```
Add-EC2CapacityReservation `
    -AvailabilityZone az_name `
    -InstanceType instance_type `
    -InstanceCount number_of_instances `
    -InstancePlatform operating_system `
    -InstanceMatchCriterion targeted `
    -DeliveryPreference incremental `
    -CommitmentDuration commitment_in_seconds `
    -StartDate  YYYY-MMDDThh:mm:ss.sssZ
```

Den Status einer Kapazitätsreservierung anzeigen

Amazon überwacht EC2 ständig den Status Ihrer Kapazitätsreservierungen.

Aufgrund des Konsistenzmodells, dem die EC2 Amazon-API folgt, kann es nach der Erstellung einer Kapazitätsreservierung bis zu 5 Minuten dauern, bis der Status der Kapazitätsreservierung angezeigt wird`active`. Während dieser Zeit bleibt die Kapazitätsreservierung möglicherweise im Status `pending`. Die Kapazitätsreservierung ist jedoch möglicherweise bereits verfügbar. In diesem Fall werden Versuche, Instances in der Kapazitätsreservierung zu starten, erfogreich.

Console

So zeigen Sie Kapazitätsreservierungen an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Kapazitätsreservierungen aus.
3. Wählen Sie die Kapazitätsreservierung aus.

AWS CLI

So beschreiben Sie Kapazitätsreservierungen

Verwenden Sie den Befehl describe-capacity-reservations.

Mit dem folgenden Befehl werden beispielsweise alle Kapazitätsreservierungen beschrieben.

```
aws ec2 describe-capacity-reservations
```

Es folgt eine Beispielausgabe.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1234abcd56EXAMPLE",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-16T09:03:18.000Z",
            "AvailableInstanceCount": 1,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 1,
            "State": "active",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "a1.medium",
            "PlacementGroupArn": "arn:aws:ec2:us-east-1:123456789012:placement-
group/MyPG"
        },
        {
            "CapacityReservationId": "cr-abcdEXAMPLE9876ef",
```

```
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-07T11:34:19.000Z",
            "AvailableInstanceCount": 3,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 3,
            "State": "cancelled",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "m5.large"
        }
    ]
}
```

PowerShell

So beschreiben Sie eine Kapazitätsreservierung

Verwenden Sie das cmdlet Get-EC2CapacityReservation.

```
Get-EC2CapacityReservation `
    -CapacityReservationId cr-1234abcd56EXAMPLE
```

Status der Kapazitätsreservierungen

Kapazitätsreservierungen können die folgenden Status aufweisen.

Status	Description
`active`	– Die Kapazität ist zur Verwendung verfügbar.
`expired`	Die Kapazitätsreservierung ist automatisch zu dem in Ihrer Reservierungsanforderung angegebenen Datum und der festgelegten Uhrzeit abgelaufen. Die reservierte Kapazität ist nicht mehr für Ihre Nutzung verfügbar.
`cancelled`	Die Kapazitätsreservierung wurde abgebrochen. Die reservierte Kapazität ist nicht mehr für Ihre Nutzung verfügbar.

Status	Description
`pending`	Die Kapazitätsreservierung-Anforderung war erfolgreich, aber die Kapazitätsbereitstellung steht noch aus.
`failed`	Die Kapazitätsreservierung-Anforderung ist fehlgeschlagen. Eine Anforderung kann aufgrund ungültiger Anforderungsparameter, aufgrund von Kapazitätsbeschränkungen oder aufgrund von Instance-Limits fehlschlagen. Anforderungen können bis zu 60 Minuten nach ihrem Fehlschlagen angezeigt werden.
`scheduled`	(Nur für zukünftige Kapazitätsreservierungen) Die Anfrage für zukünftig e Kapazitätsreservierungen wurde genehmigt und die Lieferung der Kapazitätsreservierung ist für den angeforderten Starttermin geplant.
`assessing`	(Nur für zukünftige Kapazitätsreservierungen) Amazon EC2 prüft Ihre Anfrage für eine zukünftige Kapazitätsreservierung. Weitere Informati onen finden Sie unter Bewertung der Kapazitätsreservierung für die Zukunft.
`delayed`	(Nur für zukünftige Kapazitätsreservierungen) EC2 Bei Amazon ist eine Verzögerung bei der Bereitstellung der angeforderten zukünftigen Kapazitätsreservierung aufgetreten. Amazon EC2 ist nicht in der Lage, die angeforderte Kapazität bis zum gewünschten Startdatum und zur gewünschten Startzeit zu liefern.
`unsupported`	(Nur für zukünftige Kapazitätsreservierungen) Amazon EC2 kann die Anfrage für zukünftige Kapazitätsreservierungen aufgrund von Kapazität sbeschränkungen nicht unterstützen. Sie können nicht unterstützte Anfragen 30 Tage lang einsehen. Die Kapazitätsreservierung wird nicht zugestellt werden.

Starten von Instances in einer bestehenden Kapazitätsreservierung

Sie können eine Instance nur in eine Kapazitätsreservierung starten, die:

- Übereinstimmende Attribute (Instance-Typ, Plattform, Availability Zone und Tenancy) hat
- Über ausreichend verfügbare Kapazität verfügt

- Sich im `active`-Status befindet

Wenn Sie eine Instance starten, können Sie angeben, ob die Instance in einer `open` Kapazitätsreservierung, in einer bestimmten Kapazitätsreservierung oder in einer Gruppe von Kapazitätsreservierungen gestartet werden soll.

Alternativ können Sie die Instance so konfigurieren, dass sie nicht in einem Kapazitätsreservierung ausgeführt wird, selbst wenn Sie über eine `open`Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität verfügen.

Das Starten einer Instance in einer Kapazitätsreservierung reduziert ihre verfügbare Kapazität um die Anzahl der gestarteten Instances. Wenn Sie beispielsweise drei Instances starten, wird die verfügbare Kapazität der Kapazitätsreservierung um drei reduziert.

Console

So starten Sie Instances in einer bestehenden Kapazitätsreservierung

1. Folgen Sie den Anweisungen zum Starten einer Instance, aber starten Sie die Instance erst, nachdem Sie die folgenden Schritte durchgeführt haben, um die Einstellungen für die Platzierungsgruppe und Kapazitätsreservierung anzugeben.
2. Erweitern Sie Erweiterte Einstellungen und tun Sie Folgendes:

   a. Wählen Sie unter Platzierungsgruppe die Cluster-Placement-Gruppe aus, in der die Instance gestartet werden soll.
   b. Wählen Sie für Capacity Reservation (Kapazitätsreservierung) je nach Konfiguration der Kapazitätsreservierung eine der folgenden Optionen aus:

      - Keine – Verhindert, dass Instances in eine Kapazitätsreservierung gestartet werden. Die Instances werden in On-Demand-Kapazität ausgeführt.
      - Offen – Startet die Instances in einer jeder Kapazitätsreservierung mit passenden Attributen und ausreichender Kapazität für die von Ihnen ausgewählte Anzahl von Instances. Wenn keine passende Kapazitätsreservierung mit ausreichender Kapazität vorhanden ist, verwendet die Instance On-Demand-Kapazität.
      - Kapazitätsreservierung angeben – startet die Instances in der ausgewählten Kapazitätsreservierung. Wenn die ausgewählte Kapazitätsreservierung nicht über genügend Kapazität für die Anzahl der von Ihnen ausgewählten Instances verfügt, schlägt das Starten der Instances fehl.

- Gruppe für Kapazitätsreservierungs angeben – Startet die Instances in einer beliebigen Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität in der ausgewählten Gruppe für Kapazitätsreservierung. Wenn die ausgewählte Gruppe nicht über eine Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität verfügt, werden die Instances in der On-Demand-Kapazität gestartet.
- Kapazitätsreservierung angeben – startet die Instances in eine ausgewählte Kapazitätsreservierung. Wenn keine Kapazitätsreservierungs-ID angegeben ist, starten die Instances in eine offene Kapazitätsreservierung. Wenn keine Kapazität verfügbar ist, können die Instances nicht gestartet werden.
- Nur Ressourcengruppe Kapazitätsreservierung angeben – Startet die Instances mit einer Kapazitätsreservierung in eine Ressourcengruppe der Kapazitätsreservierung. Wenn kein ARN für die Ressourcengruppe der Kapazitätsreservierung angegeben ist, starten die Instances in eine offene Kapazitätsreservierung. Wenn keine Kapazität verfügbar ist, können die Instances nicht gestartet werden.

3. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus.

AWS CLI

So starten Sie eine Instance in einer bestehenden Kapazitätsreservierung

Verwenden Sie den Befehl run-instances und geben Sie die Option `--capacity-reservation-specification` an.

Das folgende Beispiel startet eine Instance in einer beliebigen offenen Kapazitätsreservierung, die übereinstimmende Attribute und verfügbare Kapazität aufweist:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification CapacityReservationPreference=open
```

Das folgende Beispiel startet eine Instance in einer `targeted`-Kapazitätsreservierung:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification \
        CapacityReservationTarget={CapacityReservationId=cr-1234abcd56EXAMPLE}
```

Das folgende Beispiel startet eine Instance in der angegebenen Kapazitätsreservierungs-Gruppe:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification \

 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-2:123456789012:group/my-cr-group}
```

Das folgende Beispiel startet eine Instance ausschließlich in eine Kapazitätsreservierung. Da keine Kapazitätsreservierung-ID angegeben ist, wird die Instance in jeder offenen Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität gestartet:

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification \
        CapacityReservationPreference=capacity-reservations-only
```

Das folgende Beispiel startet eine Instance ausschließlich in eine angegebene Kapazitätsreservierung. Wenn in der angegebenen Kapazitätsreservierung keine Kapazität verfügbar ist, kann die Instance nicht gestartet werden.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
```

```
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification \
        CapacityReservationPreference=capacity-reservations-only \
        CapacityReservationTarget={CapacityReservationId=cr-1234abcd56EXAMPLE}
```

PowerShell

So starten Sie eine Instance in einer bestehenden Kapazitätsreservierung

Verwenden Sie das cmdlet New-EC2Instance.

Das folgende Beispiel startet eine Instance in einer beliebigen offenen Kapazitätsreservierung, die übereinstimmende Attribute und verfügbare Kapazität aufweist:

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationSpecification_CapacityReservationPreference "open"
```

Das folgende Beispiel startet eine Instance in einer `targeted`-Kapazitätsreservierung:

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationTarget_CapacityReservationId cr-1234abcd56EXAMPLE
```

Das folgende Beispiel startet eine Instance in der angegebenen Kapazitätsreservierungs-Gruppe:

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationTarget_CapacityReservationResourceGroupArn `
```

```
        "arn:aws:resource-groups:us-west-2:123456789012:group/my-cr-group"
```

Das folgende Beispiel startet eine Instance ausschließlich in eine Kapazitätsreservierung. Da keine Kapazitätsreservierung-ID angegeben ist, wird die Instance in jeder offenen Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität gestartet:

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationSpecification_CapacityReservationPreference "capacity-
reservations-only"
```

Das folgende Beispiel startet eine Instance ausschließlich in eine angegebene Kapazitätsreservierung. Wenn in der angegebenen Kapazitätsreservierung keine Kapazität verfügbar ist, kann die Instance nicht gestartet werden.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType t2.micro `
    -KeyName "my-key-pair" `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationSpecification_CapacityReservationPreference "capacity-
reservations-only" `
    -CapacityReservationTarget_CapacityReservationId cr-1234abcd56EXAMPLE
```

Eine aktive Kapazitätsreservierung ändern

Wenn Sie über eine bestehende Kapazitätsreservierung verfügen, die nicht für den Workload geeignet ist, für den die Kapazität benötigt wird, können Sie die Anzahl der Instances, die für die Instance in Frage kommen (`open` oder `targeted`) und die Endzeit (`At specific time` oder `Manually`) ändern. Wenn Sie eine neue Menge angeben, die Ihr verbleibendes On-Demand-Instance-Limit für den ausgewählten Instance-Typ überschreitet, schlägt die Aktualisierung fehl.

Die zulässigen Änderungen hängen vom Status der Kapazitätsreservierung ab:

- `assessing`- oder `scheduled`-Status – Sie können nur die Tags ändern.
- `pending`-Status – Sie können die Kapazitätsreservierung in keiner Weise ändern.

- `active`-Status, aber immer noch innerhalb der Bindungsdauer – Sie können die Anzahl der Instances nicht unter die Anzahl der gebundenen Instances senken oder ein Enddatum festlegen, das vor der festgeschriebenen Bindungsdauer liegt. Alle anderen Änderungen sind zulässig.
- `active`-Status ohne Bindungsdauer oder abgelaufene Bindungsdauer – Alle Änderungen sind zulässig.
- `expired`-, `cancelled`-, `unsupported`- oder `failed`-Status – Sie können die Kapazitätsreservierung in keiner Weise ändern.

Überlegungen

- Sie können den Instance-Typ, die Plattform, die Availability Zone und die Tenancy nach der Erstellung nicht mehr ändern. Wenn Sie eines dieser Attribute ändern müssen, empfehlen wir Ihnen, die Reservierung zu stornieren und dann eine neue mit den erforderlichen Attributen zu erstellen.
- Wenn Sie eine bestehende Kapazitätsreservierung ändern, indem Sie die Instance-Eignung von `targeted` auf `open` ändern, werden alle laufenden Instances, die den Attributen der Kapazitätsreservierung entsprechen, bei denen der Parameter `CapacityReservationPreference` auf `open` gesetzt ist und die noch nicht in einer Kapazitätsreservierung laufen, automatisch die geänderte Kapazitätsreservierung verwenden.
- Um die Instance-Eignung zu ändern, muss die Kapazitätsreservierung vollständig inaktiv sein (keine Nutzung), da Amazon die Instance-Eignung nicht ändern EC2 kann, wenn Instances innerhalb der Reservierung ausgeführt werden.

Console

So ändern Sie eine Kapazitätsreservierung

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Kapazitätsreservierungen, die zu ändernde Kapazitätsreservierung und Edit (bearbeiten) aus.
3. Ändern Sie nach Bedarf die Optionen Gesamtkapazität, Ende der Kapazitätsreservierung oder Instance-Eignung und wählen Sie Speichern.

AWS CLI

So ändern Sie eine Kapazitätsreservierung

Verwenden Sie den Befehl modify-capacity-reservation. Mit dem folgenden Befehl wird die angegebene Kapazitätsreservierung geändert, um Kapazität für acht Instances zu reservieren.

```
aws ec2 modify-capacity-reservation \
    --capacity-reservation-id cr-1234567890abcdef0 \
    --instance-count 8
```

PowerShell

So ändern Sie eine Kapazitätsreservierung

Verwenden Sie das cmdlet Edit-EC2CapacityReservation. Mit dem folgenden Befehl wird die angegebene Kapazitätsreservierung geändert, um Kapazität für acht Instances zu reservieren.

```
Edit-EC2CapacityReservation `
    -CapacityReservationId cr-1234567890abcdef0 `
    -InstanceCount 8
```

Die Einstellungen für die Kapazitätsreservierung Ihrer Instance ändern

Sie können die folgenden Kapazitätsreservierung-Einstellungen für eine angehaltene Instance jederzeit ändern:

- Beginnen Sie mit einer beliebigen Kapazitätsreservierung mit passenden Attributen (Instance-Typ, Plattform,Availability Zone und Tenancy) und verfügbarer Kapazität.
- Start der Instance in einer bestimmten Kapazitätsreservierung vornehmen.
- Beginnen Sie mit einer beliebigen Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität in einer Kapazitätsreservierung-Gruppe.
- Start der Instance in einer Kapazitätsreservierung verhindern.

Console

So ändern Sie die Einstellungen für die Kapazitätsreservierung der Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Instances und wählen Sie die zu ändernde Instance aus. Halten Sie die Instance an, falls Sie das noch nicht getan haben.

3. Wählen Sie Aktionen, Instance-Einstellungen und dann Kapazitätsreservierung-Einstellungen ändern.
4. Wählen Sie unter Kapazitätsreservierung eine der folgenden Optionen aus:

   - Offen – Startet die Instances in einer jeder Kapazitätsreservierung mit passenden Attributen und ausreichender Kapazität für die von Ihnen ausgewählte Anzahl von Instances. Wenn keine passende Kapazitätsreservierung mit ausreichender Kapazität vorhanden ist, verwendet die Instance On-Demand-Kapazität.
   - Keine – Verhindert, dass Instances in eine Kapazitätsreservierung gestartet werden. Die Instances werden in On-Demand-Kapazität ausgeführt.
   - Kapazitätsreservierung angeben – startet die Instances in der ausgewählten Kapazitätsreservierung. Wenn die ausgewählte Kapazitätsreservierung nicht über genügend Kapazität für die Anzahl der von Ihnen ausgewählten Instances verfügt, schlägt das Starten der Instances fehl.
   - Gruppe für Kapazitätsreservierung angeben – Startet die Instances in einer beliebigen Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität in der ausgewählten Gruppe für Kapazitätsreservierung. Wenn die ausgewählte Gruppe nicht über eine Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität verfügt, werden die Instances in der On-Demand-Kapazität gestartet.
   - Kapazitätsreservierung angeben – startet die Instances in eine ausgewählte Kapazitätsreservierung. Wenn keine Kapazitätsreservierungs-ID angegeben ist, starten die Instances in eine offene Kapazitätsreservierung. Wenn keine Kapazität verfügbar ist, können die Instances nicht gestartet werden.
   - Nur Ressourcengruppe Kapazitätsreservierung angeben – Startet die Instances mit einer Kapazitätsreservierung in eine Ressourcengruppe der Kapazitätsreservierung. Wenn kein ARN für die Ressourcengruppe der Kapazitätsreservierung angegeben ist, starten die Instances in eine offene Kapazitätsreservierung. Wenn keine Kapazität verfügbar ist, können die Instances nicht gestartet werden.

AWS CLI

So ändern Sie die Einstellungen für die Kapazitätsreservierung der Instance

Verwenden Sie den Befehl modify-instance-capacity-reservation-attributes.

Das folgende Beispiel ändert die Einstellung der Kapazitätsreservierung auf `none`.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification CapacityReservationPreference=none
```

Das folgende Beispiel wird das Ziel auf eine bestimmte Kapazitätsreservierung gestellt.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification \
    CapacityReservationTarget={CapacityReservationId=cr-1234567890abcdef0}
```

Im folgenden Beispiel wird das Ziel auf eine bestimmte Kapazitätsreservierungsgruppe gestellt.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification \

 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-2:123456789012:group/my-cr-group}
```

Das folgende Beispiel ändert die Einstellung der Kapazitätsreservierung auf `capacity-reservation-only`. Da keine Kapazitätsreservierung angegeben ist, wird die Instance in jeder offenen Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität gestartet:

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification CapacityReservationPreference=capacity-
reservation-only
```

Im folgenden Beispiel wird die Einstellung Kapazitätsreservierung auf `capacity-reservation-only` geändert und das Ziel wird auf eine bestimmte Kapazitätsreservierung geändert. Wenn in der angegebenen Kapazitätsreservierung keine Kapazität verfügbar ist, kann die Instances nicht gestartet werden.

```
aws ec2 modify-instance-capacity-reservation-attributes \
    --instance-id i-1234567890abcdef0 \
    --capacity-reservation-specification \
        CapacityReservationPreference=capacity-reservation-only \
```

```
        CapacityReservationTarget={CapacityReservationId=cr-1234567890abcdef0}
```

PowerShell

So ändern Sie die Einstellungen für die Kapazitätsreservierung der Instance

Verwenden Sie das cmdlet Edit-EC2InstanceCapacityReservationAttribute.

Das folgende Beispiel ändert die Einstellung der Kapazitätsreservierung auf none.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationSpecification_CapacityReservationPreference "none"
```

Das folgende Beispiel wird das Ziel auf eine bestimmte Kapazitätsreservierung gestellt.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationTarget_CapacityReservationId cr-1234567890abcdef0
```

Im folgenden Beispiel wird das Ziel auf eine bestimmte Kapazitätsreservierungsgruppe gestellt.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationTarget_CapacityReservationResourceGroupArn `
        "arn:aws:resource-groups:us-west-2:123456789012:group/my-cr-group"
```

Das folgende Beispiel ändert die Einstellung der Kapazitätsreservierung auf `capacity-reservation-only`. Da keine Kapazitätsreservierung angegeben ist, wird die Instance in jeder offenen Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität gestartet:

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationSpecification_CapacityReservationPreference "capacity-
reservation-only"
```

Im folgenden Beispiel wird die Einstellung Kapazitätsreservierung auf `capacity-reservation-only` geändert und das Ziel wird auf eine bestimmte Kapazitätsreservierung geändert. Wenn in der angegebenen Kapazitätsreservierung keine Kapazität verfügbar ist, kann die Instances nicht gestartet werden.

```
Edit-EC2InstanceCapacityReservationAttribute `
    -InstanceId i-1234567890abcdef0 `
    -CapacityReservationSpecification_CapacityReservationPreference "capacity-
reservation-only" `
    -CapacityReservationTarget_CapacityReservationId cr-1234567890abcdef0
```

Kapazität zwischen Kapazitätsreservierungen verschieben

Sie können Kapazität von einer Kapazitätsreservierung in eine andere verschieben, um Ihre reservierten Rechenressourcen nach Bedarf neu zu verteilen. Wenn Sie beispielsweise in einer Reservierung mit steigender Auslastung zusätzliche Kapazität benötigen und Sie über Kapazitäten in einer anderen Reservierung verfügen, können Sie diese Kapazität zwischen den beiden Reservierungen neu zuweisen.

Voraussetzungen für das Verschieben von Kapazitäten

Voraussetzung ist, dass die beiden Kapazitätsreservierungen die folgenden Anforderungen erfüllen:

- Beide Reservierungen müssen sich im aktiven Status befinden.
- Beide Reservierungen müssen Ihnen AWS-Konto gehören. Sie können keine Kapazität zwischen Reservierungen verschieben, die verschiedenen AWS-Konten gehören.
- Beide Reservierungen müssen dasselbe haben:
  - Instance-Typ
  - Plattform
  - Availability Zone
  - Tenancy
  - Platzierungsgruppe
  - Endzeit

Die Eignung (`open` oder `targeted`) der Ziel-Kapazitätsreservierungs-Instance und die Tags müssen nicht mit der Quellreservierung übereinstimmen. Die Konfiguration beider Reservierungen bleibt gleich, mit der Ausnahme, dass die Kapazität der Quellreservierung reduziert wurde und die Zielreservierung die Kapazität erhöht hat.

Wenn Sie die Anzahl der Instances angeben, die verschoben werden sollen, wird standardmäßig jede verfügbare Kapazität zuerst verschoben, gefolgt von allen infrage kommenden laufenden Instances

(die genutzte Kapazität in Ihrer Reservierung). Wenn Sie beispielsweise 4 Instances aus einer Reservierung mit 5 verwendeten Instances und 3 verfügbaren Instances verschieben, werden die 3 verfügbaren Instances und 1 verwendete Instance verschoben.

> **Note**
>
> Wenn Sie genutzte Kapazität aus Ihrer Reservierung verschieben, indem Sie eine zu verschiebende Menge angeben, die die verfügbare Kapazität übersteigt, open werden nur die Instances verschoben, die mit ihrer Kapazitätsreservierungsspezifikation als gestartet wurden.

Überlegungen

Die folgenden Überlegungen gelten, wenn Kapazität von einer Reservierung in eine andere verschoben wird:

- Die genutzte Kapazität kann nur zwischen Kapazitätsreservierungen mit open-Instance-Berechtigung verschoben werden, die für dieselben Konten freigegeben werden.
- Wenn Sie genutzte Kapazität verschieben, werden die infrage kommenden Instances zufällig ausgewählt. Sie können nicht angeben, welche laufenden Instances verschoben werden. Wenn nicht genügend infrage kommende Instances gefunden werden, um die Anzahl der Verschiebungen zu erfüllen, schlägt der Verschiebungsvorgang fehl.
- Wenn Sie die gesamte Kapazität aus der Quellreservierung verschieben, wird die Kapazitätsreservierung automatisch storniert.
- Zukünftige Kapazitätsreservierungen – Sie können während des Bindungszeitraums keine Kapazität für eine zukünftige Kapazitätsreservierung verschieben.

> **Note**
>
> Das Verschieben von Kapazität aus einem Kapazitätsblock wird nicht unterstützt.

Kapazität verschieben

Sie können Kapazität von einer Quell-Kapazitätsreservierung zu einer Ziel-Kapazitätsreservierung verschieben.

Console

So verschieben Sie Kapazität

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich Kapazitätsreservierungen aus.
3. Wählen Sie eine Reservierungs-ID für On-Demand-Kapazität aus, die Kapazität zum Verschieben enthält.
4. Wählen Sie unter Aktionen, Kapazität verwalten die Option Verschieben aus.
5. Wählen Sie auf der Seite Kapazität verschieben unter Ziel-Kapazitätsreservierung eine Reservierung aus der Liste aus.
6. Verwenden Sie unter Zu verschiebende Menge den Schieberegler oder geben Sie die Anzahl der Instances ein, die Sie von der Quell-Kapazitätsreservierung zur Ziel-Kapazitätsreservierung verschieben wollen.
7. Sehen Sie sich die Zusammenfassung an, und wenn Sie bereit sind, wählen Sie Verschieben aus.

AWS CLI

So verschieben Sie Kapazität

Verwenden Sie den Befehl move-capacity-reservation-instances. Im folgenden Beispiel werden 10 Instances von der angegebenen Quell-Kapazitätsreservierung zur angegebenen Ziel-Kapazitätsreservierung verschoben.

```
aws ec2 move-capacity-reservation-instances \
    --source-capacity-reservation-id cr-1234567890abcdef0 \
    --destination-capacity-reservation-id cr-021345abcdef56789 \
    --instance-count 10
```

PowerShell

So verschieben Sie Kapazität

Verwenden Sie das cmdlet Move-EC2CapacityReservationInstance. Im folgenden Beispiel werden 10 Instances von der angegebenen Quell-Kapazitätsreservierung zur angegebenen Ziel-Kapazitätsreservierung verschoben.

```
Move-EC2CapacityReservationInstance `
    -SourceCapacityReservationId cr-1234567890abcdef0 `
    -DestinationCapacityReservationId cr-021345abcdef56789 `
    -InstanceCount 10
```

Kapazität aus einer bestehenden Kapazitätsreservierung abspalten

Erfahren Sie, wie Sie Kapazität aus einer bestehenden Kapazitätsreservierung abspalten und eine neue Kapazitätsreservierung erstellen. Durch die Aufteilung der Kapazität weisen Sie einen Teil der ursprünglichen Reservierung einem bestimmten Workload zu oder teilen ihn mit einem anderen AWS-Konto. Um beispielsweise eine Kapazitätsreservierung teilweise mit einem anderen Konto zu teilen, können Sie einen Teil der Kapazität aufteilen, um eine kleinere Kapazitätsreservierung zu erstellen. Die kleinere Kapazitätsreservierung kann dann für andere Konten unter Verwendung von AWS Resource Access Manager freigegeben werden.

Wenn Sie Kapazität aus einer bestehenden Kapazitätsreservierung abspalten, wird automatisch eine neue Kapazitätsreservierung angelegt. Die bestehende Reservierung bleibt unverändert, mit Ausnahme der verringerten Gesamtkapazität aufgrund der Anzahl der abgespaltenen Instances. Instances, die im Rahmen der bestehenden Kapazitätsreservierung ausgeführt werden, sind nicht betroffen. Sie können die bestehende Reservierung in nur eine neue Kapazitätsreservierung aufteilen.

Die neue Kapazitätsreservierung wird dieselbe Konfiguration wie die bestehende Kapazitätsreservierung haben, mit Ausnahme von Tags. Standardmäßig hat die neue Kapazitätsreservierung keine Tags. Sie können während des Split-Vorgangs neue Tags angeben. Die neue Kapazitätsreservierung kann bei Bedarf auch nach ihrer Erstellung geändert werden.

Wenn Sie die Anzahl der Instances angeben, die abgespalten werden sollen, wird standardmäßig jede verfügbare Kapazität zuerst abgespalten, gefolgt von allen infrage kommenden laufenden Instances (die genutzte Kapazität in Ihrer Reservierung). Wenn Sie beispielsweise 4 Instances aus einer Kapazitätsreservierung mit 5 verwendeten Instances und 3 verfügbaren Instances verschieben, werden die 3 verfügbaren Instances und 1 verwendete Instance verschoben.

Voraussetzungen für die Aufspaltung der Kapazität

Voraussetzung ist, dass die beiden Kapazitätsreservierungen die folgenden Anforderungen erfüllen:

- Beide Reservierungen müssen sich im aktiven Status befinden.
- Die Quellreservierung muss Ihnen gehören AWS-Konto.

> **Note**
>
> Wenn Sie verbrauchte Kapazität aus Ihrer Reservierung aufteilen, indem Sie eine aufzuteilende Menge angeben, die größer ist als die verfügbare Kapazität, werden nur die Instances aufgeteilt, die mit ihrer Kapazitätsreservierungsspezifikation als `open` gestartet wurden.

Überlegungen

Die folgenden Überlegungen gelten, wenn Kapazität von einer Reservierung in eine andere abgespalten wird:

- Die genutzte Kapazität kann nur für Kapazitätsreservierungen aufgeteilt werden, für die eine „offene“ Instance-Eignung in Frage kommt und die nicht für ein Konto freigegeben werden.
- Wenn Sie genutzte Kapazität verschieben, werden die infrage kommenden Instances zufällig ausgewählt. Sie können nicht angeben, welche laufenden Instances aufgeteilt werden. Wenn nicht genügend infrage kommende Instances gefunden werden, um die Anzahl der Aufteilung zu erfüllen, schlägt der Aufteilungsvorgang fehl.
- Die maximale Anzahl von Instances, die aus einer bestehenden Reservierung aufgeteilt werden können, entspricht der Größe der Reservierung minus eins. Wenn die Gesamtkapazität Ihrer Reservierung beispielsweise 5 Instances beträgt, können Sie maximal 4 Instances in eine neue Reservierung aufteilen.
- Zukünftige Kapazitätsreservierungen – Sie können während des Bindungszeitraums keine Kapazität für eine zukünftige Kapazitätsreservierung aufteilen.
- Ressourcengruppen – Wenn die bestehende Kapazitätsreservierung zu einer Ressourcengruppe gehört, wird die neue Kapazitätsreservierung nicht automatisch zur Ressourcengruppe hinzugefügt. Sie können die neue Kapazitätsreservierung bei Bedarf zu einer Ressourcengruppe hinzufügen, nachdem sie erstellt wurde.
- Freigabe – Wenn die bestehende Kapazitätsreservierung für ein Verbraucherkonto freigegeben wird, wird die neue Kapazitätsreservierung nicht automatisch für den Verbraucherkonto freigegeben. Sie können die neue Kapazitätsreservierung bei Bedarf in einer Ressourcengruppe teilen, nachdem sie erstellt wurde.
- Cluster-Placement-Gruppe – Wenn die bestehende Kapazitätsreservierung Teil einer Cluster-Placement-Gruppe ist, wird die neue Kapazitätsreservierung in derselben Cluster-Placement-Gruppe erstellt.

> **Note**
>
> Das Verschieben von Kapazität aus einem Kapazitätsblock wird nicht unterstützt.

Den Zugriff für die Aufteilung von Kapazitätsreservierungen mithilfe von Tags steuern

Sie können Tags verwenden, um den Zugriff auf EC2 Amazon-Ressourcen zu kontrollieren, einschließlich der Aufteilung von Kapazität aus einer bestehenden Kapazitätsreservierung, um eine neue Kapazitätsreservierung zu erstellen. Weitere Informationen finden Sie unter Steuern des Zugriffs auf AWS Ressourcen mithilfe von Tags im IAM-Benutzerhandbuch.

Um den Zugriff für die Aufteilung einer Kapazitätsreservierung mithilfe von Tags zu kontrollieren, stellen Sie sicher, dass Sie in der Richtlinienerklärung sowohl Ressourcen- als auch Anforderungs-Tags angeben, da IAM-Richtlinien sowohl anhand der Quell-Kapazitätsreservierung als auch anhand der neu erstellten Kapazitätsreservierung bewertet werden. Die folgende Beispielrichtlinie umfasst den `ec2:ResourceTag`-Bedingungsschlüssel mit dem Tag `Owner=ExampleDepartment1` für die Quell-Kapazitätsreservierung und den `ec2:RequestTag`-Bedingungsschlüssel mit dem Tag `stack=production` für die neu erstellte Kapazitätsreservierung.

```
{
  "Statement": [
    {
      "Sid": "AllowSourceCapacityReservation",
      "Effect": "Allow",
      "Action": "ec2:CreateCapacityReservationBySplitting",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:capacity-reservation/
cr-1234567890abcdef0",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Owner": "ExampleDepartment1"
        }
      }
    },
    {
      "Sid": "AllowNewlyCreatedCapacityReservation",
      "Effect": "Allow",
      "Action": ["ec2:CreateCapacityReservationBySplitting", "ec2:CreateTags"],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:capacity-reservation/*",
      "Condition": {
```

```
        "StringEquals": {
          "aws:RequestTag/stack": "production"
        }
      }
    }
  ]
}
```

Kapazität abspalten

Sie können Kapazität aus einer bestehenden Kapazitätsreservierung abspalten und eine neue Kapazitätsreservierung erstellen.

Console

So spalten Sie Kapazität ab

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich Kapazitätsreservierungen aus.
3. Wählen Sie eine Kapazitätsreservierungs-ID aus, die Kapazität zum Aufteilen enthält.
4. Wählen Sie unter Aktionen, Kapazität verwalten die Option Aufteilen aus.
5. Verwenden Sie auf der Seite Kapazitätsreservierung aufteilen unter Aufzuteilende Menge den Schieberegler oder geben Sie die Anzahl der Instances ein, die aus der aktuellen Reservierung aufgeteilt werden sollen.
6. (Optional) Fügen Sie Tags für die neue Kapazitätsreservierung hinzu.
7. Sehen Sie sich die Zusammenfassung an, und wenn Sie bereit sind, wählen Sie Aufteilen aus.

AWS CLI

So spalten Sie Kapazität ab

Verwenden Sie den Befehl `create-capacity-reservation-by-splitting`. Im folgenden Beispiel wird eine neue Kapazitätsreservierung erstellt, indem 10 Instances von der angegebenen Kapazitätsreservierung abgespaltet werden.

```
aws ec2 create-capacity-reservation-by-splitting \
    --source-capacity-reservation-id cr-1234567890abdef0 \
```

```
    --instance-count 10
```

PowerShell

So spalten Sie Kapazität ab

Verwenden Sie das cmdlet New-EC2CapacityReservationBySplitting. Im folgenden Beispiel wird eine neue Kapazitätsreservierung erstellt, indem 10 Instances von der angegebenen Kapazitätsreservierung abgespaltet werden.

```
New-EC2CapacityReservationBySplitting `
    -SourceCapacityReservationId cr-1234567890abdef0 `
    -InstanceCount 10
```

Abbrechen eines Kapazitätsreservierung

Sie können eine Kapazitätsreservierung abbrechen, die sich in einem der folgenden Zustände befindet:

- `assessing`
- `active` und es gibt keine Bindungsdauer oder die Verpflichtungsdauer ist abgelaufen. Sie können eine zukünftige Kapazitätsreservierung während der Bindungsdauer nicht stornieren.

> **Note**
>
> Kapazitätsblöcke können weder bearbeitet noch abgebrochen werden. Weitere Informationen finden Sie unter Kapazitätsblöcke für ML.

Wenn eine Kapazitätsreservierung mit zukünftigem Datum in den `delayed`-Status aufgenommen wird, wird die Bindungsdauer aufgehoben und Sie können sie stornieren, sobald sie den `active`-Status erreicht.

Wenn Sie eine Kapazitätsreservierung stornieren, wird die Kapazität sofort freigegeben und ist nicht mehr zu Ihrer Verwendung reserviert.

Sie können leere Kapazitätsreservierungen und Kapazitätsreservierungen mit laufenden Instances stornieren. Wenn Sie eine Kapazitätsreservierung mit ausgeführten Instances stornieren, werden

die Instances normalerweise außerhalb der Kapazitätsreservierung zu On-Demand-Instance-Standardtarifen oder zu einem ermäßigten Tarif ausgeführt, falls ein entsprechender Savings Plan oder eine entsprechende regionale Reserved Instance vorliegt.

Nachdem Sie eine Kapazitätsreservierung storniert haben, können Instances, die auf sie ausgerichtet sind, nicht mehr starten. Ändern Sie diese Instances, sodass sie entweder auf eine andere Kapazitätsreservierung ausgerichtet sind, starten Sie sie in einer „geöffneten“ Kapazitätsreservierung mit passenden Attributen und ausreichender Kapazität oder vermeiden Sie den Start in einer Kapazitätsreservierung. Weitere Informationen finden Sie unter Die Einstellungen für die Kapazitätsreservierung Ihrer Instance ändern.

Console

So stornieren Sie eine Kapazitätsreservierung

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie erst Kapazitätsreservierungen und dann die zu stornierende Kapazitätsreservierung aus.
3. Wählen Sie Cancel reservation (Reservierung stornieren) und Cancel reservation (Reservierung stornieren) aus.

AWS CLI

So stornieren Sie eine Kapazitätsreservierung

Verwenden Sie den Befehl cancel-capacity-reservation.

```
aws ec2 cancel-capacity-reservation \
    --capacity-reservation-id cr-1234567890abcdef0
```

PowerShell

So stornieren Sie eine Kapazitätsreservierung

Verwenden Sie das cmdlet Remove-EC2CapacityReservation.

```
Remove-EC2CapacityReservation `
    -CapacityReservationId cr-1234567890abcdef0
```

Kapazitätsreservierungen mit Cluster-Placement-Gruppen verwenden

Sie können Kapazitätsreservierungen in einer Cluster-Platzierungsgruppe erstellen, um EC2 Amazon-Rechenkapazität für Ihre Workloads zu reservieren. Cluster-Placement-Gruppen bieten die Vorteile einer geringen Netzwerklatenz und eines hohen Netzwerkdurchsatzes.

Durch das Erstellen einer Kapazitätsreservierung in einer Cluster-Placement-Gruppe stellen Sie sicher, dass Sie bei Bedarf so lange wie nötig auf Rechenkapazität in Ihren Cluster-Placement-Gruppen zugreifen können. Dies ist ideal zum Reservieren von Kapazitäten für High-Performance-Computing-Workloads (HPC-Workloads), die eine Skalierung erfordern. So skalieren Sie Ihren Cluster nach unten und stellen gleichzeitig sicher, dass die Kapazität für Ihre Verwendung verfügbar bleibt, sodass Sie bei Bedarf wieder nach oben skalieren können.

Nachdem Sie eine Kapazitätsreservierung in einer Cluster-Placement-Gruppe erstellt haben, können Sie diese für andere AWS -Konten freigeben. Weitere Informationen finden Sie unter Kapazitätsreservierungen in Cluster-Placement-Gruppen freigeben.

Themen

- Einschränkungen
- Arbeiten mit Kapazitätsreservierungen in Cluster-Placement-Gruppen
- Kapazitätsreservierungen in Cluster-Placement-Gruppen freigeben

Einschränkungen

Beachten Sie beim Erstellen von Kapazitätsreservierungen in Cluster-Placement-Gruppen Folgendes:

- Befindet sich eine bestehende Kapazitätsreservierung nicht in einer Placement-Gruppe, können Sie die Kapazitätsreservierung nicht ändern, um Kapazität in einer Placement-Gruppe zu reservieren. Um Kapazität in einer Platzierungsgruppe zu reservieren, müssen Sie die Kapazitätsreservierung in der Platzierungsgruppe erstellen.
- Nachdem Sie eine Kapazitätsreservierung in einer Platzierungsgruppe erstellt haben, können Sie diese nicht ändern, um Kapazität außerhalb der Platzierungsgruppe zu reservieren.
- Sie können die reservierte Kapazität in einer Platzierungsgruppe erhöhen, indem Sie eine vorhandene Kapazitätsreservierung in der Platzierungsgruppe bearbeiten oder zusätzliche Kapazitätsreservierungen in der Platzierungsgruppe erstellen. Dadurch steigt jedoch das Risiko eines Fehlers wegen unzureichender Kapazität.

- Sie können Kapazitätsreservierungen nur von der Cluster-Placement-Gruppe aus freigeben, deren Eigentümer Sie sind. Sie können Kapazitätsreservierungen nicht von einer Cluster-Placement-Gruppe aus freigeben, deren Eigentümer Sie nicht sind.
- Sie können Cluster-Placement-Gruppen mit `active` Kapazitätsreservierungen nicht löschen. Sie müssen alle Kapazitätsreservierungen in der Cluster-Placement-Gruppe stornieren, bevor Sie sie löschen können.

Arbeiten mit Kapazitätsreservierungen in Cluster-Placement-Gruppen

Führen Sie die folgenden Schritte aus, um Kapazitätsreservierungen in Cluster-Placement-Gruppen zu verwenden.

> **Note**
>
> Wenn Sie eine Kapazitätsreservierung in einer vorhandenen Cluster-Placement-Gruppe erstellen möchten, überspringen Sie Schritt 1. Geben Sie dann für die Schritte 2 und 3 den ARN der vorhandenen Cluster-Placement-Gruppe an.

Aufgaben

- Schritt 1: (Bedingt) Erstellen einer Cluster-Placement-Gruppe zur Verwendung mit einer Kapazitätsreservierung
- Schritt 2: Erstellen einer Kapazitätsreservierung in einer Cluster-Placement-Gruppe
- Schritt 3: Instances in Kapazitätsreservierungen einer Cluster-Placement-Gruppe starten

Schritt 1: (Bedingt) Erstellen einer Cluster-Placement-Gruppe zur Verwendung mit einer Kapazitätsreservierung

Führen Sie diesen Schritt nur aus, wenn Sie eine neue Cluster-Placement-Gruppe erstellen müssen. Um eine vorhandene Cluster-Placement-Gruppe zu verwenden, überspringen Sie diesen Schritt und verwenden Sie dann für die Schritte 2 und 3 den ARN dieser Cluster-Placement-Gruppe.

Console

Eine Cluster-Placement-Gruppe erstellen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Placement Groups (Placement-Gruppen) und Create Placement Group (Placement-Gruppe erstellen) aus.
3. Geben Sie unter Name einen beschreibenden Namen für die Platzierungsgruppe an.
4. Legen Sie für die Platzierungsstrategie Cluster fest.
5. Wählen Sie Create group (Gruppe erstellen) aus.
6. Notieren Sie sich in der Tabelle Placement-Gruppen in der Spalte Gruppen-ARN den ARN der Cluster-Placement-Gruppe, die Sie erstellt haben. Sie benötigen die Notiz für den nächsten Schritt.

AWS CLI

Eine Cluster-Placement-Gruppe erstellen

Verwenden Sie den Befehl create-placement-group.

```
aws ec2 create-placement-group \
    --group-name MyPG \
    --strategy cluster
```

Notieren Sie sich den ARN der Platzierungsgruppe, die in der Ausgabe zurückgegeben wurde, da Sie ihn für den nächsten Schritt benötigen.

PowerShell

Eine Cluster-Placement-Gruppe erstellen

Verwenden Sie das cmdlet New-EC2PlacementGroup.

```
New-EC2PlacementGroup `
    -GroupName my-placement-group `
    -Strategy "cluster"
```

Notieren Sie sich den ARN der Platzierungsgruppe, die in der Ausgabe zurückgegeben wurde, da Sie ihn für den nächsten Schritt benötigen.

Schritt 2: Erstellen einer Kapazitätsreservierung in einer Cluster-Placement-Gruppe

Eine Kapazitätsreservierung in einer Cluster-Placement-Gruppe erstellen Sie auf die gleiche Weise wie eine Kapazitätsreservierung. Sie müssen jedoch auch den ARN der Cluster-Placement-Gruppe angeben, in der die Kapazitätsreservierung erstellt werden soll.

Überlegungen

- Die angegebene Cluster-Placement-Gruppe muss sich im Zustand `available` befinden. Wenn sich die Cluster-Placement-Gruppe im Zustand `pending`, `deleting` oder `deleted` befindet, schlägt die Anforderung fehl.
- Die Kapazitätsreservierung und die Cluster-Placement-Gruppe müssen sich in derselben Availability Zone befinden. Wenn bei der Anforderung zum Erstellen der Kapazitätsreservierung eine Availability Zone angegeben wird, die sich von der der Cluster-Placement-Gruppe unterscheidet, schlägt die Anforderung fehl.
- Sie können Kapazitätsreservierungen nur für Instance-Typen erstellen, die von Cluster-Placement-Gruppen unterstützt werden. Wenn Sie einen nicht unterstützten Instance-Typ angeben, schlägt die Anforderung fehl.
- Wenn Sie eine `open` Kapazitätsreservierung in einer Cluster-Placement-Gruppe erstellen und ausgeführte Instances mit übereinstimmenden Attributen (ARN der Platzierungsgruppe, Instance-Typ, Availability Zone, Plattform und Tenancy) vorhanden sind, werden diese Instances automatisch in der Kapazitätsreservierung ausgeführt.
- Ihre Anforderung, eine Kapazitätsreservierung zu erstellen, kann bei Eintreten einer der folgenden Bedingungen fehlschlagen:
  - Amazon EC2 verfügt nicht über ausreichende Kapazitäten, um die Anfrage zu bearbeiten. Versuchen Sie es entweder zu einem späteren Zeitpunkt erneut oder probieren Sie es erneut mit einer anderen Availability Zone oder einer kleineren Kapazität. Wenn Ihr Workload in Hinsicht auf Instance-Typen und -Größen flexibel ist, versuchen Sie es mit verschiedenen Instance-Attributen.
  - Die angeforderte Menge überschreitet Ihr On-Demand-Instance-Limit für die ausgewählte Instance-Familie. Erhöhen Sie Ihr On-Demand-Instance-Limit für die Instance-Familie und versuchen Sie es erneut. Weitere Informationen finden Sie unter Kontingente für On-Demand-Instances.

Console

So erstellen Sie eine Kapazitätsreservierung

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Kapazitätsreservierungen (Kapazitätsreservierungen) und dann Create Kapazitätsreservierung (Kapazitätsreservierung erstellen) aus.
3. Konfigurieren Sie auf der Seite Erstellen einer Kapazitätsreservierung den Instance-Typ, die Plattform, die Availability Zone, die Tenancy, die Menge und das Enddatum nach Bedarf.
4. Geben Sie für Placement-Gruppe den ARN der Cluster-Placement-Gruppe an, in der die Kapazitätsreservierung erstellt werden soll.
5. Wählen Sie Erstellen aus.

Weitere Informationen finden Sie unter Erstellen eines Kapazitätsreservierung.

AWS CLI

So erstellen Sie eine Kapazitätsreservierung

Verwenden Sie den Befehl create-capacity-reservation. Geben Sie für `--placement-group-arn` den ARN der Cluster-Placement-Gruppe an, in der die Kapazitätsreservierung erstellt werden soll.

```
aws ec2 create-capacity-reservation \
    --instance-type instance_type \
    --instance-platform platform \
    --availability-zone-id az_id \
    --instance-count quantity \
    --placement-group-arn "placement_group_arn"
```

PowerShell

So erstellen Sie eine Kapazitätsreservierung

Verwenden Sie das cmdlet Add-EC2CapacityReservation. Geben Sie für `-PlacementGroupArn` den ARN der Cluster-Placement-Gruppe an, in der die Kapazitätsreservierung erstellt werden soll.

```
Add-EC2CapacityReservation `
    -InstanceType instance_type `
```

```
    -InstancePlatform platform `
    -AvailabilityZoneId az_id `
    -InstanceCount quantity `
    -PlacementGroupArn "placement_group_arn"
```

Schritt 3: Instances in Kapazitätsreservierungen einer Cluster-Placement-Gruppe starten

Sie können mit einer der folgenden Optionen eine Instance in einer Kapazitätsreservierung einer Cluster-Placement-Gruppe starten:

- Angabe des ARN der Cluster-Placement-Gruppe, in der die Instance gestartet werden soll — Wenn Sie den ARN einer Cluster-Placement-Gruppe angeben, EC2 startet Amazon die Instance in dieser Cluster-Placement-Gruppe. Sie können eine der folgenden Methoden verwenden:
  - *open* angeben – Sie müssen die Kapazitätsreservierung in der Instance-Startanforderung nicht angeben. Wenn Attribute der Instance (ARN der Platzierungsgruppe, Instance-Typ, Availability Zone, Plattform und Tenancy) mit einer Kapazitätsreservierung in der angegebenen Platzierungsgruppe übereinstimmen, wird diese Instance automatisch in der Kapazitätsreservierung ausgeführt.
  - Eine Kapazitätsreservierung angeben – Wenn von der Kapazitätsreservierung nur gezielte Instance-Starts akzeptiert werden, müssen Sie bei der Anforderung zusätzlich zur Cluster-Placement-Gruppe die Ziel-Kapazitätsreservierung angeben.
  - Eine Kapazitätsreservierungsgruppe angeben – Weitere Informationen finden Sie unter Verwenden der Kapazitätsreservierung in Cluster-Placement-Gruppen mit einer Kapazitätsreservierungsgruppe.
- Nur eine Kapazitätsreservierungsgruppe angeben – Weitere Informationen finden Sie unter Verwenden der Kapazitätsreservierung in Cluster-Placement-Gruppen mit einer Kapazitätsreservierungsgruppe.
- Nur eine Kapazitätsreservierung angeben – Sie können Instances in einer Kapazitätsreservierung einer Cluster-Placement-Gruppe starten.

> **Note**
>
> Wenn Sie Instances starten, indem Sie nur eine Kapazitätsreservierung oder nur eine Kapazitätsreservierungsgruppe angeben, werden die Instances in den Kapazitätsreservierungen gestartet, die in der Cluster-Placement-Gruppe erstellt wurden, aber die Instances sind nicht direkt an die Cluster-Placement-Gruppe angehängt.

Console

So starten Sie Instances in einer bestehenden Kapazitätsreservierung

1. Folgen Sie den Anweisungen zum Starten einer Instance, aber starten Sie die Instance erst, nachdem Sie die folgenden Schritte durchgeführt haben, um die Einstellungen für die Platzierungsgruppe und Kapazitätsreservierung anzugeben.
2. Erweitern Sie Erweiterte Einstellungen und tun Sie Folgendes:
   a. Wählen Sie unter Platzierungsgruppe die Cluster-Placement-Gruppe aus, in der die Instance gestartet werden soll.
   b. Wählen Sie für Capacity Reservation (Kapazitätsreservierung) je nach Konfiguration der Kapazitätsreservierung eine der folgenden Optionen aus:
      - Offen – Um die Instances in eine beliebige `open` Kapazitätsreservierung in der Cluster-Placement-Gruppe zu starten, die übereinstimmende Attribute und ausreichend Kapazität hat.
      - Ziel nach ID – Um die Instances in einer Kapazitätsreservierung zu starten, die nur gezielte Instance-Starts zulässt.
      - Ziel nach Gruppe – Um die Instances in eine beliebige Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität in der ausgewählten Gruppe für Kapazitätsreservierung zu starten.
3. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten.

AWS CLI

So starten Sie Instances in einer bestehenden Kapazitätsreservierung

Verwenden Sie den Befehl run-instances. Wenn Sie eine bestimmte Kapazitätsreservierung oder eine Kapazitätsreservierungsgruppe anvisieren müssen, geben Sie den Parameter `--capacity-reservation-specification` an. Geben Sie für `--placement` den Parameter `GroupName` und dann dann den Namen der Platzierungsgruppe an, die Sie in den vorherigen Schritten erstellt haben.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
```

```
    --count quantity \
    --instance-type instance_type \
    --key-name key_pair_name \
    --subnet-id subnet-0abcdef1234567890 \
    --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=capacity_reservation_id} \
    --placement "GroupName=cluster_placement_group_name"
```

PowerShell

So starten Sie Instances in einer bestehenden Kapazitätsreservierung

Verwenden Sie das cmdlet New-EC2Instance. Geben Sie für `-Placement` den Parameter `GroupName` und dann dann den Namen der Platzierungsgruppe an, die Sie in den vorherigen Schritten erstellt haben.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType instance_type `
    -KeyName key_pair_name `
    -SubnetId subnet-0abcdef1234567890 `
    -CapacityReservationTarget_CapacityReservationId capacity_reservation_id `
    -Placement_GroupName cluster_placement_group_name
```

Kapazitätsreservierungen in Cluster-Placement-Gruppen freigeben

Sie können Kapazitätsreservierungen in Cluster-Platzierungsgruppen gemeinsam nutzen, indem Sie entweder nur die Kapazitätsreservierungen freigeben oder indem Sie sowohl die Kapazitätsreservierungen als auch die Cluster-Placement-Gruppe, in der sie erstellt wurden, freigeben.

Indem Sie nur die Kapazitätsreservierung freigeben, gewähren Sie Verbraucherkonten nur Zugriff auf diese Kapazitätsreservierung. Verbraucherkonten haben keine Sichtbarkeit oder keinen Zugriff auf die Cluster-Placement-Gruppe, in der die Kapazitätsreservierung erstellt wurde. Auf diese Weise haben Sie eine fein abgestufte Kontrolle über den Zugriff auf Verbraucherkonten. Verbraucherkonten können keine Informationen über die Cluster-Placement-Gruppe anzeigen, einschließlich ihres ARN.

Wenn Sie die Cluster-Placement-Gruppe und die Kapazitätsreservierung gemeinsam nutzen, ist die Cluster-Placement-Gruppe sichtbar und für Verbraucherkonten zugänglich. Sie können Instances starten und darin ihre eigenen Kapazitätsreservierungen erstellen.

Weitere Informationen finden Sie in den folgenden Ressourcen.

- Starten von Instances in Kapazitätsreservierungen einer Cluster-Placement-Gruppe
- Freigegebene Kapazitätsreservierungen
- Freigegebene Platzierungsgruppen

Kapazitätsreservierungs-Gruppen

Sie können sie verwenden AWS -Ressourcengruppen , um logische Sammlungen von Kapazitätsreservierungen zu erstellen, die als Ressourcengruppen bezeichnet werden. Eine Ressourcengruppe ist eine logische Gruppierung von AWS Ressourcen, die sich alle in derselben AWS Region befinden. Weitere Informationen zu Ressourcengruppen finden Sie unter Was sind Ressourcengruppen? im AWS -Ressourcengruppen -Benutzerhandbuch.

Sie können Kapazitätsreservierungen, die Sie besitzen, in Ihr Konto aufnehmen, und Kapazitätsreservierungen, die von anderen AWS Konten mit Ihnen geteilt wurden, in eine einzige Ressourcengruppe aufnehmen. Sie können auch Kapazitätsreservierungen mit unterschiedlichen Attributen (Instance-Typ, Plattform, Availability Zone und Tenancy) in eine einzelne Ressourcengruppe aufnehmen.

Wenn Sie Ressourcengruppen für Kapazitätsreservierungen erstellen, können Sie Instances auf eine Gruppe von Kapazitätsreservierungen statt auf eine einzelne Kapazitätsreservierung ausrichten. Instances, die eine Gruppe von Kapazitätsreservierungen anzielen, stimmen mit jeder Kapazitätsreservierung in der Gruppe überein, die übereinstimmende Attribute (Instance-Typ, Plattform, Availability Zone und Tenancy) und verfügbare Kapazität aufweist. Wenn die Gruppe nicht über eine Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität verfügt, werden die Instances mit On-Demand-Kapazität ausgeführt. Wenn der Zielgruppe zu einem späteren Zeitpunkt eine übereinstimmende Kapazitätsreservierung hinzugefügt wird, wird die Instance automatisch mit ihrer reservierten Kapazität abgeglichen und in diese verschoben.

Um eine unbeabsichtigte Verwendung von Kapazitätsreservierungen in einer Gruppe zu verhindern, konfigurieren Sie die Kapazitätsreservierungen in der Gruppe so, dass nur Instances akzeptiert werden, die explizit die Kapazitätsreservierung anvisieren. Stellen Sie dazu die Instance-Eignung auf Nur Instances ein, die diese Reservierung angeben, wenn Sie die Kapazitätsreservierung über die EC2 Amazon-Konsole erstellen. Geben Sie bei der Verwendung von an AWS CLI, `--instance-match-criteria targeted` wann Sie die Kapazitätsreservierung erstellen. Dadurch wird sichergestellt, dass nur Instances, die explizit die Gruppe oder eine Kapazitätsreservierung in der Gruppe anvisieren, in der Gruppe ausgeführt werden können.

Wenn eine Kapazitätsreservierung in einer Gruppe abgebrochen wird oder abläuft, während auf ihr Instances ausgeführt werden, werden die Instances automatisch in eine andere Kapazitätsreservierung in der Gruppe verschoben, die über übereinstimmende Attribute und verfügbare Kapazität verfügt. Wenn es in der Gruppe keine verbleibenden Kapazitätsreservierungen mit übereinstimmenden Attributen und verfügbarer Kapazität vorhanden sind, werden die Instances in On-Demand-Kapazität ausgeführt. Wenn der anvisierten Gruppe zu einem späteren Zeitpunkt eine passende Kapazitätsreservierung hinzugefügt wird, wird die Instance automatisch in ihre reservierte Kapazität verschoben.

Aufgaben

- Erstellen einer Kapazitätsreservierungsgruppe
- Hinzufügen einer Kapazitätsreservierung zu einer Gruppe
- Entfernen einer Kapazitätsreservierung aus einer Gruppe
- Löschen einer Kapazitätsreservierungsgruppe
- Verwenden der Kapazitätsreservierung in Cluster-Placement-Gruppen mit einer Kapazitätsreservierungsgruppe

Erstellen einer Kapazitätsreservierungsgruppe

Sie können die folgenden Beispiele verwenden, um eine Ressourcengruppe für Kapazitätsreservierungen mit den folgenden Anforderungsparametern zu erstellen.

- `AWS::EC2::CapacityReservationPool` – Stellt sicher, dass die Ressourcengruppe als Ziel für Instance-Starts eingerichtet werden kann.
- `AWS::ResourceGroups::Generic` mit `allowed-resource-types` auf `AWS::EC2::CapacityReservation` gesetzt – Stellt sicher, dass die Ressourcengruppe nur Kapazitätsreservierungen akzeptiert.

Nachdem Sie eine Gruppe erstellt haben, können Sie der Gruppe Kapazitätsreservierungen hinzufügen.

AWS CLI

So erstellen Sie eine Kapazitätsreservierungsgruppe

Verwenden Sie den Befehl create-group AWS CLI .

```
aws resource-groups create-group \
    --name MyCRGroup \
    --configuration \
        '{"Type": "AWS::EC2::CapacityReservationPool"}' \
        '{"Type": "AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-
resource-types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

PowerShell

So erstellen Sie eine Kapazitätsreservierungsgruppe

Verwenden Sie das Cmdlet New- RGGroup.

```
New-RGGroup `
    -Name MyCRGroup `
    -Configuration `
        @{"Type"="AWS::EC2::CapacityReserationPool"} `
        @{"Type"="AWS::ResourceGroups::Generic"; "Parameters"=@{"allowed-resource-
types"=@{"Values"="AWS::EC2::CapacityReservations"}}}
```

Hinzufügen einer Kapazitätsreservierung zu einer Gruppe

Wenn Sie eine für Sie freigegebene Kapazitätsreservierung zu einer Gruppe hinzufügen und diese Kapazitätsreservierung nicht freigegeben ist, wird sie automatisch aus der Gruppe entfernt.

AWS CLI

So fügen Sie eine Kapazitätsreservierung zu einer Gruppe hinzu

Verwenden Sie den Befehl group-resources.

Mit dem folgenden Befehl werden beispielsweise zwei Kapazitätsreservierungen zur angegebenen Gruppe hinzugefügt.

```
aws resource-groups group-resources \
    --group MyCRGroup \
    --resource-arns \
        arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1
 \
        arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

PowerShell

So fügen Sie eine Kapazitätsreservierung zu einer Gruppe hinzu

Verwenden Sie das RGResource Cmdlet Add-.

Mit dem folgenden Befehl werden beispielsweise zwei Kapazitätsreservierungen zur angegebenen Gruppe hinzugefügt.

```
Add-RGResource `
    -Group MyCRGroup `
    -ResourceArn `
        "arn:aws:ec2:sa-east-1:123456789012:capacity-
reservation/cr-1234567890abcdef1", `
        "arn:aws:ec2:sa-east-1:123456789012:capacity-
reservation/cr-54321abcdef567890"
```

Entfernen einer Kapazitätsreservierung aus einer Gruppe

Sie können die folgenden Beispiele verwenden, um eine Kapazitätsreservierung aus einer Gruppe zu entfernen.

AWS CLI

So entfernen Sie eine Kapazitätsreservierung aus einer Gruppe

Verwenden Sie den Befehl ungroup-resources.

Im folgenden Beispiel werden zwei Kapazitätsreservierungen aus der angegebenen Gruppe entfernt.

```
aws resource-groups ungroup-resources \
    --group MyCRGroup \
    --resource-arns \
        arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd
 \
        arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

PowerShell

So entfernen Sie eine Kapazitätsreservierung aus einer Gruppe

Verwenden Sie das Cmdlet Remove- RGResource.

Im folgenden Beispiel werden zwei Kapazitätsreservierungen aus der angegebenen Gruppe entfernt.

```
Remove-RGResource `
    -Group MyCRGroup `
    -ResourceArn `
        "arn:aws:ec2:sa-east-1:123456789012:capacity-
reservation/cr-0e154d26a16094dd", `
        "arn:aws:ec2:sa-east-1:123456789012:capacity-
reservation/cr-54321abcdef567890"
```

Löschen einer Kapazitätsreservierungsgruppe

Sie können die folgenden Beispiele verwenden, um eine Kapazitätsreservierungsgruppe zu löschen.

AWS CLI

So löschen Sie eine Gruppe

Verwenden Sie den Befehl delete-group.

```
aws resource-groups delete-group --group MyCRGroup
```

PowerShell

So löschen Sie eine Gruppe

Verwenden Sie das Cmdlet Remove- RGGroup.

```
Remove-RGGroup -GroupName MyCRGroup
```

Verwenden der Kapazitätsreservierung in Cluster-Placement-Gruppen mit einer Kapazitätsreservierungsgruppe

Amazon EC2 bietet verschiedene Startmethoden, mit denen Sie Kapazitätsreservierungen in einer Cluster-Platzierungsgruppe mit einer Kapazitätsreservierungsgruppe verwenden können. Sie können auf der Grundlage Ihrer Workload-Anforderungen eine der folgenden Methoden auswählen, um eine Kapazitätsreservierungsgruppe als Ziel auszuwählen:

- Den ARN der Cluster-Placement-Gruppe und der Kapazitätsreservierungsgruppe angeben – Dies wird eine beliebige verfügbare Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität in der ausgewählten Kapazitätsreservierungsgruppe verwenden. Wenn die ausgewählte Gruppe nicht über eine Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität verfügt, werden die Instances in der On-Demand-Kapazität gestartet.

  > **Note**
  >
  > Wenn Sie Instances mit dieser Methode starten, werden die Instances der angegebenen Cluster-Placement-Gruppe zugeordnet.

- Nur eine Kapazitätsreservierungsgruppe angeben – Dadurch wird die gesamte verfügbare Kapazität innerhalb der Kapazitätsreservierungsgruppe verwendet, indem nur die Kapazitätsreservierungsgruppe angegeben wird. Beim Starten von Instances wird die Kapazität in der folgenden Reihenfolge genutzt:
  - Kapazitätsreservierungen, die keiner Cluster-Placement-Gruppe zugeordnet sind.
  - Kapazitätsreservierung in einer beliebigen Cluster-Placement-Gruppe innerhalb der Kapazitätsreservierungsgruppe.
  - Wenn die Gruppe nicht über eine Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität verfügt, werden die Instances mit On-Demand-Kapazität ausgeführt und nicht in eine Cluster-Placement-Gruppe platziert.

  > **Note**
  >
  > Wenn Sie Instances starten, indem Sie nur eine Kapazitätsreservierungsgruppe angeben, werden die Instances in den Kapazitätsreservierungen gestartet, die in der Cluster-Placement-Gruppe erstellt wurden, aber die Instances werden nicht direkt an die Cluster-Placement-Gruppe angehängt.

Kapazitätsreservierungen in Local Zones

Eine lokale Zone ist eine Erweiterung einer AWS Region, die sich geografisch in der Nähe Ihrer Benutzer befindet. Ressourcen, die in einer Local Zone erstellt wurden, können von lokalen Benutzern mit sehr latenzarmen Verbindungen genutzt werden. Weitere Informationen finden Sie unter AWS -Local Zones.

Sie können eine VPC von ihrer übergeordneten AWS Region in eine lokale Zone erweitern, indem Sie in dieser lokalen Zone ein neues Subnetz erstellen. Wenn Sie ein Subnetz in einer Local Zone erstellen, wird Ihre VPC auf diese Local Zone erweitert. Das Subnetz in der Local Zone funktioniert genauso wie andere Subnetze in Ihrer VPC.

Mithilfe von Local Zones können Sie Kapazitätsreservierungen an mehreren Speicherorten platzieren, die näher an Ihren Benutzern liegen. Sie erstellen und verwenden Kapazitätsreservierungen in Local Zones auf die gleiche Weise, wie Sie Kapazitätsreservierungen in regulären Availability Zones erstellen und verwenden. Es gelten dieselben Features und dasselbe Verhalten der Instance-Übereinstimmung. Weitere Informationen zu den Preismodellen, die in Local Zones unterstützt werden, finden Sie unter AWS Local Zones FAQs.

Überlegungen

Sie können in einer Local Zone keine Kapazitätsreservierung-Gruppen verwenden.

Verwenden einer Kapazitätsreservierung in einer Local Zone

1. Aktivieren Sie die lokale Zone für die Verwendung in Ihrem AWS Konto. Weitere Informationen finden Sie unter Erste Schritte mit AWS Local Zones im AWS Local Zones User Guide.
2. Erstellen Sie eine Kapazitätsreservierung in der Local Zone. Wählen Sie für Availability Zone die Local Zone aus. Die Local Zone wird durch einen AWS -Regionscode dargestellt, gefolgt von einer ID, die den Standort angibt, z. B. `us-west-2-lax-1a`. Weitere Informationen finden Sie unter Erstellen eines Kapazitätsreservierung.
3. Erstellen Sie ein Subnetz in der Local Zone. Wählen Sie für Availability Zone die Local Zone aus. Weitere Informationen finden Sie unter Erstellen eines Subnetzes in Ihrer VPC im Amazon-VPC-Benutzerhandbuch.
4. Starten Sie eine Instance. Wählen Sie als Subnetz das Subnetz in der Local Zone (z. B. `subnet-123abc | us-west-2-lax-1a`) aus und wählen Sie bei Kapazitätsreservierung die Spezifikation (entweder `open` oder finden Sie sie nach ID), die für die Kapazitätsreservierung erforderlich ist, die Sie in der Local Zone erstellt haben. Weitere Informationen finden Sie unter Starten von Instances in einer bestehenden Kapazitätsreservierung.

Kapazitätsreservierungen in Wavelength-Zonen

Mit AWS Wavelength können Entwickler Anwendungen mit ultra-niedriger Latenz für Mobilgeräte und Endbenutzer erstellen. Wavelength stellt standardmäßige AWS -Datenverarbeitungs- und -Speicherservices am Edge der 5G-Netze von Telekommunikationsanbietern bereit. Sie können eine

Amazon Virtual Private Cloud (VPC) auf eine oder mehrere Wavelength-Zonen erweitern. Sie können dann AWS Ressourcen wie EC2 Amazon-Instances verwenden, um Anwendungen auszuführen, die eine extrem niedrige Latenz und eine Verbindung zu AWS Diensten in der Region erfordern. Weitere Informationen finden Sie unter AWS Wavelength Zonen.

Wenn Sie On-Demand Kapazitätsreservierungen erstellen, können Sie die Wavelength-Zone auswählen und Instances Kapazitätsreservierung in einer Wavelength-Zone starten, indem Sie das mit der Wavelength-Zone verknüpfte Subnetz angeben. Eine Wellenlängenzone wird durch einen AWS Regionalcode dargestellt, gefolgt von einer Kennung, die beispielsweise den Standort angibt`us-east-1-wl1-bos-wlz-1`.

Wavelength Zones sind nicht in jeder Region verfügbar. Weitere Informationen zu den Regionen, die Wavelength Zones unterstützen, finden Sie unter Verfügbare Wavelength Zones im AWS Wavelength Developerhandbuch.

Überlegungen

Sie können in einer Wavelength-Zone keine Kapazitätsreservierung-Gruppen verwenden.

Verwenden einer Kapazitätsreservierung in einer Wavelength-Zone

1. Aktivieren Sie die Wellenlängenzone für die Verwendung in Ihrem AWS Konto. Weitere Informationen finden Sie unter Erste Schritte mit AWS Wavelength im AWS Wavelength - Entwicklerhandbuch.
2. Erstellen Sie eine Kapazitätsreservierung in der Wavelength-Zone. Wählen Sie für Availability Zone die Wavelength aus. Die Wavelength wird durch einen AWS -Regionscode dargestellt, gefolgt von einer ID, die den Standort angibt, z. B. `us-east-1-wl1-bos-wlz-1`. Weitere Informationen finden Sie unter Erstellen eines Kapazitätsreservierung.
3. Erstellen Sie ein Subnetz in der Wavelength-Zone. Wählen Sie für Availability Zone die Zone Wavelength aus. Weitere Informationen finden Sie unter Erstellen eines Subnetzes in Ihrer VPC im Amazon-VPC-Benutzerhandbuch.
4. Starten Sie eine Instance. Wählen Sie als Subnetz das Subnetz in der Zone Wavelength (z. B. `subnet-123abc | us-east-1-wl1-bos-wlz-1`) aus und wählen Sie bei Kapazitätsreservierung die Spezifikation (entweder `open` oder finden Sie sie nach ID), die für die Kapazitätsreservierung erforderlich ist, die Sie in der Wavelength erstellt haben. Weitere Informationen finden Sie unter Starten von Instances in einer bestehenden Kapazitätsreservierung.

Kapazitätsreservierungen am AWS Outposts

AWS Outposts ist ein vollständig verwalteter Service, der AWS Infrastruktur APIs, Dienste und Tools auf Kundenstandorte ausdehnt. Durch den lokalen Zugriff auf die AWS verwaltete Infrastruktur AWS Outposts können Kunden Anwendungen vor Ort mit denselben Programmierschnittstellen wie in AWS Regionen erstellen und ausführen und gleichzeitig lokale Rechen- und Speicherressourcen für geringere Latenz und lokale Datenverarbeitungsanforderungen nutzen.

Ein Outpost ist ein Pool von AWS Rechen- und Speicherkapazitäten, der am Standort eines Kunden bereitgestellt wird. AWS betreibt, überwacht und verwaltet diese Kapazität als Teil einer AWS Region.

Sie können Kapazitätsreservierungen auf Outposts erstellen, die Sie in Ihrem Konto erstellt haben. Auf diese Weise können Sie Rechenkapazität auf einem Outpost an Ihrem Standort reservieren. Sie erstellen und verwenden Kapazitätsreservierungen in Outposts auf die gleiche Weise, wie Sie Kapazitätsreservierungen in regulären Availability Zones erstellen und verwenden. Es gelten dieselben Features und dasselbe Verhalten der Instance-Übereinstimmung.

Sie können Kapazitätsreservierungen auf Outposts auch mit anderen AWS Konten innerhalb Ihrer Organisation teilen, indem AWS Resource Access Manager Sie. Weitere Informationen zum Freigeben von Kapazitätsreservierungen finden Sie unter Freigegebene Kapazitätsreservierungen.

Voraussetzung

Sie müssen einen Outpost an Ihrem Standort installiert haben. Weitere Informationen finden Sie unter Outpost erstellen und die Kapazität dafür bestellen im AWS Outposts -Benutzerhandbuch.

Überlegungen

- Sie können auf einem Outpost keine Kapazitätsreservierung-Gruppen verwenden.

Verwenden einer Kapazitätsreservierung auf einem Outpost

1. Erstellen Sie ein Subnetz auf dem Outpost. Weitere Informationen finden Sie unter Erstellen eines Subnetzes im AWS Outposts -Benutzerhandbuch.
2. Erstellen Sie eine Kapazitätsreservierung auf dem Outpost.
    a. Öffnen Sie die AWS Outposts Konsole unter. https://console.aws.amazon.com/outposts/
    b. Wählen Sie im Navigationsbereich Outposts aus und klicken Sie danach auf Aktionen, Kapazitätsreservierung erstellen.

c. Konfigurieren Sie die Kapazitätsreservierung nach Bedarf und wählen Sie Create (Erstellen) aus. Weitere Informationen finden Sie unter Erstellen eines Kapazitätsreservierung.

> **Note**
>
> In der Dropdown-Liste Instance-Typ werden nur Instance-Typen aufgeführt, die vom ausgewählten Outpost unterstützt werden. In der Dropdown-Liste Availability Zone wird nur die Availability Zone aufgeführt, die dem ausgewählten Outpost zugeordnet ist.

3. Starten einer Instance in einer Kapazitätsreservierung. Wählen Sie für Subnetz das Subnetz aus, das Sie in Schritt 1 erstellt haben, und für Kapazitätsreservierung wählen Sie die Kapazitätsreservierung aus, die Sie in Schritt 2 erstellt haben. Weitere Informationen finden Sie unter Launch an Instance on your Outpost (Starten einer Instance auf Ihrem Outpost) im AWS Outposts -Benutzerhandbuch.

Freigegebene Kapazitätsreservierungen

Die gemeinsame Nutzung von Kapazitätsreservierungen ermöglicht es Besitzern von Kapazitätsreservierungen, ihre reservierte Kapazität mit anderen AWS Konten oder innerhalb einer AWS Organisation zu teilen. Auf diese Weise können Sie Kapazitätsreservierungen zentral erstellen und verwalten und die reservierte Kapazität auf mehrere AWS Konten oder innerhalb Ihrer AWS Organisation verteilen.

Bei diesem Modell teilt sich das AWS Konto, dem die Kapazitätsreservierung gehört (Eigentümer), diese mit anderen AWS Konten (Verbrauchern). Konsumenten können beim Starten von Instances in den für sie freigegebenen Kapazitätsreservierungen so vorgehen, wie sie dies beim Starten von Instances in Kapazitätsreservierungen tun würden, die zu ihrem Konto gehören. Der Kapazitätsreservierung-Besitzer ist für die Verwaltung der Kapazitätsreservierung und der Instances, die von ihm darin gestartet werden, verantwortlich. Besitzer sind nicht dazu befugt Instances, die Konsumenten in den von ihnen freigegebenen Kapazitätsreservierungen starten, zu ändern. Konsumenten sind für die Verwaltung der Instances verantwortlich, die sie in den für sie freigegebenen Kapazitätsreservierungen starten. Konsumenten können keine Instances anzeigen oder ändern, die sich im Besitz anderer Konsumenten oder des Besitzers der Kapazitätsreservierung befinden.

Ein Kapazitätsreservierung-Besitzer kann eine Kapazitätsreservierung freigeben für:

- Bestimmte AWS Konten innerhalb oder außerhalb der AWS Organisation
- Eine Organisationseinheit innerhalb ihrer AWS Organisation
- Es ist die gesamte AWS Organisation

Voraussetzungen für die Freigabe von Kapazitätsreservierungen

- Um eine Kapazitätsreservierung teilen zu können, müssen Sie sie in Ihrem AWS Konto besitzen. Sie können keine Kapazitätsreservierung freigeben, die für Sie freigegeben wurde.
- Sie können Kapazitätsreservierungen ausschließlich für freigegebene Tenancy-Instances freigeben. Sie können Kapazitätsreservierungen nicht für Dedicated Tenancy-Instances freigeben.
- Die gemeinsame Nutzung von Kapazitätsreservierungen ist nicht für neue AWS Konten oder AWS Konten mit begrenzter Abrechnungshistorie verfügbar.
- Um eine Kapazitätsreservierung mit Ihrer AWS Organisation oder einer Organisationseinheit in Ihrer AWS Organisation zu teilen, müssen Sie die gemeinsame Nutzung mit aktivieren AWS Organizations. Weitere Informationen finden Sie unter Freigabe für AWS Organizations aktivieren im AWS RAM -Benutzerhandbuch.

Zugehörige Services

Die gemeinsame Nutzung von Kapazitätsreservierungen ist in AWS Resource Access Manager (AWS RAM) integriert. AWS RAM ist ein Dienst, mit dem Sie Ihre AWS Ressourcen mit einem beliebigen AWS Konto oder über dieses teilen können AWS Organizations. Mit AWS RAM geben Sie Ressourcen in Ihrem Besitz frei, indem Sie eine Ressourcenfreigabe erstellen. Eine Ressourcenfreigabe legt die freizugebenden Ressourcen und die Konsumenten fest, für die sie freigegeben werden sollen. Verbraucher können einzelne AWS Konten, Organisationseinheiten oder eine gesamte Organisation sein AWS Organizations.

Weitere Informationen zu AWS RAM finden Sie im AWS RAM Benutzerhandbuch.

Freigeben in mehreren Availability Zones

Um sicherzustellen, dass Ressourcen auf die Availability Zones einer Region verteilt sind, ordnen wir Availability Zones einzeln Namen für jedes Konto zu. Dies könnte zu in mehreren Konten unterschiedlich benannten Availability Zones führen. Beispielsweise hat die Availability Zone `us-east-1a` für Ihr AWS Konto möglicherweise nicht denselben Standort wie `us-east-1a` für ein anderes AWS Konto.

Um den Ort Ihrer Kapazitätsreservierungen relativ zu Ihren Konten zu bestimmen, verwenden Sie die Availability Zone-ID (AZ-ID). Die AZ-ID ist eine eindeutige und konsistente Kennung für eine Availability Zone für alle AWS Konten. Dies `use1-az1` ist beispielsweise eine AZ-ID für die `us-east-1` Region und es handelt sich in jedem AWS Konto um denselben Standort.

Um die AZ IDs für die Availability Zones in Ihrem Konto anzuzeigen

1. Öffnen Sie die AWS RAM Konsole zu https://console.aws.amazon.com/ram/Hause.
2. Die AZ IDs für die aktuelle Region werden im Bereich „Ihre AZ-ID“ auf der rechten Seite des Bildschirms angezeigt.

Freigeben einer Kapazitätsreservierung

Wenn Sie eine Kapazitätsreservierung, die Sie besitzen, mit anderen teilen AWS-Konten, ermöglichen Sie ihnen, Instances in Ihrer reservierten Kapazität zu starten. Berücksichtigen Sie bei der Freigabe einer offenen Kapazitätsreservierung Folgendes, da dies zu einer unvorhergesehenen Nutzung der Kapazitätsreservierung führen könnte:

- Konsumenten mit ausgeführten Ressourcen, die den Attributen der Kapazitätsreservierung entsprechen, für die der Parameter `CapacityReservationPreference` auf `open` eingestellt ist und die noch nicht in reservierter Kapazität ausgeführt werden, verwenden automatisch die freigegebene Kapazitätsreservierung.
- Wenn Konsumenten Instances starten, die übereinstimmende Attribute (Instance-Typ, Plattform, Availability Zone und Tenancy) besitzen und für die der Parameter `CapacityReservationPreference` auf `open` eingestellt ist, werden diese automatisch in der freigegebenen Kapazitätsreservierung gestartet.

Um eine Kapazitätsreservierung freigeben zu können, müssen Sie sie einer Ressourcenfreigabe hinzufügen. Eine Ressourcenfreigabe ist eine AWS RAM Ressource, mit der Sie Ihre Ressourcen für mehrere AWS Konten gemeinsam nutzen können. Eine Ressourcenfreigabe gibt die freizugebenden Ressourcen und die Konsumenten an, für die sie freigegeben werden. Wenn Sie eine Kapazitätsreservierung über die EC2 Amazon-Konsole teilen, fügen Sie sie einer vorhandenen Ressourcenfreigabe hinzu. Um die Kapazitätsreservierung einer neuen Ressourcenfreigabe hinzufügen zu können, müssen Sie die Ressourcenfreigabe mithilfe der AWS RAM -Konsole erstellen.

Wenn Sie Teil einer Organisation in Ihrer Organisation sind AWS Organizations und die gemeinsame Nutzung innerhalb Ihrer Organisation aktiviert ist, erhalten Verbraucher in Ihrer Organisation Zugriff auf die gemeinsame Kapazitätsreservierung, sofern die Voraussetzungen für die gemeinsame Nutzung erfüllt sind. Wenn die Kapazitätsreservierung für externe Konten freigegeben ist, erhalten Konsumenten eine Einladung zur Teilnahme an der Ressourcenfreigabe und nach Annahme der Einladung wird ihnen Zugriff auf die freigegebene Kapazitätsreservierung gewährt.

> **Important**
>
> Bevor Sie Instances für eine Kapazitätsreservierung starten, die mit Ihnen geteilt wird, überprüfen Sie, ob Sie Zugriff auf die gemeinsam genutzte Kapazitätsreservierung haben, indem Sie sie in der Konsole anzeigen oder sie mit dem describe-capacity-reservations AWS CLI Befehl beschreiben. Wenn Sie die gemeinsame Kapazitätsreservierung in der Konsole anzeigen oder sie mithilfe von beschreiben können AWS CLI, steht sie Ihnen zur Verfügung und Sie können Instances darin starten. Wenn Sie versuchen, Instances in die Kapazitätsreservierung zu starten, und diese aufgrund eines Freigabefehlers nicht zugänglich ist, werden die Instances in On-Demand-Kapazität gestartet.

Console

Um eine Kapazitätsreservierung, die Sie besitzen, über die EC2 Amazon-Konsole zu teilen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Kapazitätsreservierungen aus.
3. Wählen Sie die Kapazitätsreservierung aus, die freigegeben werden soll, und wählen Sie Actions (Aktionen), Share reservation (Reservierung freigeben).
4. Wählen Sie die Ressourcenfreigabe aus, der die Kapazitätsreservierunghinzugefügt werden soll, und wählen Sie Share Kapazitätsreservierung (Kapazitätsreservierung freigeben).

   Es kann einige Minuten dauern, bis Konsumenten Zugriff auf die freigegebene Kapazitätsreservierung gewährt wird.

Um eine Kapazitätsreservierung, die Sie besitzen, über die AWS RAM Konsole zu teilen

Weitere Informationen finden Sie unter Erstellen einer Ressourcenfreigabe im AWS RAM - Benutzerhandbuch.

AWS CLI

So können Sie eine Kapazitätsreservierung freigeben, die Sie besitzen

Verwenden Sie den Befehl create-resource-share.

```
aws ram create-resource-share \
    --name my-resource-share \
    --resource-arns arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE
```

PowerShell

So können Sie eine Kapazitätsreservierung freigeben, die Sie besitzen

Verwenden Sie das Cmdlet New- RAMResource Share.

```
New-RAMResourceShare `
    -Name my-resource-share `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:capacity-
reservation/cr-1234abcd56EXAMPLE"
```

Beenden der Freigabe einer Kapazitätsreservierung

Der Kapazitätsreservierung-Besitzer kann die gemeinsame Nutzung einer Kapazitätsreservierung jederzeit beenden. Die folgenden Regeln gelten:

- Instances von Verbrauchern, die zu dem Zeitpunkt, zu dem die gemeinsame Nutzung unterbrochen wurde, in der gemeinsam genutzten Kapazität liefen, werden außerhalb der reservierten Kapazität weiterhin normal ausgeführt, und die Kapazität wird vorbehaltlich der Kapazitätsverfügbarkeit von Amazon wieder auf die EC2 Kapazitätsreservierung zurückgesetzt.
- Konsumenten, für die die Kapazitätsreservierung freigegeben wurde, können keine neuen Instances mehr in der reservierten Kapazität starten.

Um die Freigabe einer Kapazitätsreservierung in Ihrem Besitz zu beenden, müssen Sie diese aus der Ressourcenfreigabe entfernen.

Console

So beenden Sie das Teilen einer Kapazitätsreservierung, die Sie besitzen, über die EC2 Amazon-Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Kapazitätsreservierungen aus.
3. Wählen Sie die Kapazitätsreservierung aus und klicken Sie auf die Registerkarte Freigabe.
4. Auf der Registerkarte Sharing (Freigabe) werden die Ressorcenfreigaben aufgelistet, zu denen die Kapazitätsreservierung hinzugefügt wurde. Wählen Sie die Ressourcenfreigabe aus, aus der die Kapazitätsreservierung entfernt werden soll, und wählen Sie Remove from resource share (Aus Ressourcenfreigabe entfernen).

Um das Teilen einer Kapazitätsreservierung, die Sie besitzen, über die AWS RAM Konsole zu beenden

Siehe Aktualisieren einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

AWS CLI

So können Sie die Freigabe einer Kapazitätsreservierung beenden, die Sie besitzen.

Verwenden Sie den Befehl disassociate-resource-share.

```
aws ram disassociate-resource-share \
    --resource-share-arn arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
 --resource-arns arn:aws:ec2:us-east-2:123456789012:capacity-reservation/cr-1234abcd56EXAMPLE
```

PowerShell

So können Sie die Freigabe einer Kapazitätsreservierung beenden, die Sie besitzen.

Verwenden Sie das Cmdlet Disconnect- RAMResource Share.

```
Disconnect-RAMResourceShare `
    -ResourceShareArn "arn:aws:ram:us-east-2:123456789012:resource-share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE" `
    -ResourceArn "arn:aws:ec2:us-east-2:123456789012:capacity-reservation/cr-1234abcd56EXAMPLE"
```

Fakturierungszuweisung für gemeinsame EC2 Amazon-Kapazitätsreservierungen

Wenn eine Kapazitätsreservierung freigegeben wird, werden dem Eigentümer standardmäßig die Instances, die er in der Kapazitätsreservierung ausführt, und alle verfügbaren Kapazitäten, auch ungenutzte Kapazität genannt, in der Kapazitätsreservierung in Rechnung gestellt. Verbrauchern werden dagegen nur die Instances in Rechnung gestellt, die sie im Rahmen der gemeinsamen Kapazitätsreservierung ausführen.

Bei Bedarf kann der Eigentümer der Kapazitätsreservierung die Abrechnung aller verfügbaren Kapazitäten in der Kapazitätsreservierung jedem der Konten zuweisen, für die die Kapazitätsreservierung freigegeben wird. Nachdem die Abrechnung einem anderen Konto zugewiesen wurde, wird dieses Konto zum Abrechnungsinhaber aller verfügbaren Kapazitäten in der Kapazitätsreservierung. Ab diesem Zeitpunkt werden alle Gebühren für verfügbare Kapazität in der Kapazitätsreservierung dem zugewiesenen Konto und nicht dem Konto des Eigentümers in Rechnung gestellt. Dem Eigentümer der Kapazitätsreservierung und der Konten, für die die Kapazitätsreservierung freigegeben wird, werden weiterhin die Instances in Rechnung gestellt, die sie in der Kapazitätsreservierung ausführen.

> **Important**
>
> Der Kapazitätsreservierung-Besitzer bleibt der Ressourcenbesitzer und bleibt für die Verwaltung der Kapazitätsreservierung verantwortlich. Das Konto, dem die Fakturierung zugewiesen wurde, erhält keine zusätzlichen Rechte. Es kann die Kapazitätsreservierung in keiner Weise stornieren, ändern oder teilen.

Themen

- Funktionsweise
- Überlegungen
- Weisen Sie die Abrechnung einer gemeinsamen EC2 Kapazitätsreservierung einem anderen Konto zu
- Anfragen zur Fakturierungszuweisung für gemeinsam genutzte EC2 Kapazitätsreservierungen anzeigen
- Akzeptieren oder lehnen Sie die Abrechnung einer gemeinsamen EC2 Kapazitätsreservierung ab
- Stornieren oder widerrufen Sie Anfragen zur Rechnungszuweisung für Reservierungen mit gemeinsam genutzter EC2 Kapazität
- Anfragen für die Fakturierung von freigegebenen Kapazitätsreservierungen überwachen

Funktionsweise

Nur der Eigentümer der Kapazitätsreservierung kann die Fakturierung einer freigegebenen Kapazitätsreservierung einem anderen Konto zuweisen. Die Abrechnung kann nur einem Konto zugewiesen werden, mit dem die Kapazitätsreservierung gemeinsam genutzt wird und das unter demselben AWS Organizations Zahlerkonto wie der Eigentümer der Kapazitätsreservierung zusammengefasst ist.

Um die Abrechnung der verfügbaren Kapazität einer Kapazitätsreservierung einem anderen Konto zuzuweisen, muss der Eigentümer der Kapazitätsreservierung eine Anfrage an das erforderliche Konto stellen. Das angegebene Konto erhält die Anfrage und muss sie innerhalb von 12 Stunden entweder annehmen oder ablehnen.

- Wenn sie zustimmen, werden sie der Rechnungsinhaber aller verfügbaren Kapazitäten, auch ungenutzte Kapazität genannt, in der Kapazitätsreservierung. Ab diesem Zeitpunkt werden alle Gebühren für verfügbare Kapazität in der Kapazitätsreservierung dem zugewiesenen Konto und nicht dem Konto des Eigentümers in Rechnung gestellt. Nach der Annahme kann nur der Inhaber der Kapazitätsreservierung die Fakturierung über das zugewiesene Konto widerrufen.
- Im Falle einer Ablehnung bleibt der Eigentümer der Kapazitätsreservierung weiterhin der Abrechnungsinhaber der verfügbaren Kapazität in der Kapazitätsreservierung. Die Gebühren für jede verfügbare Kapazität in der Kapazitätsreservierung werden weiterhin dem Konto des Eigentümers in Rechnung gestellt.
- Wenn sie die Anfrage nicht innerhalb von 12 Stunden annehmen oder ablehnen, verfällt sie und die Gebühren für jede verfügbare Kapazität in der Kapazitätsreservierung werden weiterhin dem Konto des Eigentümers in Rechnung gestellt.

Für den Zeitraum, in dem die Abrechnung einem anderen Konto zugeordnet ist, erscheinen die `Reservation`- und `UnusedBox`-Einzelposten im Kosten- und Nutzungsbericht (CUR) des zugeordneten Kontos anstelle des CUR des Eigentümers.

Die folgende Tabelle zeigt, welche Einzelposten in der CUR für Eigentümer- und Verbraucherkonten für Kapazitätsreservierungen erscheinen, bevor die Abrechnung einem anderen Konto zugewiesen wird.

Account	CUR-Einzelposten, bevor die Fakturierung zugewiesen wird
Kapazitätsreservierungs-Eigentümer	•

Account	CUR-Einzelposten, bevor die Fakturierung zugewiesen wird
	• `Reservation` • `BoxUsage *` • `UnusedBox`
Verbraucherkonten, mit denen die Kapazitätsreservierung geteilt wird	• `BoxUsage *`

Die folgende Tabelle zeigt, welche Einzelposten in der CUR für Eigentümer- und Verbraucherkonten für Kapazitätsreservierungen erscheinen, nachdem die Abrechnung einem anderen Konto zugewiesen wird.

Account	CUR-Einzelposten, nachdem die Fakturierung zugewiesen wird
Kapazitätsreservierungs-Eigentümer	• `BoxUsage *`
Verbraucherkonto, dem die Abrechnung zugewiesen ist	• `Reservation` • `BoxUsage *` • `UnusedBox`
Andere Verbraucherkonten, mit denen die Kapazitätsreservierung geteilt wird	• `BoxUsage *`

Note

- * Der `BoxUsage`-Einzelposten wird nur dann in der CUR eines Accounts angezeigt, wenn es in der Kapazitätsreservierung laufende Instances gibt. Weitere Informationen zu den CUR-Einzelposten finden Sie unter Kapazitätsreservierungen überwachen.
- Verwenden Sie den Kapazitätsreservierungs-ARN in der CUR, um zu ermitteln, wem die Kapazitätsreservierung gehört. Wenn der ARN Ihre AWS Konto-ID enthält, sind Sie der Eigentümer der Kapazitätsreservierung. Andernfalls gehört die Kapazitätsreservierung einem anderen Konto, aber die Abrechnung wird Ihnen zugewiesen.
- Tags zur Kostenzuweisung, die der Eigentümer der Kapazitätsreservierung zugewiesen hat, werden nicht in der CUR des Verbraucherkontos angezeigt. Tags für die Kostenzuweisung werden nur in der CUR des Besitzers der Kapazitätsreservierung angezeigt.

Überlegungen

Beachten Sie beim Zuweisen der Fakturierung einer freigegebenen Kapazitätsreservierung Folgendes:

- Sie können keine teilweisen oder geteilten Abrechnungszuweisungen vornehmen. Die Abrechnung der gesamten verfügbaren Kapazität einer Kapazitätsreservierung kann jeweils einem Konto zugewiesen werden.
- Die verfügbare Kapazität einer Kapazitätsreservierung kann sich im Laufe der Zeit ändern. Dies wirkt sich auf die Abrechnung für das zugewiesene Konto aus. Beispielsweise kann sich die verfügbare Kapazität erhöhen, wenn der Eigentümer der Kapazitätsreservierung die Größe der Kapazitätsreservierung erhöht oder wenn andere Benutzerkonten ihre Instances, die im Rahmen der Kapazitätsreservierung laufen, anhalten oder beenden.
- Die Abrechnung kann nur einem Verbraucherkonto zugewiesen werden, das unter demselben AWS Organizations Zahlerkonto konsolidiert ist. Die Fakturierung wird dem Kundenkonto automatisch entzogen, wenn der Kunde die Organisation verlässt oder wenn die Kapazitätsreservierung nicht mehr für ihn freigegeben wird.
- Nur der Inhaber der Kapazitätsreservierung kann eine ausstehende Anfrage zur Rechnungszuweisung stornieren und die Abrechnung für ein zugewiesenes Konto widerrufen, nachdem die Anfrage akzeptiert wurde.

Weisen Sie die Abrechnung einer gemeinsamen EC2 Kapazitätsreservierung einem anderen Konto zu

Um die Fakturierung der verfügbaren Kapazität einer Kapazitätsreservierung einem anderen Konto zuzuweisen, muss der Eigentümer der Kapazitätsreservierung eine Anfrage an das erforderliche Konto stellen. In der EC2 Amazon-Konsole wird diese Anfrage als Übertragungsanfrage bezeichnet.

Ein Kapazitätsreservierungsinhaber kann die Abrechnung der verfügbaren Kapazität der Kapazitätsreservierung nur dann einem Konto zuordnen, wenn:

- Die Kapazitätsreservierung wurde bereits für dieses Konto freigegeben.
- Das Konto wird unter demselben AWS Organizations Zahlerkonto konsolidiert wie der Inhaber der Kapazitätsreservierung.

Die Abrechnung dem angegebenen Konto erst zugewiesen wird, wenn die Anfrage akzeptiert wurde.

Wenn ein Inhaber einer Kapazitätsreservierung eine Anfrage einleitet, wird ein EventBridge Amazon-Event an das angeforderte Konto gesendet. Weitere Informationen finden Sie unter Anfragen für die Fakturierung von freigegebenen Kapazitätsreservierungen überwachen.

Console

So weisen Sie die Abrechnung einer freigegebenen Kapazitätsreservierung zu

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Kapazitätsreservierungen und wählen Sie die freigegebene Kapazitätsreservierung aus.
3. Wählen Sie im Abschnitt Abrechnung der verfügbaren Kapazität die Option Abrechnung zuweisen aus.
4. Wählen Sie auf dem Bildschirm Abrechnung zuweisen das Verbraucherkonto aus, dem die Abrechnung zugewiesen werden soll, und wählen Sie dann Anfrage.

AWS CLI

So weisen Sie die Abrechnung einer freigegebenen Kapazitätsreservierung zu

Verwenden Sie den Befehl associate-capacity-reservation-billing-owner. Geben Sie für `--capacity-reservation-id` die ID der freigegebenen Kapazitätsreservierung an. Geben

Sie für `--unused-reservation-billing-owner-id` die ID des AWS Kontos an, dem die Abrechnung zugewiesen werden soll.

```
aws ec2 associate-capacity-reservation-billing-owner \
    --capacity-reservation-id cr-01234567890abcdef \
    --unused-reservation-billing-owner-id 123456789012
```

PowerShell

So weisen Sie die Abrechnung einer freigegebenen Kapazitätsreservierung zu

Verwenden Sie das cmdlet Register-EC2CapacityReservationBillingOwner. Geben Sie für `-CapacityReservationId` die ID der freigegebenen Kapazitätsreservierung an. Geben Sie für `-UnusedReservationBillingOwnerId` die ID des AWS Kontos an, dem die Abrechnung zugewiesen werden soll.

```
Register-EC2CapacityReservationBillingOwner `
    -CapacityReservationId cr-01234567890abcdef `
    -UnusedReservationBillingOwnerId 123456789012
```

Anfragen zur Fakturierungszuweisung für gemeinsam genutzte EC2 Kapazitätsreservierungen anzeigen

Ein Inhaber einer Kapazitätsreservierung kann nur die letzte von ihm initiierte Anfrage zur Rechnungszuweisung einsehen. Und Kundenkonten können nur die neuesten Anfragen zur Rechnungszuweisung einsehen, die an sie gesendet wurden.

Anfragen können bis zu 24 Stunden lang eingesehen werden, nachdem sie den Status `cancelled`, `expired`, oder `revoked` erreicht haben. Nach 24 Stunden können sie nicht mehr angezeigt werden.

Console

(Inhaber der Kapazitätsreservierung) So zeigen Sie von Ihnen initiierte Anfragen an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Kapazitätsreservierungen und wählen Sie die freigegebene Kapazitätsreservierung aus, für die Anfragen angezeigt werden sollen.
3. Im Abschnitt Abrechnung der verfügbaren Kapazität werden die letzte Anfrage und ihr aktueller Status angezeigt.

(Kundenkonto) Für an Sie gesendete Anfragen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Kapazitätsreservierungen aus.
3. Wenn Sie ausstehende Anfragen haben, wird oben auf dem Bildschirm das Banner Ausstehende Anfragen zur Rechnungszuweisung angezeigt. Wenn das Banner nicht angezeigt wird, haben Sie keine ausstehenden Anfragen.

   Um die Anfragen anzusehen, wählen Sie im Banner Anfragen überprüfen aus.

AWS CLI

(Inhaber der Kapazitätsreservierung) So zeigen Sie von Ihnen initiierte Anfragen an

Verwenden Sie den Befehl describe-capacity-reservation-billing-requests.

```
aws ec2 describe-capacity-reservation-billing-requests \
    --role odcr-owner
```

(Kundenkonto) Für an Sie gesendete Anfragen

Verwenden Sie den Befehl describe-capacity-reservation-billing-requests.

```
aws ec2 describe-capacity-reservation-billing-requests \
    --role unused-reservation-billing-owner
```

PowerShell

(Inhaber der Kapazitätsreservierung) So zeigen Sie von Ihnen initiierte Anfragen an

Verwenden Sie das cmdlet Get-EC2CapacityReservationBillingRequest.

```
Get-EC2CapacityReservationBillingRequest `
    -Role odcr-owner
```

(Kundenkonto) Für an Sie gesendete Anfragen

Verwenden Sie das cmdlet Get-EC2CapacityReservationBillingRequest.

```
Get-EC2CapacityReservationBillingRequest `
```

```
    -Role unused-reservation-billing-owner
```

Eine Anfrage kann einen der folgenden Status aufweisen.

Status	Description
`pending`	Die Anfrage wurde nicht akzeptiert oder abgelehnt, ist aber noch nicht abgelaufen.
`accepted`	Die Anfrage wurde vom angegebenen Konto akzeptiert. Die Abrechnung der verfügbaren Kapazität der Kapazitätsreservierung ist dem Kundenkonto zugewiesen.
`rejected`	Die Anfrage wurde vom Verbraucherkonto abgelehnt.
`cancelled`	Die Anfrage wurde vom Inhaber der Kapazitätsreservierung storniert, während sie sich im `pending`-Status befand.
`revoked`	Die Abrechnung wurde aus folgenden Gründen vom Verbraucherkonto gesperrt: • Sie wurde vom Kapazitätsreservierung-Besitzer ausdrücklich widerrufen. • Die Kapazitätsreservierung wird nicht mehr für den

Status	Description
	Verbraucherkonto freigegeben. • Das Verbraucherkonto ist nicht mehr Teil der AWS -Organisation.
`expired`	Die Anfrage ist abgelaufen, weil das Verbraucherkonto sie nicht innerhalb von 12 Stunden akzeptiert oder abgelehnt hat.

Akzeptieren oder lehnen Sie die Abrechnung einer gemeinsamen EC2 Kapazitätsreservierung ab

Wenn Sie eine Anfrage zur Fakturierungszuweiseung für eine Kapazitätsreservierung erhalten, die für Sie freigegeben ist, können Sie sie entweder annehmen oder ablehnen. Die Anfrage bleibt so lange im `pending`-Status, bis sie angenommen oder abgelehnt wird.

Wenn Sie die Anfrage annehmen, wechselt sie in den `accepted`-Status. Die Abrechnung aller verfügbaren oder ungenutzten Kapazitäten dieser Kapazitätsreservierung wird Ihrem Konto ab diesem Zeitpunkt zugewiesen. Nachdem Sie eine Anfrage akzeptiert haben, kann nur der Inhaber der Kapazitätsreservierung die Abrechnung von Ihrem Konto widerrufen.

Wenn Sie die Anfrage ablehnen, wird sie in den `rejected`-Status übernommen, und die Abrechnung der verfügbaren Kapazität der Kapazitätsreservierung bleibt dem Eigentümer der Kapazitätsreservierung zugewiesen.

Anfragen laufen ab, wenn sie nicht innerhalb von 12 Stunden akzeptiert oder abgelehnt werden. Wenn eine Anfrage abläuft, bleibt die Abrechnung der ungenutzten Kapazität der Kapazitätsreservierung weiterhin dem Eigentümer der Kapazitätsreservierung zugewiesen.

Wenn eine Anfrage akzeptiert oder abgelehnt wird, wird eine EventBridge Amazon-Veranstaltung an das Konto des Besitzers der Kapazitätsreservierung gesendet. Wenn eine Anfrage abläuft, wird ein EventBridge Amazon-Event an den Inhaber der Kapazitätsreservierung und das Kundenkonto

gesendet. Weitere Informationen finden Sie unter Anfragen für die Fakturierung von freigegebenen Kapazitätsreservierungen überwachen.

Console

So akzeptieren oder lehnen Sie eine Anfrage ab

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Kapazitätsreservierungen aus.
3. Wenn Sie ausstehende Anfragen haben, wird oben auf dem Bildschirm das Banner Ausstehende Anfragen zur Rechnungszuweisung angezeigt. Wenn das Banner nicht angezeigt wird, haben Sie keine ausstehenden Anfragen.

   Um die Anfragen anzusehen, wählen Sie im Banner Anfragen überprüfen aus.
4. Wählen Sie die Anfrage aus, die Sie annehmen oder ablehnen möchten, und wählen Sie dann entweder Annehmen oder Ablehnen.

AWS CLI

So nehmen Sie eine Anfrage an

Verwenden Sie den Befehl accept-capacity-reservation-billing-ownership. Geben Sie für `--capacity-reservation-id` die ID der Kapazitätsreservierung an, für die Sie die Anfrage annehmen möchten.

```
aws ec2 accept-capacity-reservation-billing-ownership \
    --capacity-reservation-id cr-01234567890abcdef
```

So lehnen Sie eine Anfrage ab

Verwenden Sie den Befehl reject-capacity-reservation-billing-ownership. Geben Sie für `--capacity-reservation-id` die ID der Kapazitätsreservierung an, für die Sie die Anfrage ablehnen möchten.

```
aws ec2 reject-capacity-reservation-billing-ownership \
    --capacity-reservation-id cr-01234567890abcdef
```

PowerShell

So nehmen Sie eine Anfrage an

Verwenden Sie das cmdlet Approve-EC2CapacityReservationBillingOwnership.

```
Approve-EC2CapacityReservationBillingOwnership `
    -CapacityReservationId cr-01234567890abcdef
```

So lehnen Sie eine Anfrage ab

Verwenden Sie das cmdlet Deny-EC2CapacityReservationBillingOwnership.

```
Deny-EC2CapacityReservationBillingOwnership `
    -CapacityReservationId cr-01234567890abcdef
```

Stornieren oder widerrufen Sie Anfragen zur Rechnungszuweisung für Reservierungen mit gemeinsam genutzter EC2 Kapazität

Nur der Inhaber der Kapazitätsreservierung kann eine Anfrage zur `pending`-Rechnungszuweisung abbrechen. Wenn eine ausstehende Anfrage abgebrochen wird, tritt sie in den Status `cancelled` ein und die Abrechnung der verfügbaren oder ungenutzten Kapazität der Kapazitätsreservierung bleibt dem Eigentümer der Kapazitätsreservierung zugeordnet.

Sobald eine Anfrage `accepted` ist, kann nur der Eigentümer der Kapazitätsreservierung die Fakturierung des zugeordneten Kontos widerrufen. Wenn die Abrechnung widerrufen wird, geht die Anfrage in den Zustand `revoked` über und die Abrechnung der verfügbaren Kapazität der Kapazitätsreservierung wird wieder dem Eigentümer der Kapazitätsreservierung zugewiesen.

Wenn eine Anfrage storniert oder widerrufen wird, werden EventBridge Amazon-Ereignisse an den Inhaber der Kapazitätsreservierung und das angegebene Kundenkonto gesendet. Weitere Informationen finden Sie unter Anfragen für die Fakturierung von freigegebenen Kapazitätsreservierungen überwachen.

Console

So stornieren oder widerrufen Sie eine Anfrage

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Kapazitätsreservierungen und wählen Sie dann die Kapazitätsreservierung aus, für welche die Anforderungen abgebrochen oder widerrufen werden sollen.

3. Wählen Sie im Abschnitt Abrechnung der verfügbaren Kapazität je nach aktuellem Status der Anfrage die Option Übertragung abbrechen oder Übertragung widerrufen aus.

AWS CLI

So stornieren oder widerrufen Sie eine Anfrage

Verwenden Sie den Befehl disassociate-capacity-reservation-billing-owner. Geben Sie für `--unused-reservation-billing-owner-id` die ID des AWS Kontos an, an das die Anfrage gesendet wurde.

```
aws ec2 disassociate-capacity-reservation-billing-owner \
    --capacity-reservation-id cr-01234567890abcdef \
    --unused-reservation-billing-owner-id 123456789012
```

PowerShell

So stornieren oder widerrufen Sie eine Anfrage

Verwenden Sie das cmdlet Unregister-EC2CapacityReservationBillingOwner. Geben Sie für `-UnusedReservationBillingOwnerId` die ID des AWS Kontos an, an das die Anfrage gesendet wurde.

```
Unregister-EC2CapacityReservationBillingOwner `
    -CapacityReservationId cr-01234567890abcdef `
    -UnusedReservationBillingOwnerId 123456789012
```

Anfragen für die Fakturierung von freigegebenen Kapazitätsreservierungen überwachen

Amazon EC2 sendet EventBridge Amazon-Ereignisse, wenn sich der Status einer Fakturierungsanfrage ändert.

- Ereignisse werden an den Inhaber der Kapazitätsreservierung gesendet, wenn eine Anfrage in einen der folgenden Zustände übergeht: `accepted` | `rejected` | `expired` | `revoked`.
- Ereignisse werden an das angeforderte Verbraucherkonto gesendet, wenn eine Anfrage in einen der folgenden Zustände übergeht: `pending` | `expired` | `cancelled` | `revoked`.

Weitere Informationen zu Amazon EventBridge finden Sie im EventBridge Amazon-Benutzerhandbuch.

Das Folgende ist das EventBridge Amazon-Ereignismuster.

```
{
   "version":"0",
   "id":"12345678-1234-1234-1234-123456789012",
   "detail-type":"On-Demand Capacity Reservation Billing Ownership Request pending|
accepted|rejected|cancelled|revoked|expired",
   "source":"aws.ec2",
   "account":"account_id",
   "time":"state_change_timestamp",
   "region":"region",
   "resources":[
      "arn:aws:ec2:region:cr_owner_account_id:capacity-reservation/cr_id"
   ],
   "detail":{
      "capacity-reservation-id":"cr_id",
      "updateTime":timestamp,
      "ownerAccountId":"cr_owner_account_id",
      "unusedReservationChargesOwnerID":"consumer_account_id",
      "status":"pending|accepted|rejected|cancelled|revoked|expired",
      "statusMessage":"message
   }
}
```

Im Folgenden finden Sie ein Beispiel für ein Ereignis, das an den Eigentümer der Kapazitätsreservierung (222222222222) gesendet wird, wenn ein Verbraucherkonto (111111111111) eine Anfrage zur Fakturierungszuweisung für eine freigegebene Kapazitätsreservierung (`cr-01234567890abcdef`) akzeptiert.

```
{
   "version":"0",
   "id":"12345678-1234-1234-1234-123456789012",
   "detail-type":"On-Demand Capacity Reservation Billing Ownership Request accepted",
   "source":"aws.ec2",
   "account":"222222222222",
   "time":"2024-09-01Thh:59:59Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:222222222222:capacity-reservation/cr-01234567890abcdef"
   ],
   "detail":{
      "capacity-reservation-id":"cr-01234567890abcdef",
```

```
      "updateTime":"2024-08-01Thh:59:59Z",
      "ownerAccountId":"222222222222",
      "unusedReservationChargesOwnerID":"111111111111",
      "status":"accepted",
      "statusMessage":"billing transfer status message"
   }
}
```

Berechtigungen für freigegebene Kapazitätsreservierung

Berechtigungen für Besitzer

Besitzer sind für die Verwaltung und Stornierung ihrer freigegebenen Kapazitätsreservierungen verantwortlich. Besitzer können keine Änderungen an Instances vornehmen, die in der freigegebenen Kapazitätsreservierung im Besitz anderer Konten ausgeführt werden. Besitzer sind weiterhin für die Verwaltung von Instances verantwortlich, die sie selbst in der freigegebenen Kapazitätsreservierung starten.

Berechtigungen für Konsumenten

Konsumenten sind für die Verwaltung ihrer Instances verantwortlich, die in der freigegebenen Kapazitätsreservierung ausgeführt werden. Konsumenten können die freigegebene Kapazitätsreservierung keinesfalls ändern und können keine Instances anzeigen oder bearbeiten, die sich im Besitz anderer Konsumenten oder des Kapazitätsreservierung-Besitzers befinden. Verbraucher können nur die Gesamtkapazität und die verfügbare Kapazität in der gemeinsamen Reservierung einsehen.

Fakturierung und Messung

Für die Freigabe von Kapazitätsreservierungen fallen keine zusätzlichen Gebühren an.

Standardmäßig werden dem Eigentümer der Kapazitätsreservierung die Instances, die er innerhalb der Kapazitätsreservierung betreibt, sowie die ungenutzte reservierte Kapazität in Rechnung gestellt, während den Verbrauchern die Instances, die sie innerhalb der freigegebenen Kapazitätsreservierung betreiben, in Rechnung gestellt werden. Sie können jedoch die Fakturierung des Kapazitätsangebots einer freigegebenen Kapazitätsreservierung einem bestimmten Verbraucherkonto zuordnen. Weitere Informationen finden Sie unter Fakturierungszuweisung für gemeinsame EC2 Amazon-Kapazitätsreservierungen.

Wenn der Besitzer der Kapazitätsreservierung einem anderen Zahlerkonto angehört und die Kapazitätsreservierung durch eine regionale Reserved Instance oder einen Savings Plan

abgedeckt ist, werden dem Besitzer der Kapazitätsreservierung weiterhin die Kosten für die regionale Reserved Instance oder den Savings Plan in Rechnung gestellt. In diesen Fällen zahlt der Besitzer der Kapazitätsreservierung für die regionale Reserved Instance oder den Savings Plan, und den Verbrauchern werden die Instances in Rechnung gestellt, die in der gemeinsamen Kapazitätsreservierung ausgeführt werden.

Instance-Limits

Die gesamte Kapazitätsreservierung-Nutzung wird auf die On-Demand-Instance-Beschränkungen des Kapazitätsreservierung-Besitzers angerechnet. Dies umfasst:

- Ungenutzte reservierte Kapazität
- Nutzung durch Instances im Besitz des Kapazitätsreservierung-Besitzers
- Nutzung durch Instances im Besitz von Konsumenten

Instances, die von Konsumenten in der freigegebenen Kapazität gestartet werden, werden auf die On-Demand-Instance-Beschränkung des Kapazitätsreservierung-Besitzers angerechnet. Instance-Beschränkungen von Konsumenten sind die Summe aus ihren eigenen On-Demand-Instance-Beschränkungen und der in der freigegebenen Kapazitätsreservierungen verfügbaren Kapazität, auf die sie Zugriff haben.

Kapazitätsreservierungsflotten

Eine On-Demand-Kapazitätsreservierungsflotte ist eine Gruppe von Kapazitätsreservierungen.

Die Anforderung einer Kapazitätsreservierungsflotte enthält alle Konfigurationsinformationen, die zum Starten einer Kapazitätsreservierungsflotte erforderlich sind. Mit einer einzigen Anfrage können Sie große Mengen an EC2 Amazon-Kapazität für Ihren Workload über mehrere Instance-Typen hinweg reservieren, bis zu einer von Ihnen angegebenen Zielkapazität.

Nachdem Sie eine Kapazitätsreservierungsflotte erstellt haben, können Sie die Kapazitätsreservierungen in der Flotte verwalten, indem Sie die Flotte ändern oder auflösen.

Themen

- Funktionsweise von Kapazitätsreservierungsflotten
- Überlegungen
- Preisgestaltung

- Konzepte und Planung von Flotten für Kapazitätsreservierungen
- Erstellen einer Kapazitätsreservierungsflotte
- Ändern einer Kapazitätsreservierungsflotte
- Stornieren einer Kapazitätsreservierungsflotte
- Beispiel für Kapazitätsreservierungsflotten-Konfigurationen
- Verwenden von serviceverknüpften Rollen für Kapazitätsreservierungsflotten

Funktionsweise von Kapazitätsreservierungsflotten

Wenn Sie eine Kapazitätsreservierungsflotte erstellen, versucht die Flotte, individuelle Kapazitätsreservierungen festzulegen, um die in Ihrer Flottenanforderung angegebene Gesamtzielkapazität zu erreichen.

Die Anzahl der Instances, für die die Flotte Kapazität reserviert, hängt von der Gesamtzielkapazität und den Instance-Typ-Gewichtungen ab, die Sie angeben. Der Instance-Typ, für den die Flotte Kapazität reserviert, hängt von der Zuweisungsstrategie und den Instance-Typ-Prioritäten ab, die Sie verwenden.

Wenn zum Zeitpunkt der Erstellung nicht genügend Kapazität vorhanden ist und die Flotte ihre Gesamtzielkapazität nicht sofort erreichen kann, versucht sie auf asynchrone Weise, Kapazitätsreservierungen zu erstellen, bis die angeforderte Kapazitätsmenge reserviert ist.

Wenn die Flotte ihre Gesamtzielkapazität erreicht, versucht sie, diese Kapazität beizubehalten. Wird eine Kapazitätsreservierung in der Flotte storniert, erstellt die Flotte je nach Ihrer Flottenkonfiguration automatisch eine oder mehrere Kapazitätsreservierungen, um die verlorene Kapazität zu ersetzen und ihre Gesamtzielkapazität beizubehalten.

Die Kapazitätsreservierungen in der Flotte können nicht einzeln verwaltet werden. Sie müssen gemeinsam durch eine Änderung der Flotte verwaltet werden. Wenn Sie eine Flotte ändern, werden die Kapazitätsreservierungen in der Flotte automatisch den Änderungen entsprechend aktualisiert.

Derzeit unterstützen Kapazitätsreservierungsflotten die Übereinstimmungskriterien für open-Instances. Alle von einer Flotte gestarteten Kapazitätsreservierungen verwenden automatisch diese Übereinstimmungskriterien. Mit diesen Kriterien werden neue und bestehende Instances mit übereinstimmenden Attributen (Instance-Typ, Plattform, Availability Zone und Tenancy) automatisch innerhalb der Kapazitätsreservierungen ausgeführt, die eine Flotte erstellt hat. Kapazitätsreservierungsflotten unterstützen keine Übereinstimmungskriterien für Instances.

Überlegungen

Bei der Arbeit mit Kapazitätsreservierungsflotten sollten Sie Folgendes bedenken:

- Eine Flotte für Kapazitätsreservierungen kann mithilfe der AWS API und erstellt, geändert, angezeigt AWS CLI und storniert werden.
- Die Kapazitätsreservierungen in einer Flotte können nicht einzeln verwaltet werden. Sie müssen gemeinsam durch eine Änderung oder Stornierung der Flotte verwaltet werden.
- Eine Kapazitätsreservierungsflotte kann nicht für mehrere Regionen gelten.
- Eine Kapazitätsreservierungsflotte kann nicht für mehrere Availability Zones gelten.
- Kapazitätsreservierungen, die von einer Kapazitätsreservierungsflotte erstellt wurden, werden automatisch mit dem folgenden durch AWS generierten Tag markiert:
  - Schlüssel: `aws:ec2-capacity-reservation-fleet`
  - Wert: *`fleet_id`*

  Anhand dieses Tags können Sie Kapazitätsreservierungen erkennen, die von einer Kapazitätsreservierungsflotte erstellt wurden.

Preisgestaltung

Für die Verwendung von Kapazitätsreservierungsflotten fallen keine zusätzlichen Gebühren an. Ihnen werden die einzelnen Kapazitätsreservierungen in Rechnung gestellt, die von Ihren Kapazitätsreservierungsflotten erstellt wurden. Weitere Informationen zur Abrechnung von Kapazitätsreservierungen finden Sie unter Preise und Fakturierung für Kapazitätsreservierung.

Konzepte und Planung von Flotten für Kapazitätsreservierungen

In den folgenden Informationen wird beschrieben, wie eine Flotte für Kapazitätsreservierungen geplant wird, und es werden Konzepte für die Flotte für Kapazitätsreservierungen beschrieben, einschließlich der Gesamtzielkapazität, der Zuweisungsstrategie, der Gewichtung des Instance-Typs und der Priorität des Instance-Typs.

Themen

- Eine Flotte für Kapazitätsreservierungen planen
- Gesamtzielkapazität
- Zuweisungsstrategie

- Instance-Typ-Gewichtung
- Instance-Typ-Priorität

Eine Flotte für Kapazitätsreservierungen planen

Bei der Planung Ihrer Flotte für Kapazitätsreservierungen empfehlen wir Ihnen Folgendes zu tun:

1. Bestimmen Sie die Höhe der Rechenkapazität, die Ihre Workload erfordert.
2. Legen Sie die zu verwendenden Instance-Typen und Availability Zones fest.
3. Weisen Sie jedem Instance-Typ eine Priorität zu, die auf Ihren Anforderungen und Einstellungen basiert. Weitere Informationen finden Sie unter Instance-Typ-Priorität.
4. Erstellen Sie ein für Ihre Workload sinnvolles Kapazitätsgewichtungssystem. Weisen Sie jedem Instance-Typ eine Gewichtung zu und bestimmen Sie die Gesamtzielkapazität. Weitere Informationen erhalten Sie unter Instance-Typ-Gewichtung und Gesamtzielkapazität.
5. Bestimmen Sie, ob Sie die Kapazitätsreservierung auf unbestimmte Zeit oder nur für einen bestimmten Zeitraum benötigen.

Gesamtzielkapazität

Die Gesamtzielkapazität definiert die Gesamtmenge der Rechenkapazität, den die Kapazitätsreservierungsflotte reserviert. Sie geben die Gesamtzielkapazität beim Erstellen der Kapazitätsreservierungsflotte an. Nachdem die Flotte erstellt wurde, erstellt Amazon EC2 automatisch Kapazitätsreservierungen, um Kapazität bis zur gesamten Zielkapazität zu reservieren.

Die Anzahl der Instances, für die die Kapazitätsreservierungsflotte Kapazität reserviert, wird durch die Gesamtzielkapazität und die Instance-Typ-Gewichtung bestimmt, die Sie für jeden Instance-Typ in der Kapazitätsreservierungsflotte angeben (`total target capacity` / `instance type weight` = `number of instances`).

Sie können die Gesamtzielkapazität basierend auf sinnvollen Einheiten für Ihre Workload zuweisen. Wenn Ihre Arbeitslast beispielsweise eine bestimmte Anzahl von v erfordertCPUs, können Sie die gesamte Zielkapazität auf der Grundlage der CPUs erforderlichen Anzahl von v zuweisen. Wenn Ihr Workload `2048` v erfordertCPUs, geben Sie eine Gesamtzielkapazität von an `2048` und weisen Sie dann Gewichtungen für die Instance-Typen auf der Grundlage der Anzahl von v zu, die von den Instance-Typen in der Flotte CPUs bereitgestellt werden. Ein Beispiel finden Sie unter Instance-Typ-Gewichtung.

Zuweisungsstrategie

Die Zuweisungsstrategie für Ihre Kapazitätsreservierungsflotte bestimmt, wie die Anforderung von reservierter Kapazität aus den Instance-Typ-Spezifikationen in der Konfiguration der Kapazitätsreservierungsflotte erfüllt wird.

Derzeit wird nur die Zuweisungsstrategie `prioritized` unterstützt. Diese Strategie sieht vor, dass die Kapazitätsreservierungsflotte Kapazitätsreservierungen unter Verwendung der Prioritäten erstellt, die Sie den Instance-Typ-Spezifikationen in der Konfiguration der Kapazitätsreservierungsflotte zugewiesen haben. Niedrigere Prioritätswerte bedeuten eine höhere Priorität für die Verwendung. Angenommen, Sie erstellen eine Kapazitätsreservierungsflotte, die die folgenden Instance-Typen und Prioritäten verwendet:

- `m4.16xlarge` – Priorität = 1
- `m5.16xlarge` – Priorität = 3
- `m5.24xlarge` – Priorität = 2

Die Flotte versucht zunächst, Kapazitätsreservierungen für `m4.16xlarge` zu erstellen. Wenn Amazon nicht EC2 über ausreichende `m4.16xlarge` Kapazitäten verfügt, versucht die Flotte, Kapazitätsreservierungen für zu erstellen`m5.24xlarge`. Wenn Amazon nicht EC2 über ausreichende `m5.24xlarge` Kapazitäten verfügt, erstellt die Flotte Kapazitätsreservierungen für`m5.16xlarge`.

Instance-Typ-Gewichtung

Die Instance-Typ-Gewichtung ist eine Gewichtung, die Sie jedem Instance-Typ in der Kapazitätsreservierungsflotte zuweisen. Die Gewichtung bestimmt, wie viele Kapazitätseinheiten jede Instance des jeweiligen Instance-Typs der Gesamtzielkapazität der Flotte anrechnet.

Sie können Gewichtungen basierend auf sinnvollen Einheiten für Ihre Workload zuweisen. Wenn Ihre Arbeitslast beispielsweise eine bestimmte Anzahl von v erfordertCPUs, können Sie Gewichtungen auf der Grundlage der Anzahl von v zuweisen, die von jedem Instance-Typ in der Kapazitätsreservierungsflotte CPUs bereitgestellt wird. Wenn Sie in diesem Fall eine Flotte CPUs für Kapazitätsreservierungen mithilfe von `m4.16xlarge` `m5.24xlarge` and-Instances erstellen, würden Sie jeder Instance wie folgt Gewichte zuweisen, die der Anzahl von v entsprechen:

- `m4.16xlarge`— 64 vCPUs, Gewicht = 64 Einheiten
- `m5.24xlarge`— 96 vCPUs, Gewicht = 96 Einheiten

Die Instance-Typ-Gewichtung bestimmt die Anzahl der Instances, für die die Kapazitätsreservierungsflotte Kapazität reserviert. Wenn eine Kapazitätsreservierungsflotte mit einer Gesamtzielkapazität von 384 Einheiten beispielsweise die Instance-Typen und Gewichtungen aus dem vorhergehenden Beispiel verwendet, könnte die Flotte Kapazität für 6 `m4.16xlarge`-Instances reservieren (384 Gesamtzielkapazität / 64 Instance-Typ-Gewichtung = 6 Instances) oder 4 `m5.24xlarge`-Instances (384 / 96 = 4).

Weisen Sie keine Instance-Typ-Gewichtungen oder eine Gewichtung von 1 zu, basiert die Gesamtzielkapazität ausschließlich auf der Anzahl der Instances. Wenn eine Kapazitätsreservierungsflotte mit einer Gesamtzielkapazität von 384 Einheiten beispielsweise die Instance-Typen aus dem vorhergehenden Beispiel verwendet, aber die Gewichtungen weglässt oder eine Gewichtung von 1 für beide Instance-Typen angibt, könnte die Flotte Kapazität für 384 `m4.16xlarge`- oder 384 `m5.24xlarge`-Instances reservieren.

Instance-Typ-Priorität

Die Instance-Typ-Priorität ist ein Wert, den Sie den Instance-Typen in der Flotte zuweisen. Anhand der Prioritäten wird bestimmt, welcher der für die Flotte angegebenen Instance-Typen für die Verwendung priorisiert werden soll.

Niedrigere Prioritätswerte bedeuten eine höhere Priorität für die Verwendung.

Erstellen einer Kapazitätsreservierungsflotte

Wenn Sie eine Kapazitätsreservierungsflotte erstellen, werden für die in der Flottenanforderung angegebenen Instance-Typen automatisch Kapazitätsreservierungen bis zur angegebenen Gesamtzielkapazität erstellt. Die Anzahl der Instances, für die die Kapazitätsreservierungsflotte Kapazität reserviert, hängt von der Gesamtzielkapazität und den Instance-Typ-Gewichtungen ab, die Sie in der Anforderung angeben. Weitere Informationen erhalten Sie unter Instance-Typ-Gewichtung und Gesamtzielkapazität.

Wenn Sie die Flotte erstellen, müssen Sie die zu verwendenden Instance-Typen und eine Priorität für jeden dieser Instance-Typen angeben. Weitere Informationen erhalten Sie unter Zuweisungsstrategie und Instance-Typ-Priorität.

> **Note**
>
> Die AWSServiceRoleForEC2CapacityReservationFleetserviceverknüpfte Rolle wird automatisch in Ihrem Konto erstellt, wenn Sie zum ersten Mal eine

Kapazitätsreservierungsflotte erstellen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Kapazitätsreservierungsflotten.

Derzeit unterstützen Kapazitätsreservierungsflotten nur die Übereinstimmungskriterien für open-Instances.

AWS CLI

So erstellen Sie eine Kapazitätsreservierungsflotte

Verwenden Sie den Befehl create-capacity-reservation-fleet.

```
aws ec2 create-capacity-reservation-fleet \
    --total-target-capacity 24 \
    --allocation-strategy prioritized \
    --instance-match-criteria open \
    --tenancy default \
    --end-date 2021-12-31T23:59:59.000Z \
    --instance-type-specifications file://instanceTypeSpecification.json
```

Der Inhalt von `instanceTypeSpecification.json` ist wie folgt:

```
[
  {
    "InstanceType": "m5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "Weight": 3.0,
    "AvailabilityZone":"us-east-1a",
    "EbsOptimized": true,
    "Priority" : 1
  }
]
```

Es folgt eine Beispielausgabe.

```
{
    "Status": "submitted",
    "TotalFulfilledCapacity": 0.0,
    "CapacityReservationFleetId": "crf-abcdef01234567890",
    "TotalTargetCapacity": 24
```

```
}
```

PowerShell

So erstellen Sie eine Kapazitätsreservierungsflotte

Verwenden Sie das cmdlet New-EC2CapacityReservationFleet.

```
New-EC2CapacityReservationFleet `
    -TotalTargetCapacity 24 `
    -AllocationStrategy "prioritized" `
    -InstanceMatchCriterion "open" `
    -Tenancy "default" `
    -EndDate 2021-12-31T23:59:59.000Z `
    -InstanceTypeSpecification $specification
```

Die Spezifikation ist wie folgt definiert.

```
$specification = New-Object Amazon.EC2.Model.ReservationFleetInstanceSpecification
$specification.InstanceType = "m5.xlarge"
$specification.InstancePlatform = "Linux/UNIX"
$specification.Weight = 3.0
$specification.AvailabilityZone = "us-east-1a"
$specification.EbsOptimized = $true
$specification.Priority = 1
```

Ändern einer Kapazitätsreservierungsflotte

Sie können die Gesamtzielkapazität und das Datum einer Kapazitätsreservierungsflotte jederzeit ändern. Wenn Sie die Gesamtzielkapazität einer Kapazitätsreservierungsflotte ändern, erstellt die Flotte automatisch neue Kapazitätsreservierungen oder ändert bzw. storniert bestehende Kapazitätsreservierungen in der Flotte, um die neue Gesamtzielkapazität zu erreichen. Wenn Sie das Enddatum für die Flotte ändern, werden die Enddaten für alle einzelnen Kapazitätsreservierungen entsprechend angepasst.

Überlegungen

- Nachdem Sie eine Flotte geändert haben, wechselt ihr Zustand zu `modifying`. Sie können keine zusätzlichen Änderungen an einer Flotte vornehmen, wenn sie sich im Zustand `modifying` befindet.

- Sie können keine Änderungen bezüglich Tenancy, Availability Zone, Instance-Typen, Instance-Plattformen, Prioritäten oder Gewichtungen vornehmen, die von einer Kapazitätsreservierungsflotte verwendet werden. Wenn Sie einen dieser Parameter ändern möchten, müssen Sie die vorhandene Flotte stornieren und eine neue Flotte mit den erforderlichen Parametern erstellen.
- Sie können `--end-date` und `--remove-end-date` nicht im selben Befehl angeben.

AWS CLI

Kapazitätsreservierungsflotte ändern

Verwenden Sie den Befehl modify-capacity-reservation-fleet.

Beispiel 1: Gesamtzielkapazität ändern

```
aws ec2 modify-capacity-reservation-fleet \
    --capacity-reservation-fleet-id crf-01234567890abcedf \
    --total-target-capacity 160
```

Beispiel 2: Enddatum ändern

```
aws ec2 modify-capacity-reservation-fleet \
    --capacity-reservation-fleet-id crf-01234567890abcedf \
    --end-date 2021-07-04T23:59:59.000Z
```

Beispiel 3: Enddatum entfernen

```
aws ec2 modify-capacity-reservation-fleet \
    --capacity-reservation-fleet-id crf-01234567890abcedf \
    --remove-end-date
```

PowerShell

Kapazitätsreservierungsflotte ändern

Verwenden Sie das cmdlet Edit-EC2CapacityReservationFleet.

Beispiel 1: Gesamtzielkapazität ändern

```
Edit-EC2CapacityReservationFleet `
```

```
    -CapacityReservationFleetId crf-01234567890abcedf `
    -TotalTargetCapacity 160
```

Beispiel 2: Enddatum ändern

```
Edit-EC2CapacityReservationFleet `
    -CapacityReservationFleetId crf-01234567890abcedf `
    -EndDate 2021-07-04T23:59:59.000Z
```

Beispiel 3: Enddatum entfernen

```
Edit-EC2CapacityReservationFleet `
    -CapacityReservationFleetId crf-01234567890abcedf `
    -RemoveEndDate
```

Stornieren einer Kapazitätsreservierungsflotte

Wenn Sie eine Kapazitätsreservierungsflotte und die reservierte Kapazität nicht mehr benötigen, können Sie die Flotte stornieren. Wenn Sie eine Flotte stornieren, ändert sich ihr Zustand in `cancelled` und sie kann keine neuen Kapazitätsreservierungen mehr erstellen. Außerdem werden alle individuellen Kapazitätsreservierungen in der Flotte abgebrochen. Die Instances, die zuvor in der reservierten Kapazität ausgeführt wurden, werden in der freigegebenen Kapazität weiterhin normal ausgeführt.

AWS CLI

So stornieren Sie eine Kapazitätsreservierungsflotte

Verwenden Sie den Befehl cancel-capacity-reservation-fleets.

```
aws ec2 cancel-capacity-reservation-fleets \
    --capacity-reservation-fleet-ids crf-abcdef01234567890
```

Es folgt eine Beispielausgabe.

```
{
    "SuccessfulFleetCancellations": [
        {
            "CurrentFleetState": "cancelling",
```

```
            "PreviousFleetState": "active",
            "CapacityReservationFleetId": "crf-abcdef01234567890"
        }
    ],
    "FailedFleetCancellations": []
}
```

PowerShell

So stornieren Sie eine Kapazitätsreservierungsflotte

Verwenden Sie das cmdlet Stop-EC2CapacityReservationFleet.

```
Stop-EC2CapacityReservationFleet `
    -CapacityReservationFleetId crf-abcdef01234567890
```

Beispiel für Kapazitätsreservierungsflotten-Konfigurationen

Im folgenden Beispiel wird eine Kapazitätsreservierungsflotte erstellt, die zwei Instance-Typen verwendet: `m5.4xlarge` und `m5.12xlarge`.

Es verwendet ein Gewichtungssystem, das auf der Anzahl von v basiert, die von den angegebenen Instance-Typen CPUs bereitgestellt werden. Die Gesamtzielkapazität ist `480` v. CPUs Der `m5.4xlarge` liefert 16 V CPUs und erhält ein Gewicht von`16`, während der 48 V `m5.12xlarge` liefert CPUs und ein Gewicht von erhält`48`. Mit diesem Gewichtungssystem wird die Kapazitätsreservierungsflotte dafür konfiguriert, Kapazität für 30 `m5.4xlarge`-Instances (480 / 16 = 30) oder 10 `m5.12xlarge`-Instances (480 / 48 = 10) zu reservieren.

Gemäß der Flottenkonfiguration wird die `m5.12xlarge`-Kapazität priorisiert und erhält die Priorität `1`. Der `m5.4xlarge`-Instance hingegen wird eine niedrigere Priorität zugeteilt: `2`. Das bedeutet, dass die Flotte zuerst versucht, die `m5.12xlarge` Kapazität zu reservieren, und nur dann versucht, die `m5.4xlarge` Kapazität zu reservieren, wenn Amazon nicht EC2 über ausreichende `m5.12xlarge` Kapazitäten verfügt.

Die Flotte reserviert die Kapazität für `Windows`-Instances und die Reservierung läuft automatisch am `October 31, 2021` um`23:59:59` UTC ab.

```
aws ec2 create-capacity-reservation-fleet \
    --total-target-capacity 480 \
    --allocation-strategy prioritized \
```

```
    --instance-match-criteria open \
    --tenancy default \
    --end-date 2021-10-31T23:59:59.000Z \
    --instance-type-specifications file://instanceTypeSpecification.json
```

Im Folgenden sehen Sie den Inhalt von `instanceTypeSpecification.json`.

```
[
    {
        "InstanceType": "m5.4xlarge",
        "InstancePlatform":"Windows",
        "Weight": 16,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 2
    },
    {
        "InstanceType": "m5.12xlarge",
        "InstancePlatform":"Windows",
        "Weight": 48,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 1
    }
]
```

Verwenden von serviceverknüpften Rollen für Kapazitätsreservierungsflotten

Die On-Demand-Kapazitätsreservierungsflotte verwendet dienstgebundene Rollen AWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle ist eine spezielle IAM-Rolle, die direkt mit Kapazitätsreservierungsflotten verknüpft ist. Servicebezogene Rollen sind von Capacity Reservation Fleet vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle vereinfacht das Einrichten von Kapazitätsreservierungsflotten, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Kapazitätsreservierungsflotten definieren die Berechtigungen ihrer serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, können die Rollen nur von der jeweiligen Kapazitätsreservierungsflotte übernommen werden. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre Kapazitätsreservierungsflotten-Ressourcen, da Sie die Berechtigung für den Zugriff auf die Ressourcen nicht versehentlich entfernen können.

Berechtigungen von serviceverknüpften Rollen für Kapazitätsreservierungsflotten

Capacity Reservation Fleet verwendet die angegebene dienstbezogene Rolle, AWSServiceRoleForEC2CapacityReservationFleetum in Ihrem Namen Kapazitätsreservierungen in einer Kapazitätsreservierungsflotte zu erstellen, zu beschreiben, zu ändern und zu stornieren.

Die AWSService RoleFor EC2 CapacityReservationFleet dienstbezogene Rolle vertraut darauf, dass die folgende Entität die Rolle übernimmt:

- `capacity-reservation-fleet.amazonaws.com`

Die Rolle verwendet die `AWSEC2CapacityReservationFleetRolePolicy` AWS verwaltete Richtlinie. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AWSEC2CapacityReservationFleetRolePolicy.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen von serviceverknüpften Rollen für Kapazitätsreservierungsflotten

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie mithilfe des `create-capacity-reservation-fleet` AWS CLI Befehls oder der `CreateCapacityReservationFleet` API eine Flotte für Kapazitätsreservierungen erstellen, wird die serviceverknüpfte Rolle automatisch für Sie erstellt.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie eine Kapazitätsreservierungsflotte erstellen, erstellt die Kapazitätsreservierungsflotte wieder die serviceverknüpfte Rolle für Sie.

Bearbeiten von serviceverknüpften Rollen für Kapazitätsreservierungsflotten

Mit der Kapazitätsreservierungsflotte können Sie die AWSService RoleFor EC2 CapacityReservationFleet servicebezogene Rolle nicht bearbeiten. Da möglicherweise verschiedene

Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rollenbeschreibung im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Kapazitätsreservierungsflotten

Wenn Sie ein Feature oder einen Service, die bzw. der eine servicegebundene Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle löschen, bevor Sie sie manuell löschen können.

> **Note**
>
> Falls der Kapazitätsreservierungsflotten-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt der Löschvorgang möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um die AWSService RoleFor EC2 CapacityReservationFleet serviceverknüpfte Rolle zu löschen

1. Verwenden Sie den `delete-capacity-reservation-fleet` AWS CLI Befehl oder die `DeleteCapacityReservationFleet` API, um die Kapazitätsreservierungsflotten in Ihrem Konto zu löschen.
2. Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSService RoleFor EC2 CapacityReservationFleet serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte Rollen für Kapazitätsreservierungsflotten

Kapazitätsreservierungsflotten unterstützen die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWS -Regionen und Endpunkte.

Überwachen Sie die Nutzung von Kapazitätsreservierungen anhand von Kennzahlen CloudWatch

Mithilfe von CloudWatch Kennzahlen können Sie Ihre Kapazitätsreservierungen effizient überwachen und ungenutzte Kapazitäten identifizieren, indem Sie CloudWatch Alarme einrichten, die Sie

benachrichtigen, wenn die Nutzungsgrenzwerte erreicht werden. Dies kann Ihnen helfen, ein konstantes Kapazitätsreservierung-Volumen beizubehalten und eine höhere Auslastung zu erreichen.

Kapazitätsreservierungen senden CloudWatch alle fünf Minuten Metrikdaten. Metriken für Kapazitätsreservierungen werden nicht unterstützt, die weniger als fünf Minuten aktiv sind.

Weitere Informationen zum Anzeigen von Metriken in der CloudWatch Konsole finden Sie unter Amazon CloudWatch Metrics verwenden. Weitere Informationen zum Erstellen von Alarmen finden Sie unter CloudWatch Amazon-Alarme erstellen.

Inhalt

- Kapazitätsreservierung-Nutzungsmetriken
- Kapazitätsreservierung-Metrikdimensionen
- CloudWatch Metriken für Kapazitätsreservierungen anzeigen

Kapazitätsreservierung-Nutzungsmetriken

Der `AWS/EC2CapacityReservations`-Namespace enthält die folgenden Nutzungsmetriken, mit denen Sie On-Demand-Kapazität innerhalb von Schwellenwerten überwachen und verwalten können, die Sie für Ihre Reservierung angeben.

Metrik	Beschreibung
`UsedInstanceCount`	Die Anzahl der Instances, die derzeit verwendet werden. Einheit: Anzahl
`AvailableInstanceCount`	Die Anzahl der verfügbaren Instances. Einheit: Anzahl
`TotalInstanceCount`	Die Gesamtzahl der reservierten Instances. Einheit: Anzahl
`InstanceUtilization`	

Metrik	Beschreibung
	Der Prozentsatz der Instances für reservierte Kapazität, die derzeit verwendet werden. Einheit: Prozent

Kapazitätsreservierung-Metrikdimensionen

Sie können die folgenden Dimensionen innerhalb der gewählten Region und dem ausgewählten Konto verwenden, um die in den vorherigen Tabellen aufgeführten Metriken zu verfeinern.

Dimension	Description
(Keine Dimension)	Diese Dimension filtert die angegebene Metrik für alle Kapazitätsreservierungen.
`CapacityReservationId`	Diese Dimension filtert die angegebene Metrik für alle identifizierten Kapazitätsreservierungen.
`InstanceType`	Diese Dimension filtert die angegebene Metrik für den identifizierten Instance-Typ.
`AvailabilityZone`	Diese Dimension filtert die angegebene Metrik für die identifizierte Availability Zone.
`InstanceMatchCriteria`	Diese Dimension filtert die angegebene Metrik für die identifizierten Instance-Übereinstimmungskriterien (`open` oder `targeted`).
`InstancePlatform`	Diese Dimension filtert die angegebene Metrik für die identifizierte Plattform.
`Tenancy`	

Dimension	Description
	Diese Dimension filtert die angegebene Metrik für die identifiz ierte Tenancy.

CloudWatch Metriken für Kapazitätsreservierungen anzeigen

Metriken werden zuerst nach dem Service-Namespace und dann nach den unterstützten Dimensionen gruppiert. Sie können die folgenden Vorgehensweisen nutzen, um die Metriken für Kapazitätsreservierungen anzuzeigen.

Um Metriken zur Kapazitätsreservierung über die CloudWatch Konsole anzuzeigen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Ändern Sie, falls erforderlich, die Region. Wählen Sie auf der Navigationsleiste die Region aus, in der sich Ihr Kapazitätsreservierung befindet. Weitere Informationen finden Sie unter -Regionen und Endpunkte.
3. Wählen Sie im Navigationsbereich Metrics (Metriken) aus.
4. Wählen Sie für Alle Metriken die Option EC2 Kapazitätsreservierungen aus.
5. Wählen Sie aus den vorherigen Metrikdimensionen Alle Kapazitätsreservierungen, Nach Kapazitätsreservierung, Nach Instance-Typ, Nach Availability Zone, Nach Plattform, Nach Instance-Übereinstimmungskriterien oder Nach Tenancy. Die Metriken werden dann nach „Keine Dimension“, `CapacityReservationId`, `InstanceType`, `AvailabilityZone`, `Platform`, `InstanceMatchCriteria` und `Tenancy` entsprechend gruppiert.
6. Verwenden Sie die Spaltenüberschrift, um die Metriken zu sortieren. Um eine Metrik grafisch darzustellen, müssen Sie das Kontrollkästchen neben der Metrik aktivieren.

Um Kennzahlen zur Kapazitätsreservierung anzuzeigen, verwenden Sie AWS CLI

Verwenden Sie den folgenden list-metrics-Befehl:

```
aws cloudwatch list-metrics --namespace "AWS/EC2CapacityReservations"
```

Unterauslastung der Kapazitätsreservierung überwachen

Sie können die Unterauslastung der Kapazitätsreservierung wie folgt überwachen:

Themen

- EventBridge Amazon-Veranstaltungen
- E-Mail- und Dashboard-Benachrichtigungen AWS Health

EventBridge Amazon-Veranstaltungen

AWS Health sendet Ereignisse an Amazon, EventBridge wenn eine Kapazitätsreservierung in Ihrem Konto in bestimmten Zeiträumen unter 20 Prozent ausgelastet ist. Mit EventBridge können Sie Regeln festlegen, die als Reaktion auf solche Ereignisse programmatische Aktionen auslösen. Sie können beispielsweise eine Regel erstellen, die eine Kapazitätsreservierung automatisch aufhebt, wenn ihre Auslastung über einen Zeitraum von 7 Tagen unter 20 Prozent fällt.

Ereignisse in EventBridge werden als JSON-Objekte dargestellt. Die Felder, die für das Ereignis einzigartig sind, sind im Abschnitt "Detail" des JSON-Objekt enthalten. Im Feld "Ereignis" ist der Name des Ereignisses enthalten. Das Feld "Ergebnis" enthält den vollständigen Status der Aktion, die zur Auslösung des Ereignisses führte. Weitere Informationen finden Sie unter Amazon EventBridge Event Patterns im EventBridge Amazon-Benutzerhandbuch.

Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Diese Funktion wird in nicht unterstützt AWS GovCloud (US).

Ereignisse

AWS Health sendet die folgenden Ereignisse, wenn die Kapazitätsnutzung für eine Kapazitätsreservierung unter 20 Prozent liegt.

- `AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION`

  Im Folgenden finden Sie ein Beispiel für ein Ereignis, das generiert wird, wenn eine neu erstellte Kapazitätsreservierung über einen Zeitraum von 24 Stunden unter 20 Prozent Kapazitätsauslastung liegt.

```
{
    "version": "0",
    "id": "b3e00086-f271-12a1-a36c-55e8ddaa130a",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-03-10T12:03:38Z",
```

```
    "region": "ap-south-1",
    "resources": [
        "cr-01234567890abcdef"
    ],
    "detail": {
        "eventArn": "arn:aws:health:ap-south-1::event/EC2/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_cr-01234567890abcdef-6211-4d50-9286-0c9fbc243f04",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION",
        "eventTypeCategory": "accountNotification",
        "startTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "endTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided
 here"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "cr-01234567890abcdef"
            }
        ]
    }
    }
```

- AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY

  Im Folgenden finden Sie ein Beispiel für ein Ereignis, das generiert wird, wenn eine oder mehrere Kapazitätsreservierungen über einen Zeitraum von 7 Tagen unter 20 Prozent Kapazitätsauslastung liegen.

```
{
    "version": "0", "id":"7439d42b-3c7f-ad50-6a88-25e2a70977e2",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-03-07T06:06:01Z",
    "region": "us-east-1",
    "resources": [
        "cr-01234567890abcdef | us-east-1b | t3.medium | Linux/UNIX | 0.0%",
```

```
        "cr-09876543210fedcba | us-east-1a | t3.medium | Linux/UNIX | 0.0%"
    ],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/
EC2/AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY_726c1732-d6f6-4037-b9b8-
bec3c2d3ba65",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY",
        "eventTypeCategory": "accountNotification",
        "startTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "endTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided
 here"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "cr-01234567890abcdef | us-east-1b | t3.medium |
 Linux/UNIX | 0.0%"
            },
            {
                "entityValue": "cr-09876543210fedcba | us-east-1a | t3.medium |
 Linux/UNIX | 0.0%"
            }
        ]
    }
}
```

Erstellen Sie eine EventBridge Regel

Um E-Mail-Benachrichtigungen zu erhalten, wenn Ihre Kapazitätsreservierungsauslastung unter 20 Prozent fällt, erstellen Sie ein Amazon SNS SNS-Thema und dann eine EventBridge Regel für das `AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION` Ereignis.

So erstellen Sie das Amazon-SNS-Thema

1. Öffnen Sie die Amazon SNS SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie im Navigationsbereich Topics (Themen) und Create topic (Thema erstellen).

3. Wählen Sie unter Type (Typ) die Option Standard aus.
4. Geben Sie unter Name einen Namen für das neue Thema ein.
5. Wählen Sie Thema erstellen aus.
6. Wählen Sie Create subscription (Abonnement erstellen) aus.
7. Wählen Sie für Protokoll die Option E-Mail aus und geben Sie dann für Endpunkt die E-Mail-Adresse ein, die die Benachrichtigungen erhält.
8. Wählen Sie Create subscription (Abonnement erstellen) aus.
9. Die oben eingegebene E-Mail-Adresse erhält eine E-Mail-Nachricht mit der folgenden Betreffzeile: `AWS Notification - Subscription Confirmation`. Befolgen Sie die Anweisungen, um Ihr Abonnement zu bestätigen.

Um die Regel zu erstellen EventBridge

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Rules (Regeln) und anschließend Create rule (Regel erstellen) aus.
3. Geben Sie unter Name einen Namen für die neue Regel ein.
4. Bei Regeltyp wählen Sie Regel mit einem Ereignismuster aus.
5. Wählen Sie Weiter aus.
6. Gehen Sie bei Ereignismuster wie folgt vor:
   a. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.
   b. Wählen Sie unter AWS -Service die Option AWS Health aus.
   c. Wählen Sie als Ereignistyp die Option EC2 ODCR-Benachrichtigung zur Unterauslastung aus.
7. Wählen Sie Weiter aus.
8. Gehen Sie bei Ziel 1 wie folgt vor:
   a. Bei Zieltypen wählen Sie AWS -Service aus.
   b. Für Select a target (Wählen Sie ein Ziel aus), wählen Sie SNS-Thema aus.
   c. Wählen Sie für Thema das Thema aus, das Sie zuvor erstellt haben.
9. Wählen Sie Weiter und dann erneut Weiter.
10. Wählen Sie Regel erstellen aus.

E-Mail- und Dashboard-Benachrichtigungen AWS Health

AWS Health sendet die folgenden E-Mails und AWS Health Dashboard Benachrichtigungen, wenn die Kapazitätsauslastung für Kapazitätsreservierungen in Ihrem Konto unter 20 Prozent fällt.

- Individuelle Benachrichtigungen für jede neu erstellte Kapazitätsreservierung, die in den letzten 24 Stunden weniger als 20 Prozent ausgelastet war.
- Eine zusammenfassende Benachrichtigung für alle Kapazitätsreservierungen, die in den letzten 7 Tagen weniger als 20 Prozent ausgelastet waren.

Die E-Mail-Benachrichtigungen und AWS Health Dashboard Benachrichtigungen werden an die E-Mail-Adresse gesendet, die mit dem AWS Konto verknüpft ist, dem die Kapazitätsreservierungen gehören. Die Benachrichtigungen enthalten die folgenden Informationen:

- Die ID der Kapazitätsreservierung.
- Die Availability Zone der Kapazitätsreservierung.
- Die durchschnittliche Nutzungsrate für die Kapazitätsreservierung.
- Der Instance-Typ und die Plattform (Betriebssystem) der Kapazitätsreservierung.

Wenn die Kapazitätsauslastung für eine Kapazitätsreservierung in Ihrem Konto innerhalb von 24 Stunden und 7 Tagen unter 20 Prozent fällt, werden außerdem Ereignisse AWS Health an EventBridge gesendet. Mit können Sie Regeln erstellenEventBridge, die automatische Aktionen wie das Senden von E-Mail-Benachrichtigungen oder das Auslösen von AWS Lambda Funktionen als Reaktion auf solche Ereignisse aktivieren. Weitere Informationen finden Sie unter Unterauslastung der Kapazitätsreservierung überwachen.

Statusänderungen von zukünftigen Kapazitätsreservierungen überwachen

Amazon EC2 sendet ein Ereignis an Amazon, EventBridge wenn sich der Status einer zukünftigen Kapazitätsreservierung ändert.

Es folgt ein Beispiel für dieses Ereignis. In diesem Beispiel ist die zukünftige Kapazitätsreservierung in den Status `scheduled` übergegangen. Beachten Sie den im `detail-type`-Feld hervorgehobenen Status.

```
{
   "version":"0",
```

```
   "id":"12345678-1234-1234-1234-123456789012",
   "detail-type":"EC2 Capacity Reservation Scheduled",
   "source":"aws.ec2",
   "account":"123456789012",
   "time":"yyyy-mm-ddThh:mm:ssZ",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdefg"
   ],
   "detail":{
      "capacity-reservation-id":"cr-1234567890abcdefg",
      "state":"scheduled"
   }
}
```

Die möglichen Werte für das `detail-type`-Feld sind:

- `Scheduled`
- `Active`
- `Delayed`
- `Unsupported`
- `Failed`
- `Expired`

Weitere Informationen zu diesen Zuständen finden Sie unter Den Status einer Kapazitätsreservierung anzeigen.

Sie können EventBridge Amazon-Ereignisse erstellen, die diese Ereignisse überwachen und dann bestimmte Aktionen auslösen, wenn sie auftreten. Weitere Informationen finden Sie unter Regeln erstellen, die auf Ereignisse in Amazon reagieren EventBridge.

Sie können das folgende Ereignismuster verwenden, um eine Regel zu erstellen, die alle Statusänderungs-Ereignisse überwacht.

```
{
  "source": ["aws.ec2"],
  "detail-type": [{
    "prefix": "EC2 Capacity Reservation"
  }]
```

```
}
```

Sie können das folgende Ereignismuster verwenden, um eine Regel zu erstellen, die nur bestimmte Statusänderungen überwacht.

```
{
  "source": ["aws.ec2"],
  "detail-type": [{
    "prefix": "EC2 Capacity Reservation state"
  }]
}
```

Das folgende Ereignismuster überwacht beispielsweise Ereignisse, die gesendet werden, wenn eine zukünftige Kapazitätsreservierung in den Status `active` übergeht.

```
{
  "source": ["aws.ec2"],
  "detail-type": [{
    "prefix": "EC2 Capacity Reservation Active"
  }]
}
```

Reservierungen für unterbrechbare Kapazitäten

Reservierungen für unterbrechbare Kapazitäten helfen Ihnen dabei, ungenutzte Kapazität vorübergehend für andere Workloads innerhalb Ihres Kontos verfügbar zu machen. Auf diese Weise haben Sie die Kontrolle darüber, Kapazität bei Bedarf zurückzugewinnen. Wenn Sie Kapazität zurückfordern, werden alle Instances, die innerhalb der unterbrechbaren Reservierung laufen, beendet. Nachdem Sie eine unterbrechbare Reservierung erstellt haben, können Sie sie mithilfe von AWS Resource Access Manager (RAM) für weitere AWS Konten oder Ihre AWS Organisation freigeben.

Verwenden Sie unterbrechbare Kapazitätsreservierungen, wenn Sie ungenutzte reservierte Kapazität außerhalb der Spitzenzeiten, zwischen Bereitstellungen oder bei sinkender Arbeitslast haben. Wenn Sie ein anderes Team kennen, das diese Kapazität nutzen könnte, können Sie sie zur Verfügung stellen, indem Sie eine unterbrechbare Kapazitätsreservierung erstellen. Wenn Ihre kritische Arbeitslast wieder Kapazität benötigt, können Sie sie zurückgewinnen.

Sie können unterbrechbare Kapazitätsreservierungen wie folgt verwenden:

- Kapazitätsinhaber — Sie sind der Eigentümer der Quellkapazitätsreservierung und erstellen die unterbrechbare Kapazitätsreservierung, um ungenutzte Kapazität mit anderen Teams zu teilen und gleichzeitig die Kontrolle zu behalten, um sie bei Bedarf zurückzugewinnen.
- Kapazitätsverbraucher — Sie starten Instances im Rahmen gemeinsam genutzter unterbrechbarer Reservierungen und sind sich bewusst, dass Ihre Instances beendet werden können, wenn der Eigentümer Kapazität zurückfordert.

Themen

- Funktionsweise
- Fakturierung
- Überlegungen
- Reservierungen für unterbrechbare Kapazitäten für Kapazitätsbesitzer
- Reservierungen für unterbrechbare Kapazitäten für Kapazitätsverbraucher
- Überwachen Sie unterbrechbare Kapazitätsreservierungen mit und EventBridge CloudTrail

Funktionsweise

Um ungenutzte Kapazität anderen Teams zur Verfügung zu stellen, erstellen Sie eine unterbrechbare Reservierung, indem Sie die Anzahl der ungenutzten Instances aus Ihrer Quellreservierung angeben, die Sie gemeinsam nutzen möchten. Wenn Sie die unterbrechbare Reservierung erstellen, übertragen wir diese Instanzen aus Ihrer Quellreservierung auf die neue unterbrechbare Reservierung in Ihrem Konto.

Wir behalten die Verknüpfung zwischen der Quellreservierung und der unterbrechbaren Kapazitätsreservierung bei. Wenn Sie Ihre Kapazität zurückfordern, werden daher alle laufenden Consumer-Instances beendet und die Kapazität wird auf Ihre ursprüngliche Quellreservierung zurückgesetzt.

Wichtigste Funktionen:

- Machen Sie ungenutzte Kapazität vorübergehend verfügbar und behalten Sie gleichzeitig die Kontrolle, um sie zurückzugewinnen
- Sie können jederzeit Kapazität zurückgewinnen. Weitere Informationen finden Sie unter Prozess und Nachverfolgung der Reklamation.
- Mit AWS Resource Access Manager (RAM) für weitere Konten oder Ihre AWS Organisation freigeben

Fakturierung

Wenn Sie eine unterbrechbare Reservierung erstellen, wird sie Ihnen als eigenständige neue Reservierung in Rechnung gestellt. Dadurch wird Ihre Abrechnung aufgeteilt:

- Quellenreservierung: Ihnen wird die Gesamtkapazität abzüglich der zugewiesenen Kapazität in Rechnung gestellt
- Unterbrechbare Reservierung: Ihnen wird die zugewiesene Kapazität in Rechnung gestellt

Weitere Informationen zur Abrechnung von Kapazitätsreservierungen auf Abruf finden Sie unter Preise und Abrechnung von Kapazitätsreservierungen.

Überlegungen

Bevor Sie unterbrechbare Kapazitätsreservierungen nutzen, sollten Sie sich mit den folgenden Einschränkungen und Anforderungen vertraut machen, die für Kapazitätsbesitzer und -verbraucher gelten.

Besitzer von Kapazitäten

- Sie können eine unterbrechbare Kapazitätsreservierung nicht direkt ändern oder stornieren. Um sie zu bearbeiten, aktualisieren Sie die Kapazität, die aus der Quellkapazitätsreservierung zugewiesen wurde.
- Sie können nur unterbrechbare Reservierungen anzeigen, starten, taggen, teilen und ihnen die Abrechnung zuweisen.
- Sie können pro Quellkapazitätsreservierung nur eine unterbrechbare Zuteilung erstellen.

Kapazitätsverbraucher

- Bei unterbrechbaren Kapazitätsreservierungen handelt es sich standardmäßig um gezielte Kapazitätsreservierungen. Sie müssen sie also beim Start Ihrer Instance gezielt einsetzen.
- Sie können keine unterbrechbaren Kapazitätsreservierungen zu Kapazitätsreservierungsgruppen hinzufügen.
- Wir empfehlen, unterbrechbare Kapazitätsreservierungen nur für Anwendungen zu verwenden, die unterbrochen werden können.

- Ihre Instances werden beendet, wenn der Eigentümer Kapazität zurückfordert — es gibt keinen Fallback auf On-Demand oder Spot. Weitere Informationen finden Sie unter Erfahrung mit Unterbrechungen.

Reservierungen für unterbrechbare Kapazitäten für Kapazitätsbesitzer

Der Kapazitätsinhaber ist der Account, der Eigentümer der Quellkapazitätsreservierung ist und der die unterbrechbare Kapazitätsreservierung erstellt, um ungenutzte Kapazität mit anderen Teams zu teilen und gleichzeitig die Kontrolle zu behalten, um sie bei Bedarf zurückzufordern.

In diesem Abschnitt wird beschrieben, wie Sie (der Kapazitätsinhaber) eine unterbrechbare Kapazitätsreservierung erstellen, ändern, zurückfordern und nachverfolgen können.

Themen

- Eine unterbrechbare Kapazitätsreservierung erstellen
- Sehen Sie sich Ihre Reservierung für unterbrechbare Kapazitäten an
- Änderung Ihrer Reservierung für unterbrechbare Kapazitäten
- Prozess und Nachverfolgung der Reklamation
- Unterbrechbare Reservierungen teilen

Eine unterbrechbare Kapazitätsreservierung erstellen

Erstellen Sie eine unterbrechbare Kapazitätsreservierung, um ungenutzte Kapazität aus Ihrer Quellreservierung für andere Workloads verfügbar zu machen und gleichzeitig die Kontrolle zu behalten, um sie bei Bedarf zurückzugewinnen.

Voraussetzungen

Bevor Sie eine unterbrechbare Zuteilung erstellen, stellen Sie sicher, dass Ihre On-Demand-Kapazitätsreservierung an der Quelle die folgenden Anforderungen erfüllt:

- Ihre Kapazitätsreservierung muss sich im Status „Aktiv“ befinden und es muss kein Enddatum festgelegt sein. Sie können keine Zuweisungen für Reservierungen erstellen, die ausstehen, abgelaufen oder storniert sind oder deren Enddatum geplant ist.
- Ihre Kapazitätsreservierung muss über verfügbare Kapazitäten für die Zuweisung verfügen. Sie können nur verfügbare Instances (auch ungenutzte Kapazität genannt) zuweisen.

- Sie können pro Quellkapazitätsreservierung nur eine unterbrechbare Zuteilung erstellen. Wenn bereits eine Zuweisung vorhanden ist, müssen Sie sie ändern oder stornieren, bevor Sie eine neue erstellen können.
- Sie können einer unterbrechbaren Kapazitätsreservierung maximal 1000 Instances gleichzeitig zuweisen.

Sie können die Konsole oder die verwenden, AWS CLI um eine unterbrechbare Kapazitätsreservierung zu erstellen.

Console

Um eine unterbrechbare Kapazitätsreservierung zu erstellen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Kapazitätsreservierungen.
3. Wählen Sie Ihre Kapazitätsreservierung aus.
4. Wählen Sie „Aktionen“, „Unterbrechbare Zuteilung erstellen“.
5. Geben Sie unter Zuzuordnende Instanzen die Anzahl der zuzuweisenden Instanzen ein.
6. (Optional) Fügen Sie Tags hinzu.
7. Wählen Sie „Unterbrechbare Kapazitätszuweisung erstellen“.

AWS CLI

Um eine unterbrechbare Kapazitätsreservierung zu erstellen

Verwenden Sie den Befehl create-interruptible-capacity-reservation-allocation:

```
aws ec2 create-interruptible-capacity-reservation-allocation \
    --capacity-reservation-id cr-1234567890abcdef0 \
    --instance-count 10
```

Sehen Sie sich Ihre Reservierung für unterbrechbare Kapazitäten an

Nachdem Sie eine unterbrechbare Kapazitätsreservierung erstellt haben, können Sie die unterbrechbare Reservierung in Ihrem Konto oder von einer bestimmten Ressource aus einsehen.

Alle Reservierungen für unterbrechbare Kapazitäten in Ihrem Konto anzeigen

Gehen Sie wie folgt vor, um die Reservierungen für unterbrechbare Kapazitäten in Ihrem Konto einzusehen.

Console

Um die unterbrechbaren Kapazitätsreservierungen in Ihrem Konto einzusehen

1. Rufen Sie in der Konsole die Seite „Kapazitätsreservierungen“ auf.
2. Suchen Sie in der Spalte „Typ“ nach Reservierungen mit „Unterbrechungsfrei“.
3. Wählen Sie die unterbrechbare Reservierung aus, um Details anzuzeigen.

AWS CLI

Um die Reservierungen für unterbrechbare Kapazitäten in Ihrem Konto einzusehen

```
aws ec2 describe-capacity-reservations \
    --capacity-reservation-id cr-interruptible-id \
    --filters Name=interruptible,Values=true
```

Sehen Sie sich die Reservierung unterbrechbarer Kapazitäten aus einer bestimmten Quelle an

Gehen Sie wie folgt vor, um die unterbrechbare Kapazitätsreservierung anzuzeigen, die aus einer bestimmten Quellkapazitätsreservierung erstellt wurde.

```
aws ec2 describe-capacity-reservations \
    --capacity-reservation-id cr-source-id
```

In der Antwort finden Sie ein `interruptibleCapacityAllocations` Objekt, das die Reservierungs-ID für unterbrechbare Kapazitäten und Details zur Zuteilung enthält. Informationen zur Antwortstruktur finden Sie InterruptibleCapacityAllocationin der Amazon EC2 API-Referenz.

Änderung Ihrer Reservierung für unterbrechbare Kapazitäten

Gehen Sie wie folgt vor, um Ihre Reservierung für unterbrechbare Kapazitäten zu bearbeiten oder zu stornieren.

Note

- Wenn Sie die Zuteilung reduzieren, fordern wir zuerst die verfügbaren Instances zurück, dann die laufenden Instances, bis wir die angeforderte Anzahl erreicht haben. Wenn wir die Anzahl mit verfügbaren Instances vollständig decken können, erfolgt keine Kündigung. Alle Änderungen an der Anzahl der zugewiesenen Instanzen werden über die Quellkapazitätsreservierung vorgenommen, nicht direkt über die unterbrechbare Kapazitätsreservierung.
- Sie können eine unterbrechbare Kapazitätsreservierung nur um maximal 1000 Instanzen gleichzeitig ändern (erhöhen oder verringern).

Bearbeiten Sie Ihre Reservierung für unterbrechbare Kapazitäten

Gehen Sie wie folgt vor, um Ihre Reservierung für unterbrechbare Kapazitäten zu bearbeiten.

Console

1. Wählen Sie auf der Detailseite der Quellkapazitätsreservierung die Option Aktionen aus. Klicken Sie dann auf „Reservierung unterbrechbarer Kapazitäten bearbeiten“.
2. Geben Sie für zuzuweisende Instances die neue Nummer ein:
   - Fügen Sie mehr Kapazität zur gemeinsamen Nutzung hinzu
   - Nutzen Sie die Kapazität Ihrer ursprünglichen Kapazitätsreservierung zurück
3. Wählen Sie Aktualisieren aus.

AWS CLI

```
aws ec2 update-interruptible-capacity-reservation-allocation \
    --capacity-reservation-id cr-1234567890abcdef0 \
    --target-instance-count 80
```

Stornieren Sie Ihre unterbrechbare Kapazitätsreservierung

Gehen Sie wie folgt vor, um die Zuweisung dauerhaft zu entfernen und die gesamte Kapazität zurückzugeben.

Console

1. Navigieren Sie auf der Seite mit den Details zur Quellkapazitätsreservierung zu den Details der unterbrechbaren Kapazitätszuweisung.
2. Wählen Sie Allokation für unterbrechbare Dateien bearbeiten aus.
3. Geben Sie für Anzahl der Instanzen den Wert 0 ein.
4. Wählen Sie Aktualisieren aus.

AWS CLI

```
aws ec2 update-interruptible-capacity-reservation-allocation \
--capacity-reservation-id cr-1234567890abcdef0 \
--target-instance-count 0
```

Prozess und Nachverfolgung der Reklamation

Wenn Sie Kapazität zurückfordern:

- Laufende Instances erhalten aufgrund von EventBridge Ereignissen eine zweiminütige Warnung, dass sie unterbrochen wird.
- Nach Ablauf der Kündigungsfrist werden laufende Instances in der zurückgeforderten Kapazität heruntergefahren und beendet.
- Nach der Kündigung stehen die zurückgeforderten Instances in Ihrer Quellkapazitätsreservierung zur sofortigen Nutzung zur Verfügung.
- Ihr Zuteilungsstatus ändert sich von aktuell zu aktiv, wenn der Vorgang abgeschlossen ist.

Die vollständige Rückforderung kann je nach Instance-Typ und Shutdown-Zeit einige Minuten dauern. Weitere Informationen zu der EventBridge Benachrichtigung, die Sie erhalten, wenn der Vorgang abgeschlossen ist, finden Sie unter. Abschluss der Reklamation

Verfolgen Sie den Status der Reklamation

Überwachen Sie den Fortschritt der Reklamation, indem Sie Ihre ursprüngliche Reservierung beschreiben:

```
aws ec2 describe-capacity-reservations \
```

```
--capacity-reservation-id cr-1234567890abcdef0
```

In der Antwort werden die folgenden Felder innerhalb des `interruptibleCapacityAllocation` Objekts angezeigt:

- `instance-count`: Aktuell zugewiesene Instanzen
- `target-instance-count`: Angeforderte Menge nach der Rückforderung
- `status`: Wird während der Reklamation aktualisiert und ist aktiv, wenn sie abgeschlossen ist

Unterbrechbare Reservierungen teilen

Mit AWS Resource Access Manager (RAM) können Sie unterbrechbare Reservierungen nur innerhalb Ihrer AWS Organisation gemeinsam nutzen.

Überlegungen:

- Wenn ein Kundenkonto Ihr Unternehmen verlässt, wird die unterbrechbare Reservierung automatisch von diesem Konto getrennt.
- Alle Instances, die im Rahmen der Reservierung ohne gemeinsame Nutzung laufen, werden irgendwann beendet.
- Alle anderen Funktionen zur gemeinsamen Nutzung funktionieren genauso wie standardmäßige Kapazitätsreservierungen.

Vollständige Verfahren zur gemeinsamen Nutzung finden Sie unter Kapazitätsreservierungen teilen.

Reservierungen für unterbrechbare Kapazitäten für Kapazitätsverbraucher

Der Kapazitätsverbraucher ist der Account, der Instances in gemeinsam genutzte unterbrechbare Kapazitätsreservierungen einleitet, wobei davon ausgegangen wird, dass ihre Instances beendet werden können, wenn der Eigentümer Kapazität zurückfordert.

In diesem Abschnitt erfahren Sie, wie Sie (der Kapazitätsverbraucher) Instances in einer unterbrechbaren Kapazitätsreservierung starten können. Außerdem erfahren Sie, was passiert, wenn Kapazität vom Eigentümer zurückgefordert wird.

Themen

- Eine unterbrechbare Kapazitätsreservierung anzeigen

- Starten Sie Instances in unterbrechbaren Reservierungen
- Erfahrung mit Unterbrechungen

Eine unterbrechbare Kapazitätsreservierung anzeigen

Gehen Sie wie folgt vor, um eine unterbrechbare Kapazitätsreservierung einzusehen.

Console

Um Reservierungen für unterbrechbare Kapazitäten in Ihrem Konto einzusehen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Kapazitätsreservierungen.
3. Suchen Sie in der Spalte Typ nach Reservierungen, die als unterbrechbar gekennzeichnet sind.
4. Beachten Sie, dass die Reservierung IDs zur Verwendung in Ihrer Instance gestartet wird.

AWS CLI

Um alle unterbrechbaren Kapazitätsreservierungen in Ihrem Konto zu finden

Verwenden Sie den -Befehl:describe-capacity-reservations

```
aws ec2 describe-capacity-reservations \
--filters Name=state,Values=active
```

Suchen Sie nach Reservierungen, wo `Interruptible` `true` in der Antwort darauf gesetzt wurde.

Um gezielt nach unterbrechbaren Reservierungen zu filtern

Verwenden Sie den folgenden Befehl:

```
aws ec2 describe-capacity-reservations \
--capacity-reservation-ids cr-example123 \
--query 'CapacityReservations[?Interruptible==`true`]'
```

> **Note**
>
> Bei Reservierungen für unterbrechbare Kapazitäten handelt es sich standardmäßig um gezielte Kapazitätsreservierungen. Sie müssen sie daher beim Start Ihrer Instance gezielt auswählen. Im Gegensatz zu offenen Reservierungen decken unterbrechbare Reservierungen nicht automatisch die entsprechenden Instances ab. Sie müssen die Reservierungs-ID beim Start explizit angeben.

Starten Sie Instances in unterbrechbaren Reservierungen

Gehen Sie wie folgt vor, um EC2 Amazon-Instances für unterbrechbare Kapazitätsreservierungen innerhalb Ihres Kontos zu starten.

> **Note**
>
> Wir empfehlen, dass Sie unterbrechbare Kapazitätsreservierungen nur für Anwendungen verwenden, die unterbrochen werden können.

Console

Um Instances in unterbrechbaren Kapazitätsreservierungen zu starten

1. Öffnen Sie die Amazon EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im EC2 Amazon-Dashboard die Option Launch instance aus.
3. Konfigurieren Sie Ihre Instance-Einstellungen.
4. Wählen Sie unter Erweiterte Informationen zur Kapazitätsreservierung die Option Unterbrechungsfreie Instances in Ihrer aktiven Reservierung starten aus.
5. Wählen Sie die Reservierungs-ID für unterbrechbare Dateien und die Kaufoption für neue Instances aus.
6. Wählen Sie Launch Instance (Instance starten) aus.

AWS CLI

```
aws ec2 run-instances \
```

```
--instance-type m5.large \
--count 2 \
--image-id ami-12345678 \
--instance-market-options '{
    "MarketType": "interruptible-capacity-reservation"
}' \
--capacity-reservation-specification '{
    "CapacityReservationTarget": {
        "CapacityReservationId": "cr-abcdef1234567890"
    }
}'
```

Starten Sie Instances mit Auto Scaling Scaling-Gruppen

Sie können Instances auch mithilfe von Auto Scaling Scaling-Gruppen mit Startvorlagen in unterbrechbaren Reservierungen starten. Konfigurieren Sie die Startvorlage mit dem Markttyp für Unterbrechungen und der Reservierungs-ID und erstellen Sie dann mithilfe dieser Vorlage Ihre Auto Scaling Scaling-Gruppe. Weitere Informationen finden Sie unter Unterbrechungskapazitätsreservierungen mit EC2 Auto Scaling.

Erfahrung mit Unterbrechungen

Wenn Kapazität vom Eigentümer zurückgefordert wird, erhalten Sie 2 Minuten vor Beendigung der Instance eine Benachrichtigung über die Unterbrechung. Diese Warnung kommt aufgrund von EventBridge Ereignissen, sodass Sie Zeit haben, um:

- Speichern Sie Ihre Arbeit oder überprüfen Sie Ihre Anwendungen
- Prozesse herunterfahren
- Bereiten Sie sich zum Beispiel auf die Kündigung vor

Die EventBridge Veranstaltung enthält Einzelheiten darüber, welche Instanzen beendet werden, und die genaue Kündigungszeit. Weitere Informationen finden Sie unter Warnung vor Instanzunterbrechung.

Überwachen Sie unterbrechbare Kapazitätsreservierungen mit und EventBridge CloudTrail

Reservierungen für unterbrechbare Kapazitäten senden EventBridge Benachrichtigungen und CloudTrail Ereignisse, die Ihnen helfen, Kapazitätsänderungen zu überwachen und darauf zu reagieren.

Themen

- EventBridge Benachrichtigungen
- CloudTrail Ereignisse

EventBridge Benachrichtigungen

Sie erhalten zwei Arten von EventBridge Benachrichtigungen. Informationen zum Einrichten von EventBridge Benachrichtigungen finden Sie unter EventBridge Amazon-Regeln erstellen.

Warnung vor Instanzunterbrechung

Wenn Sie Instances in einer unterbrechbaren Reservierung ausführen, erhalten Sie diese Benachrichtigung 2 Minuten vor der Kündigung Ihrer Instances:

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Interruptible Capacity Reservation Instance Interruption
 Warning",
    "source": "aws.ec2",
    "account": "[instance owner Account ID]",
    "time": "[Current time in yyyy-mm-ddThh:mm:ssZ]",
    "resources": "[instance arn]",
    "region": "[region]",
    "detail": {
        "instance-id": "[instance-id]",
        "instance-action": "terminate",
        "instance-termination-time": "yyyy-mm-ddThh:mm:ssZ",
        "azId": "[availability-zone-id]"
    }
}
```

Abschluss der Reklamation

Wenn Sie Eigentümer der Quellreservierung sind, erhalten Sie diese Benachrichtigung, wenn die Kapazitätsrückgewinnung abgeschlossen ist:

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Capacity Reservation Interruptible Reclamation Complete",
```

```
    "source": "aws.ec2",
    "account": "[source Capacity Reservation Owner Account ID]",
    "time": "[Current time in yyyy-mm-ddThh:mm:ssZ]",
    "region": "us-east-1",
    "resources": ["source_cr_arn"],
    "detail": {
        "sourceCapacityReservationId": "string",
        "instanceType": "string",
        "availabilityZoneId": "string",
        "TotalInstanceCount": "current total count in the source",
        "ReclaimedInstanceCount": "count of instances added to the source",
        "targetInstanceCount": "number"
    }
}
```

CloudTrail Ereignisse

CloudTrail protokolliert diese Ereignisse für unterbrechbare Kapazitätsreservierungen:

- `InterruptibleCapacityReservationCreated`— Wenn Sie eine unterbrechbare Zuteilung erstellen
- `InterruptibleCapacityReservationAllocationUpdated`— Wenn Sie die Zuordnung ändern
- `InterruptibleCapacityReservationCancelled`— Wenn Sie die Zuordnung stornieren
- `CapacityReservationModified`— Wenn wir die Quellreservierung für die Zuordnung ändern
- `InterruptibleCapacityReservationInstancesTerminated`— Wenn wir Instanzen während der Rückforderung beenden

Kapazitätsblöcke für ML

Kapazitätsblöcke für ML erlauben es Ihnen, GPU-basierte beschleunigte Computing-Instances für einen zukünftigen Zeitpunkt zu reservieren, um Ihre kurzfristigen Machine Learning (ML)-Workloads zu unterstützen. Instances, die innerhalb eines Kapazitätsblocks ausgeführt werden, werden innerhalb von Amazon automatisch nahe beieinander platziert EC2 UltraClusters, um blockierungsfreie Netzwerke im Petabit-Bereich mit niedriger Latenz zu gewährleisten.

Sie können Kapazitätsblöcke auch verwenden, um Kapazität für Amazon zu reservieren EC2 UltraServers. UltraServers verbinden Sie mehrere EC2 Amazon-Instances innerhalb einer Accelerator-Verbindung mit niedriger Latenz und hoher Bandbreite. Sie können UltraServers es

verwenden, um die rechen- und speicherintensivsten AI/ML Workloads in den Bereichen Training, Feinabstimmung und Inferenz zu bewältigen. Weitere Informationen finden Sie auf Amazon EC2 UltraServers.

Mit Kapazitätsblöcken können Sie sehen, wann GPU-Instance-Kapazität an zukünftigen Terminen verfügbar ist, und Sie können einen Kapazitätsblock so planen, dass er zu einem Zeitpunkt startet, der für Sie am besten passt. Wenn Sie einen Kapazitätsblock reservieren, erhalten Sie eine vorhersehbare Kapazitätsgarantie für GPU-Instance und zahlen nur für die Zeit, die Sie benötigen. Wir empfehlen Capacity Blocks GPUs , wenn Sie Ihre ML-Workloads tage- oder wochenlang unterstützen müssen und nicht für eine Reservierung bezahlen möchten, während Ihre GPU-Instances nicht genutzt werden.

Im Folgenden sind einige häufige Anwendungsfälle für Kapazitätsblöcke aufgeführt.

- Modell-Training und Feinabstimmung für Machine Learning (ML) – Erhalten Sie ununterbrochenen Zugriff auf die GPU-Instances, die Sie für die Durchführung des ML-Modell-Trainings und der Feinabstimmung reserviert haben.
- ML-Experimente und Prototypen – Führen Sie Experimente durch und erstellen Sie Prototypen, die kurzfristig GPU-Instances erfordern.

Sie können einen Kapazitätsblock mit den folgenden Spezifikationen reservieren:

- Reservieren Sie eine Startzeit bis zu 8 Wochen im Voraus
- Legen Sie eine Reservierungsdauer von einem bis 14 Tagen oder einem Vielfachen von 7 Tagen bis zu 182 Tagen fest (z. B. 21 Tage, 28 Tage)
- Konfigurieren Sie bis zu 64 Instances pro Kapazitätsblock
- Konfigurieren Sie bis zu 256 Instances über mehrere Kapazitätsblöcke hinweg

Bei Amazon EC2 UltraServers UltraServer entspricht jeder Block einem Kapazitätsblock. Sie können mit einer UltraServers einzigen Anfrage mehrere anfordern.

Sie können Kapazitätsblöcke verwenden, um `p6-b300`,`p6-b200`,`p5`,`p5e`,`p5en`, `p4d` `p4detrn1`, und `trn2` Instanzen zu reservieren. Sie können die folgenden UltraServer Typen über Capacity Blocks erwerben: `P6e-GB200` und `Trn2` (in der Vorschauversion).

Um einen Kapazitätsblock zu reservieren, geben Sie zunächst Ihren Kapazitätsbedarf an, einschließlich des Instance-Typs oder UltraServer -Typs, der Anzahl der Instances oder der

Zeitspanne UltraServers, des frühesten Startdatums und des spätesten Enddatums, die Sie benötigen. Anschließend wird Ihnen ein verfügbares Kapazitätsblock-Angebot angezeigt, das Ihren Spezifikationen entspricht. Das Angebot für den Kapazitätsblock enthält Details wie Startzeit, Availability Zone und Reservierungspreis. Der Angebotspreis eines Kapazitätsblocks hängt vom verfügbaren Angebot und der Nachfrage zum Zeitpunkt der Bereitstellung des Angebots ab. Nach der Reservierung eines Kapazitätsblocks ändert sich der Preis nicht. Weitere Informationen finden Sie unter Preise und Fakturierung für Kapazitätsblöcke.

Wenn Sie ein Angebot für ein Kapazitätsblock erwerben, wird Ihre Reservierung für das von Ihnen ausgewählte Datum und die Anzahl der Instances erstellt. Wenn Ihre Kapazitätsblock-Reservierung beginnt, können Sie Instances gezielt starten, indem Sie die Reservierungs-ID in Ihren Startanfragen angeben.

Sie können alle Instances, die Sie reserviert haben, bis 30 Minuten (für Instance-Typen) oder 60 Minuten (für UltraServer Typ) vor der Endzeit des Kapazitätsblocks verwenden. Wenn noch 30 Minuten (für Instance-Typen) oder 60 Minuten (für UltraServer Typen) in Ihrer Kapazitätsblock-Reservierung übrig sind, beginnen wir damit, alle Instances zu beenden, die im Capacity-Block ausgeführt werden. Wir nutzen diese Zeit zur Bereinigung Ihrer Instances, bevor wir den Kapazitätsblock dem nächsten Kunden bereitstellen. Bis zu EventBridge 10 Minuten vor Beginn des Kündigungsvorgangs senden wir ein Ereignis aus. Weitere Informationen finden Sie unter Überwachen Sie Kapazitätsblöcke mit EventBridge.

Themen

- Unterstützte Plattformen
- Überlegungen
- Zugehörige Ressourcen
- Preise und Fakturierung für Kapazitätsblöcke
- Voraussetzungen für Kapazitätsblöcke
- Suchen und Erwerben von Kapazitätsblöcken
- Instances mit Kapazitätsblöcken starten
- Anzeigen von Kapazitätsblöcken
- Kapazitätsblöcke erweitern
- Erstellen Sie eine Ressourcengruppe für UltraServer Capacity Blocks
- Überwachen Sie Kapazitätsblöcke mit EventBridge
- Kapazität protokollieren Blockiert API-Aufrufe mit AWS CloudTrail

Unterstützte Plattformen

Capacity Blocks für ML unterstützen derzeit nur Instances und nur UltraServers mit Standard-Tenancy. Wenn Sie den AWS-Managementkonsole zum Kauf eines Kapazitätsblocks verwenden, ist die Standardplattformoption Linux/UNIX. Wenn Sie das AWS Command Line Interface (AWS CLI) oder AWS SDK zum Kauf eines Capacity-Blocks verwenden, sind die folgenden Plattformoptionen verfügbar:

- Linux/Unix
- Red Hat Enterprise Linux
- RHEL mit HA
- SUSE Linux
- Ubuntu Pro

Überlegungen

Berücksichtigen Sie vor der Verwendung von Kapazitätsblöcken die folgenden Details und Einschränkungen.

- Wenn wir eine Beeinträchtigung feststellen, die sich auf einen UltraServer Kapazitätsblock auswirkt, werden wir Sie benachrichtigen, aber im Allgemeinen werden wir keine Maßnahmen ergreifen, um Ihre Instances auf dem Kapazitätsblock zu beenden. Dies dient dazu, unbeabsichtigte Unterbrechungen Ihrer Workloads zu minimieren. Nach Erhalt dieser Benachrichtigung können Sie den UltraServer Kapazitätsblock unverändert weiter verwenden oder eine Behebung beantragen, indem Sie alle Instances auf dem Kapazitätsblock beenden und eine AWS Support-Anfrage einreichen. Nachdem wir Ihre Support-Anfrage erhalten haben, werden wir Sie benachrichtigen, sobald wir die Behebung abgeschlossen haben und Sie Instances auf Ihrem Capacity Block neu starten können. UltraServer
- Bei `P6e-GB200` UltraServer Kapazitätsblöcken müssen Sie Ihre Instances mindestens 60 Minuten vor dem Ende des Kapazitätsblocks beenden.
- Um `P6e-GB200` UltraServer Capacity Blocks verwenden zu können, müssen Sie für die lokale Zone von Dallas (Nord-Virginia) angemeldet sein.
- Jeder Kapazitätsblock kann bis zu 64 Instances haben, und Sie können bis zu 256 Instances in mehreren Kapazitätsblöcken haben.
- Sie können Kapazitätsblockangebote beschreiben, die bereits in 30 Minuten beginnen können.
- Kapazitätsblöcke beginnen und enden um 11:30 Uhr koordinierte Weltzeit (UTC).

- Der Beendigungsprozess für Instances, die in einem Kapazitätsblock ausgeführt werden, beginnt um 11:00 Uhr koordinierter Weltzeit (UTC) am letzten Tag der Reservierung.
- Kapazitätsblöcke können mit einer Startzeit bis zu 8 Wochen in der Zukunft reserviert werden.
- Stornierungen von Kapazitätsblöcken sind nicht zulässig.
- Ein Kapazitätsblock kann nicht verschoben oder aufgeteilt werden.
- Kapazitätsblöcke können nicht zwischen AWS Konten oder innerhalb Ihrer AWS Organisation gemeinsam genutzt werden.
- Nur UltraServer Kapazitätsblöcke können mit Ressourcengruppen verwendet werden. Instance-Kapazitätsblöcke können nicht mit Ressourcengruppen verwendet werden. Weitere Informationen finden Sie unter Erstellen Sie eine Ressourcengruppe für UltraServer Capacity Blocks.
- Die Gesamtzahl der Instanzen, die in Kapazitätsblöcken für alle Konten in Ihrer AWS Organisation reserviert werden können, darf an einem bestimmten Datum 256 Instanzen nicht überschreiten.
- Um einen Kapazitätsblock zu verwenden, müssen Instances gezielt die Reservierungs-ID verwenden.
- Instances in einem Kapazitätsblock werden nicht auf Ihre On-Demand-Instances angerechnet.
- Stellen Sie für P5-Instances, die ein benutzerdefiniertes AMI verwenden, sicher, dass Sie über die erforderliche Software und Konfiguration für EFA verfügen.
- Informationen zu verwalteten Amazon EKS-Knotengruppen finden Sie unter Erstellen einer verwalteten Knotengruppe mit Amazon EC2 Capacity Blocks for ML. Informationen zu selbstverwalteten Amazon-EKS-Knotengruppen finden Sie unter Verwenden von Kapazitätsblöcken für ML mit selbstverwalteten Knoten.

Zugehörige Ressourcen

Nachdem Sie einen Kapazitätsblock erstellt haben, können Sie mit dem Kapazitätsblock Folgendes tun:

- Starten Sie Instances im Kapazitätsblock. Weitere Informationen finden Sie unter Instances mit Kapazitätsblöcken starten.
- Erstellen Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe. Weitere Informationen finden Sie unter Verwenden von Kapazitätsblöcken für Machine-Learning-Workloads im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

> **Note**
>
> Wenn Sie Amazon EC2 Auto Scaling oder Amazon EKS verwenden, können Sie die Skalierung so planen, dass sie zu Beginn der Kapazitätsblockreservierung ausgeführt wird. Bei der geplanten Skalierung werden Wiederholungsversuche AWS automatisch für Sie erledigt, sodass Sie sich keine Gedanken über die Implementierung der Wiederholungslogik für vorübergehende Ausfälle machen müssen.

- Verbessern Sie ML-Workflows mit. AWS ParallelCluster Weitere Informationen finden Sie unter Verbesserung von ML-Workflows mit AWS ParallelCluster und Amazon EC2 Capacity Blocks for ML.

Weitere Informationen zu AWS ParallelCluster finden Sie unter Was ist AWS ParallelCluster.

Preise und Fakturierung für Kapazitätsblöcke

Mit Amazon EC2 Capacity Blocks for ML zahlen Sie nur für das, was Sie reservieren. Der Preis eines Kapazitätsblocks hängt vom verfügbaren Angebot und der verfügbaren Nachfrage für Kapazitätsblöcke zum Zeitpunkt des Kaufs ab. Sie können den Preis eines Kapazitätsblockangebots anzeigen, bevor Sie es reservieren. Der Preis für den Kapazitätsblocks wird zum Zeitpunkt der Reservierung im Voraus berechnet. Wenn Sie über einen Zeitraum hinweg nach einem Kapazitätsblock suchen, erhalten Sie von uns das günstigste verfügbare Kapazitätsblockangebot. Nachdem Sie einen Kapazitätsblock reserviert haben, ändert sich der Preis nicht.

Wenn Sie einen Kapazitätsblock verwenden, zahlen Sie für das Betriebssystem, das Sie nutzen, wenn Ihre Instances ausgeführt werden. Weitere Informationen zu den Preisen für Betriebssysteme finden Sie unter Amazon EC2 Capacity Blocks for ML Pricing.

Fakturierung

Der Preis für das Angebot eines Kapazitätsblocks wird im Voraus berechnet. Die Zahlung wird innerhalb von 5 Minuten bis 12 Stunden nach dem Kauf eines Kapazitätsblocks über Ihr AWS -Konto abgerechnet. Während Ihre Zahlung bearbeitet wird, verbleibt die Ressource für Ihre Kapazitätsblock-Reservierung im Status `payment-pending`. Wenn Ihre Zahlung nicht mindestens 5 Minuten vor der Startzeit Ihres Blocks oder innerhalb von 12 Stunden (je nachdem, was zuerst eintritt) bearbeitet werden kann, wird Ihr Kapazitätsblock freigegeben und der Reservierungsstatus ändert sich zu `payment-failed`.

Nachdem Ihre Zahlung erfolgreich verarbeitet wurde, ändert sich der Status der Kapazitätsblock-Ressource von `payment-pending` in `scheduled`. Sie erhalten eine Rechnung mit der einmaligen Vorauszahlung. Auf der Rechnung können Sie den gezahlten Betrag der Kapazitätsblock-Reservierungs-ID zuordnen.

Wenn Ihre Kapazitätsblock-Reservierung beginnt, erfolgt die Abrechnung nur auf Grundlage des Betriebssystems, das Sie verwenden, während Ihre Instances in der Reservierung ausgeführt werden. Sie können Ihre Nutzung und die damit verbundenen Gebühren in Ihrer Jubiläumsrechnung für den Nutzungsmonat in Ihrem AWS Cost and Usage Report anzeigen.

> **Note**
>
> Savings Plans und Rabatte für Reserved Instances gelten nicht für Kapazitätsblöcke.

Anzeigen Ihrer Rechnung

Sie können Ihre Rechnung in der AWS Fakturierung und Kostenmanagement Konsole einsehen. Die Vorauszahlung für Ihren Kapazitätsblock erfolgt in dem Monat, in dem Sie die Reservierung erworben haben.

Nachdem Ihre Reservierung begonnen hat, werden auf Ihrer Rechnung separate Zeilen für die genutzte und ungenutzte Zeit der Blockreservierung angezeigt. Anhand dieser Einzelposten können Sie sehen, wie viel Zeit für Ihre Reservierung aufgewendet wurde. Wenn Sie ein Premium-Betriebssystem nutzen, wird Ihnen in der Zeile für die genutzte Zeit nur eine Nutzungsgebühr angezeigt. Weitere Informationen finden Sie unter Preise und Fakturierung für Kapazitätsblöcke. Für nicht genutzte Zeit fallen keine zusätzlichen Gebühren an.

Weitere Informationen finden Sie unter Anzeigen Ihrer Rechnung im AWS Fakturierung und Kostenmanagement -Benutzerhandbuch.

Wenn Ihr Kapazitätsblock in einem anderen Monat beginnt als dem, in dem Sie Ihre Reservierung erworben haben, werden der Vorabpreis und die Reservierungsnutzung in separaten Abrechnungsmonaten angezeigt. In Ihrem AWS Cost and Usage Report ist die Reservierungs-ID für den Kapazitätsblock in der Reservation/ReservationARN-Position Ihrer Vorausgebühr und unter LineItem/ResourceID in Ihrer Jubiläumsrechnung aufgeführt, sodass Sie die Nutzung dem entsprechenden Vorabpreis zuordnen können.

Voraussetzungen für Kapazitätsblöcke

Sie müssen Instances in einer AWS-Region starten, die den Instance-Typ unterstützt, den Sie verwenden möchten.

Kapazitätsblöcke mit **`p6-b300.48xlarge`**Instances sind im Folgenden verfügbar AWS-Regionen.

Regionscode	Name der Region
us-west-2	USA West (Oregon)

Kapazitätsblöcke mit **`p6-b200.48xlarge`**Instanzen sind im Folgenden verfügbar AWS-Regionen.

Regionscode	Name der Region
us-east-1	USA Ost (Nord-Virginia)
us-east-2	USA Ost (Ohio)
us-west-2	USA West (Oregon)

Kapazitätsblöcke mit **`p5.4xlarge`**Instanzen sind im Folgenden verfügbar AWS-Regionen.

Regionscode	Name der Region
us-east-1	USA Ost (Nord-Virginia)
us-east-2	USA Ost (Ohio)
us-west-2	USA West (Oregon)
eu-west-2	Europa (London)
ap-south-1	Asien-Pazifik (Mumbai)
ap-northeast-1	Asien-Pazifik (Tokio)
ap-southeast-2	Asien-Pazifik (Sydney)

Regionscode	Name der Region
sa-east-1	Südamerika (São Paulo)

Kapazitätsblöcke mit **`p5.48xlarge`**-Instances sind im Folgenden AWS-Regionen verfügbar.

Regionscode	Name der Region
us-east-1	USA Ost (Nord-Virginia)
us-east-2	USA Ost (Ohio)
us-west-1	USA West (Nordkalifornien)
us-west-2	USA West (Oregon)
eu-north-1	Europa (Stockholm)
eu-west-2	Europa (London)
sa-east-1	Südamerika (São Paulo)
ap-northeast-1	Asien-Pazifik (Tokio)
ap-south-1	Asien-Pazifik (Mumbai)
ap-southeast-2	Asien-Pazifik (Sydney)
ap-southeast-3	Asien-Pazifik (Jakarta)

Kapazitätsblöcke mit **`p5e.48xlarge`**-Instances sind im Folgenden AWS-Regionen verfügbar.

Regionscode	Name der Region
us-east-1	USA Ost (Nord-Virginia)
us-east-2	USA Ost (Ohio)
us-west-1	USA West (Nordkalifornien)

Regionscode	Name der Region
us-west-2	USA West (Oregon)
eu-north-1	Europa (Stockholm)
eu-west-2	Europa (London)
sa-east-1	Südamerika (São Paulo)
ap-northeast-1	Asien-Pazifik (Tokio)
ap-south-1	Asien-Pazifik (Mumbai)
ap-southeast-2	Asien-Pazifik (Sydney)
ap-southeast-3	Asien-Pazifik (Jakarta)

Kapazitätsblöcke mit **`p5en.48xlarge`**-Instances sind im Folgenden AWS-Regionen verfügbar.

Regionscode	Name der Region
us-east-1	USA Ost (Nord-Virginia)
us-east-2	USA Ost (Ohio)
us-west-1	USA West (Nordkalifornien)
us-west-2	USA West (Oregon)
eu-north-1	Europa (Stockholm)
eu-west-2	Europa (London)
eu-south-2	Europa (Spain)
sa-east-1	Südamerika (São Paulo)
ap-northeast-1	Asien-Pazifik (Tokio)

Regionscode	Name der Region
ap-northeast-2	Asien-Pazifik (Seoul)
ap-south-1	Asien-Pazifik (Mumbai)
ap-southeast-3	Asien-Pazifik (Jakarta)

Kapazitätsblöcke mit **`p4d.24xlarge`**-Instances sind im Folgenden AWS-Regionen verfügbar.

Regionscode	Name der Region
us-east-1	USA Ost (Nord-Virginia)
us-east-2	USA Ost (Ohio)
us-west-2	USA West (Oregon)

Kapazitätsblöcke mit **`p4de.24xlarge`**-Instances sind im Folgenden AWS-Regionen verfügbar.

Regionscode	Name der Region
us-east-1	USA Ost (Nord-Virginia)
us-west-2	USA West (Oregon)

Kapazitätsblöcke mit **`trn1.32xlarge`**-Instances sind im Folgenden AWS-Regionen verfügbar.

Regionscode	Name der Region
us-east-1	USA Ost (Nord-Virginia)
us-east-2	USA Ost (Ohio)
us-west-1	USA West (Nordkalifornien)
us-west-2	USA West (Oregon)

Regionscode	Name der Region
eu-north-1	Europa (Stockholm)
ap-south-1	Asien-Pazifik (Mumbai)
ap-southeast-2	Asien-Pazifik (Sydney)
ap-southeast-4	Asien-Pazifik (Melbourne)

Kapazitätsblöcke mit **`Trn2.3xlarge`**-Instances sind im Folgenden AWS-Region verfügbar.

Regionscode	Name der Region
ap-southeast-4	Asien-Pazifik (Melbourne)
sa-east-1	Südamerika (São Paulo)

Kapazitätsblöcke mit **`trn2.48xlarge`**-Instances sind im Folgenden AWS-Region verfügbar.

Regionscode	Name der Region
us-east-2	USA Ost (Ohio)

EC2 UltraServers Amazon-Kapazitätsblöcke

Kapazitätsblöcke mit **`Trn2`** UltraServers sind in der Vorschauversion wie folgt verfügbar AWS-Region.

Regionscode	Name der Region
us-east-2	USA Ost (Ohio)

Kapazitätsblöcke mit **`P6e-GB200`** UltraServers sind in der folgenden AWS lokalen Zone verfügbar.

Regionscode	Name der Region
us-east-1-dfw-2a	Dallas Local Zone (Nord-Virginia)

> **Note**
>
> Kapazitätsblockgrößen von 64 Instances werden nicht für alle Instance-Typen in allen AWS-Regionen unterstützt.

Suchen und Erwerben von Kapazitätsblöcken

Um einen Kapazitätsblock zu reservieren, müssen Sie zunächst einen Zeitblock finden, in dem Kapazität verfügbar ist, der Ihren Anforderungen entspricht. Um nach einen Kapazitätsblock zu finden, der reserviert werden kann, geben Sie Folgendes an.

- Die Anzahl der von Ihnen benötigten Instances
- Die Zeitdauer, für die Sie die Instances benötigen
- Der Zeitraum, in dem Sie Ihre Reservierung benötigen

Um nach einem verfügbaren Kapazitätsblock-Angebot zu suchen, geben Sie eine Reservierungsdauer und die Anzahl der Instances an. Sie müssen die Reservierungsdauer in 1-Tages-Schritte bis zu 14 Tagen und 7-Tages-Schritte bis zu 182 Tagen angeben. Jeder Kapazitätsblock kann bis zu 64 Instances haben, und Sie können bis zu 256 Instances in mehreren Kapazitätsblöcken haben.

Wenn Sie einen Kapazitätsblock anfordern, der Ihren Spezifikationen entspricht, geben wir die Details von bis zu 3 verfügbaren Blöcken an. Alle Kapazitätsblöcke enden um 11:30 Uhr UTC, sodass die Blöcke, die am selben Tag beginnen, eine Dauer haben, die Ihrer gewünschten Dauer am nächsten kommt. Ein Block hat eine Dauer, die etwas unter Ihrer gewünschten Dauer liegt, während der andere eine etwas längere Dauer als Ihre gewünschte Dauer hat.

Zu den Angebotsdetails gehören die Startzeit der Reservierung, die Availability Zone für die Reservierung und der Preis der Reservierung. Weitere Informationen finden Sie unter Preise und Fakturierung für Kapazitätsblöcke.

Sie können das angezeigte Kapazitätsblock-Angebot erwerben oder Ihre Suchkriterien ändern, um andere verfügbaren Optionen anzuzeigen. Es gibt keine vordefinierte Verfallszeit für das Angebot, die Angebote sind jedoch nur nach dem Prinzip „Wer zuerst kommt, wird zuerst bedient“ verfügbar.

Wenn Sie ein Kapazitätsblock-Angebot erwerben, erhalten Sie sofort eine Antwort, die bestätigt, dass Ihr Kapazitätsblock reserviert wurde. Nach der Bestätigung wird in Ihrem Konto eine neue Kapazitätsreservierung mit dem Reservierungstyp `capacity-block` und einem `start-date` angezeigt, das auf die Startzeit des von Ihnen erworbenen Angebots festgelegt ist. Ihre Kapazitätsblock-Reservierung wurde mit dem Status `payment-pending` erstellt. Nachdem die Vorauszahlung erfolgreich verarbeitet wurde, ändert sich der Reservierungsstatus in `scheduled`. Weitere Informationen finden Sie unter Fakturierung.

> **Note**
>
> Um `P6e-GB200` UltraServer Capacity Blocks verwenden zu können, müssen Sie für die lokale Zone Dallas (Nord-Virginia) angemeldet sein.

Console

So suchen und erwerben Sie einen Kapazitätsblock

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Navigationsleiste oben auf dem Bildschirm eine AWS-Region aus. Die Wahl ist wichtig, weil Kapazitätsblockgrößen von 64 Instances nicht für alle Instance-Typen in allen Regionen unterstützt werden.
3. Wählen Sie im Navigationsbereich Kapazitätsreservierungen und dann Kapazitätsblöcke erstellen aus.
4. Wählen Sie unter Kapazitätsblocktypen entweder Instances oder aus UltraServers.
5. Unter Kapazitätsattributen können Sie Ihre Kapazitätsblock-Suchparameter definieren. Standardmäßig ist die Plattform Linux. Wenn Sie ein anderes Betriebssystem auswählen möchten, verwenden Sie die AWS CLI. Weitere Informationen finden Sie unter Unterstützte Plattformen.
6. Geben Sie unter Gesamtkapazität (für Instances) oder UltraServer Anzahl (für UltraServers) die Anzahl der Instances an, die UltraServers Sie reservieren möchten.
7. Geben Sie unter Dauer die Anzahl der Tage oder Wochen ein, für die Sie die Reservierung benötigen.

8. Geben Sie unter Zeitraum für die Suche nach Kapazitätsblöcken das früheste Datum ein, an dem Ihre Reservierung beginnen soll.
9. Wählen Sie Kapazitätsblöcke suchen.
10. Wenn ein Kapazitätsblock verfügbar ist, der Ihren Spezifikationen entspricht, wird unter Empfohlene Kapazitätsblöcke ein Angebot angezeigt. Wenn mehrere Angebote Ihren Spezifikationen entsprechen, wird das preisgünstigste verfügbare Kapazitätsblock-Angebot angezeigt. Um andere Kapazitätsblock-Angebote anzuzeigen, passen Sie Ihre Sucheingaben an und wählen Sie erneut Kapazitätsblöcke suchen.
11. Wenn Sie ein Kapazitätsblock-Angebot finden, das Sie erwerben möchten, wählen Sie Weiter.
12. (Optional) Wählen Sie auf der Seite Tags hinzufügen die Option Neues Tag hinzufügen aus.
13. Auf der Seite Überprüfen und Kaufen werden das Start- und Enddatum, die Dauer, die Gesamtzahl der Instances und der Preis aufgeführt.

> **Note**
>
> Kapazitätsblöcke können nach der Reservierung nicht mehr storniert werden.

14. Geben Sie im Popup-Fenster Einen Kapazitätsblock kaufen Bestätigen ein und wählen Sie dann Kaufen aus.

AWS CLI

So suchen Sie einen Kapazitätsblock für eine Instance

Verwenden Sie den Befehl describe-capacity-block-offerings.

Im folgenden Beispiel wird nach Instance-Kapazitätsblöcken gesucht.

```
aws ec2 describe-capacity-block-offerings \
--instance-type p5.48xlarge \
--instance-count 16 \
--start-date-range 2023-08-14T00:00:00Z \
--end-date-range 2023-10-22-T00:00:00Z \
--capacity-duration-hours 48
```

Im folgenden Beispiel werden UltraServer Kapazitätsblöcke gefunden.

```
aws ec2 describe-capacity-block-offerings \
--ultraserver-type u-p6e-gb200x72 \
--ultraserver-count 1 \
--start-date-range 2023-08-14T00:00:00Z \
--end-date-range 2023-10-22-T00:00:00Z \
--capacity-duration-hours 48
```

So erwerben Sie einen Kapazitätsblock

Verwenden Sie den purchase-capacity-blockBefehl mit der Angebots-ID des Capacity-Blocks aus der Ausgabe des vorherigen Beispiels.

```
aws ec2 purchase-capacity-block \
--capacity-block-offering-id cb-0123456789abcdefg \
--instance-platform Linux/UNIX
```

PowerShell

So suchen Sie Kapazitätsblöcke

Verwenden Sie das cmdlet Get-EC2CapacityBlockOffering.

Im folgenden Beispiel wird nach Instance-Kapazitätsblöcken gesucht.

```
Get-EC2CapacityBlockOffering `
-InstanceType p5.48xlarge `
-InstanceCount 16 `
-CapacityDurationHour 48 `
-StartDateRange 2023-08-14T00:00:00Z `
-EndDateRange 2023-10-22-T00:00:00Z
```

Im folgenden Beispiel werden UltraServer Capacity-Blöcke gesucht.

```
Get-EC2CapacityBlockOffering `
-UltraserverType u-p6e-gb200x72 `
-UltraserverCount  1 `
-CapacityDurationHour 48 `
-StartDateRange 2023-08-14T00:00:00Z `
-EndDateRange 2023-10-22-T00:00:00Z
```

So erwerben Sie einen Kapazitätsblock

Verwenden Sie das EC2 EC2 CapacityBlock Cmdlet New- mit der Angebots-ID des Capacity-Blocks aus der Ausgabe des vorherigen Beispiels.

```
New-EC2EC2CapacityBlock `
-CapacityBlockOfferingId cb-0123456789abcdefg `
-InstancePlatform Linux/UNIX
```

Instances mit Kapazitätsblöcken starten

Um Ihren Kapazitätsblock zu verwenden, müssen Sie beim Starten von Instances die Kapazitätsblock-Reservierungs-ID angeben. Das Starten einer Instance in einem Kapazitätsblock verringert die verfügbare Kapazität um die Anzahl der gestarteten Instances. Wenn Ihre erworbene Instance-Kapazität beispielsweise acht Instances beträgt und Sie vier Instances starten, verringert sich die verfügbare Kapazität um vier.

Wenn Sie eine im Kapazitätsblock ausgeführte Instance beenden, bevor die Reservierung endet, können Sie an ihrer Stelle eine neue Instance starten. Wenn Sie eine Instance in einem Kapazitätsblock anhalten oder beenden, dauert die Bereinigung Ihrer Instance mehrere Minuten, bevor Sie eine andere Instance starten können, um sie zu ersetzen. Während dieser Zeit befindet sich Ihre Instance im Anhalte- oder `shutting-down`-Status. Nachdem dieser Vorgang abgeschlossen ist, ändert sich Ihr Instance-Status in `stopped` oder `terminated`. Anschließend wird die verfügbare Kapazität in Ihrem Kapazitätsblock aktualisiert, um eine weitere zur Verwendung verfügbare Instance anzuzeigen.

Voraussetzungen

- Ihre Instance kann nicht in einem Subnetz in einer anderen Availability Zone als der Availability Zone gestartet werden, in der sich Ihr Kapazitätsblock befindet.
- Ihre Instance kann nicht mit einem AMI gestartet werden, das eine andere Plattform als die Plattform Ihres Kapazitätsblocks verwendet.
- Um `P6e-GB200` UltraServer Capacity Blocks verwenden zu können, müssen Sie für die lokale Zone Dallas (Nord-Virginia) angemeldet sein.

Console

So starten Sie Instances in einem Kapazitätsblock

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie in der Navigationsleiste am oberen Bildschirmrand die Region für Ihre Kapazitätsblock-Reservierung aus.
3. Wählen Sie im Dashboard der EC2 Amazon-Konsole die Option Launch instance aus.
4. Befolgen Sie das Verfahren zum Starten einer Instance.
5. Erweitern Sie Erweiterte Details und wählen Sie für Kaufoption die Option Kapazitätsblöcke aus. Führen Sie dann einen der folgenden Schritte aus:

   - Um die Instances in einem bestimmten Kapazitätsblock zu starten, wählen Sie für Kapazitätsreservierung die Option Kapazitätsreservierung angeben und dann den Kapazitätsblock aus.
   - (UltraServers nur) Um die Instances in einer UltraServer Capacity Block-Ressourcengruppe zu starten, wählen Sie für Capacity Reservation Resource Group Specify Capacity Reservation und wählen Sie dann die Ressourcengruppe aus.
6. Wählen Sie Launch Instance (Instance starten) aus.

AWS CLI

So starten Sie Instances in einem Kapazitätsblock

Verwenden den Befehl run-instances mit der Option `instance-market-options MarketType`.

Das folgende Beispiel startet eine Instance in einen bestimmten Kapazitätsblock.

```
aws ec2 run-instances \
--image-id ami-0abcdef1234567890 \
--count 1 \
--instance-type p5.48xlarge \
--key-name my-key-pair \
--subnet-id subnet-0abcdef1234567890 \
--instance-market-options MarketType='capacity-block' \
--capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=capacity_block_id}
```

Im folgenden Beispiel wird eine Instance in einer UltraServer Capacity Block-Ressourcengruppe gestartet.

```
aws ec2 run-instances \
```

```
--image-id ami-0abcdef1234567890 \
--count 1 \
--instance-type p6e-gb200.36xlarge \
--key-name my-key-pair \
--subnet-id subnet-0abcdef1234567890 \
--instance-market-options MarketType='capacity-block' \
--capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationResourceGroupArn=resource_group_arn}
```

PowerShell

So starten Sie Instances in einem Kapazitätsblock

Verwenden Sie das New-EC2InstanceCmdlet mit der wie `-InstanceMarketOption` folgt definierten Option.

```
$marketoption = New-Object Amazon.EC2.Model.InstanceMarketOptionsRequest
$marketoption.MarketType = "capacity-block"
```

Das folgende Beispiel startet eine Instance in einen bestimmten Kapazitätsblock.

```
New-EC2Instance `
-ImageId ami-0abcdef1234567890 `
-InstanceType p5.48xlarge `
-KeyName "my-key-pair" `
-SubnetId subnet-0abcdef1234567890 `
-InstanceMarketOptions $marketoption `
-CapacityReservationTarget_CapacityReservationId capacity_block_id
```

Im folgenden Beispiel wird eine Instance in einer UltraServer Capacity Block-Ressourcengruppe gestartet.

```
New-EC2Instance `
-ImageId ami-0abcdef1234567890 `
-InstanceType p6e-gb200.36xlarge `
-KeyName "my-key-pair" `
-SubnetId subnet-0abcdef1234567890 `
-InstanceMarketOptions $marketoption `
-CapacityReservationTarget_CapacityReservationResourceGroupArn "resource_group_arn"
```

Zugehörige Ressourcen

- Informationen zum Erstellen einer Startvorlage, die auf einen Kapazitätsblock abzielt, finden Sie unter the section called “Startvorlagen”.
- Informationen zum Starten von Instances in einem Capacity-Block mithilfe von EC2 Fleet finden Sie unterTutorial: Ihre EC2-Flotte konfigurieren, um Instances in Kapazitätsblöcken zu starten.
- Informationen zum Einrichten einer verwalteten EKS-Knotengruppe mit einem Kapazitätsblock finden Sie unter Eine verwaltete Knotengruppe mit Kapazitätsblöcken für ML erstellen im Benutzerhandbuch für Amazon EKS.
- Informationen zur Einrichtung AWS ParallelCluster mithilfe eines Capacity-Blocks finden Sie unter ML on AWS ParallelCluster.

Anzeigen von Kapazitätsblöcken

Nachdem Sie einen Kapazitätsblock reserviert haben, können Sie die Kapazitätsblock-Reservierung in Ihrem AWS -Konto anzeigen. Sie können das `start-date` und `end-date` anzeigen, um zu sehen, wann Ihre Reservierung beginnt und endet. Vor Beginn einer Kapazitätsblock-Reservierung wird die verfügbare Kapazität als Null angezeigt. Wie viele Instances in Ihrem Kapazitätsblock verfügbar sein werden, können Sie anhand des Tag-Werts für den Tag-Schlüssel `aws:ec2capacityreservation:incrementalRequestedQuantity` anzeigen.

Wenn eine Kapazitätsblock-Reservierung beginnt, ändert sich der Reservierungsstatus von `scheduled` zu `active`. Wir senden ein Ereignis über Amazon EventBridge, um Sie darüber zu informieren, dass der Capacity Block zur Verwendung verfügbar ist. Weitere Informationen finden Sie unter Überwachen Sie Kapazitätsblöcke mit EventBridge.

Kapazitätsblöcke weisen die folgenden Status auf:

- `payment-pending` – Die Vorauszahlung wurde noch nicht verarbeitet.
- `payment-failed` – Die Zahlung konnte nicht innerhalb des 12-Stunden-Zeitraums verarbeitet werden. Ihr Kapazitätsblock wurde veröffentlicht.
- `scheduled` – Die Zahlung wurde verarbeitet und die Kapazitätsblock-Reservierung hat noch nicht begonnen.
- `active` – Die reservierte Kapazität steht Ihnen zur Nutzung zur Verfügung.
- `expired` – Die Kapazitätsblock-Reservierung ist automatisch zu dem in Ihrer Reservierungsanfrage angegebenen Datum und der angegebenen Uhrzeit abgelaufen. Die reservierte Kapazität ist nicht mehr für Ihre Nutzung verfügbar.

Console

So zeigen Sie Kapazitätsblöcke an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Kapazitätsreservierungen aus.
3. Auf der Übersichtsseite für Kapazitätsreservierungen sehen Sie eine Ressourcentabelle mit Details zu allen Ihren Ressourcen für Kapazitätsreservierungen. Um nach Ihren Kapazitätsblock-Reservierungen zu suchen, wählen Sie Kapazitätsblöcke aus der Dropdown-Liste über der Kapazitätsreservierungs-ID aus. In der Tabelle können Sie Informationen zu Ihren Kapazitätsblöcken anzeigen, z. B. Start- und Enddatum, Dauer und Status.
4. Für weitere Details zu einem Kapazitätsblock wählen Sie die Reservierungs-ID für den Kapazitätsblock aus, den Sie anzeigen möchten. Auf der Seite mit den Details zur Kapazitätsreservierung werden alle Eigenschaften der Reservierung sowie die Anzahl der genutzten und im Kapazitätsblock verfügbaren Instances angezeigt.

> **Note**
>
> Vor Beginn einer Kapazitätsblock-Reservierung wird die verfügbare Kapazität als Null angezeigt. Die Anzahl der verfügbaren Instances bei Beginn der Kapazitätsblockreservierung kann mithilfe des folgenden Tag-Werts für den Tag-Schlüssel ermittelt werden: `aws:ec2capacityreservation:incrementalRequestedQuantity`.

AWS CLI

So zeigen Sie Kapazitätsblöcke an

Wenn Sie den describe-capacity-reservationsBefehl verwenden, werden standardmäßig sowohl On-Demand-Kapazitätsreservierungen als auch Kapazitätsblockreservierungen aufgelistet. Um nur Ihre Kapazitätsblock-Reservierungen anzuzeigen, filtern Sie nach Reservierungen des Typs `capacity-block`.

```
aws ec2 describe-capacity-reservations \
    --filters Name=reservation-type,Values=capacity-block
```

PowerShell

So zeigen Sie Kapazitätsblöcke an

Verwenden Sie das cmdlet Get-EC2CapacityReservation. Standardmäßig werden sowohl On-Demand-Kapazitätsreservierungen als auch Kapazitätsblock-Reservierungen aufgelistet. Um nur Ihre Kapazitätsblock-Reservierungen anzuzeigen, filtern Sie nach Reservierungen des Typs `capacity-block`.

```
Get-EC2CapacityReservation `
    -Filter @{Name="reservation-type"; Values="capacity-block"}
```

Kapazitätsblöcke erweitern

Mit Kapazitätsblöcken reservieren Sie Datenverarbeitungskapazität für Ihre Workloads und sorgen so für Verfügbarkeit und Konsistenz. Um Ihren sich ändernden Anforderungen gerecht zu werden, können Sie die Dauer Ihrer vorhandenen Kapazitätsblöcke nach Bedarf verlängern.

Um einen Kapazitätsblock zu verlängern, muss er den Status `active` oder `scheduled` haben und darf keine Erweiterungen haben, die `payment-pending` sind. Sie können beantragen, dass die Dauer Ihres Kapazitätsblocks auf mindestens 1 Stunde oder maximal 56 Tage verlängert wird, bevor er abläuft. Sie können Ihren Kapazitätsblock in Schritten von einem Tag bis zu 14 Tagen und in Schritten von 7 Tagen auf insgesamt bis zu 182 Tage (26 Wochen) verlängern. Wenn Sie Ihren Kapazitätsblock verlängern, wird dessen Enddatum aktualisiert, sodass Ihre Instances weiterhin ohne Unterbrechung ausgeführt werden können.

- Die Anzahl der Erweiterungen, die Sie für einen Kapazitätsblock anwenden können, ist unbegrenzt
- Ihre Kapazitätsreservierungs-ID bleibt nach der Verlängerung des Blocks erhalten
- Kapazitätsblöcke können nur verlängert werden, wenn genügend Kapazität zur Verfügung steht, um sie zu unterstützen, was nicht garantiert werden kann.

Fakturierung

Der Preis für das Angebot eines Kapazitätsblocks wird im Voraus berechnet. Die Verlängerung bleibt in `payment-pending` bestehen, bis die Rechnung bezahlt ist. Wenn Ihre Zahlung nicht innerhalb von 12 Stunden oder bis zu 35 Minuten vor dem geplanten Ende des Kapazitätsblocks bearbeitet werden kann (je nachdem, was zuerst eintritt), ist Ihre Verlängerung nicht erfolgreich und der Status

ändert sich in `payment-failed`. Ihre Kapazitätsblock-Reservierung bleibt `active` und wird am ursprünglichen Enddatum beendet.

Nachdem Ihre Zahlung erfolgreich bearbeitet wurde, ändert sich der Status der Kapazitätsblock-Verlängerung auf `payment-succeeded` und das Enddatum der Kapazitätsblock-Reservierung wird auf das neue Enddatum aktualisiert. Die Details Ihrer Erweiterung können im Abschnitt mit den Details zur Capacity Block Extension der Konsole oder mithilfe des Befehls describe-capacity-block-extension-history eingesehen werden.

Ihren Kapazitätsblock erweitern

Console

So verlängern Sie einen Kapazitätsblock

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Kapazitätsreservierungen aus.
3. Auf der Seite Übersicht der Kapazitätsreservierungen sehen Sie eine Ressourcentabelle mit Details zu allen Ihren Ressourcen für Kapazitätsreservierungen. Wählen Sie die Reservierungs-ID für den Kapazitätsblock aus, den Sie erweitern möchten.
4. Wählen Sie im Dropdownmenü Aktionen die Option Kapazitätsblock erweitern aus.
5. Geben Sie unter Dauer die Anzahl der Tage oder Wochen ein, für die Sie die Reservierung verlängern möchten.
6. Wählen Sie Kapazitätsblöcke suchen.
7. Wenn ein Kapazitätsblock verfügbar ist, der Ihren Spezifikationen entspricht, wird unter Empfohlene Kapazitätsblöcke ein Angebot angezeigt. Um andere Kapazitätsblock-Angebote anzuzeigen, passen Sie Ihre Sucheingaben an und wählen Sie erneut Kapazitätsblöcke suchen.
8. Wenn Sie ein Kapazitätsblock-Angebot finden, das Sie erwerben möchten, wählen Sie Erweitern.
9. Geben Sie im Popup-Fenster Kapazitätsblock erweitern Bestätigen ein und wählen Sie dann Erweitern.

AWS CLI

So suchen Sie eine Kapazitätsblock-Verlängerung

Verwenden Sie den Befehl describe-capacity-block-extension-offering. Im folgenden Beispiel wird nach einer Verlängerung des Kapazitätsblocks für die angegebene Reservierung um 48 Stunden gesucht.

```
aws ec2 describe-capacity-block-extension-offerings \
    --capacity-reservation-id cr-1234567890abcdefg \
    --capacity-block-extension-duration-hours 48
```

So verlängern Sie einen Kapazitätsblock

Verwenden Sie den Befehl purchase-capacity-block-extension. Geben Sie die Angebots-ID der Verlängerung aus der Ausgabe des vorherigen Beispiels an.

```
aws ec2 purchase-capacity-block-extension \
    --capacity-block-extension-offering-id cbe-0123456789abcdefg \
    --capacity-reservation-id cr-1234567890abcdefg
```

PowerShell

So suchen Sie eine Kapazitätsblock-Verlängerung

Verwenden Sie das cmdlet Get-EC2CapacityBlockExtensionOffering. Im folgenden Beispiel wird nach einer Verlängerung des Kapazitätsblocks für die angegebene Reservierung um 48 Stunden gesucht.

```
Get-EC2CapacityBlockExtensionOffering `
    -CapacityReservationId cr-1234567890abcdefg `
    -CapacityBlockExtensionDurationHour 48
```

So verlängern Sie einen Kapazitätsblock

Verwenden Sie das cmdlet Invoke-EC2CapacityBlockExtension. Geben Sie die Angebots-ID der Verlängerung aus der Ausgabe des vorherigen Beispiels an.

```
Invoke-EC2CapacityBlockExtension `
    -CapacityBlockExtensionOfferingId cbe-0123456789abcdefg `
    -CapacityReservationId cr-1234567890abcdefg
```

Erstellen Sie eine Ressourcengruppe für UltraServer Capacity Blocks

Sie können sie verwenden AWS -Ressourcengruppen , um logische Sammlungen von UltraServer Kapazitätsblöcken zu erstellen. Nachdem Sie die Ressourcengruppe erstellt haben, können Sie Ihrem Konto UltraServer Kapazitätsblöcke hinzufügen, die Sie besitzen. Nachdem Sie die UltraServer Capacity-Blöcke hinzugefügt haben, können Sie Instance-Starts auf die Ressourcengruppe statt auf die einzelnen Capacity-Blöcke ausrichten. Instances, die auf eine Ressourcengruppe abzielen, stimmen mit allen UltraServer Capacity-Blöcken in der Gruppe überein, deren Attribute und verfügbare Kapazität übereinstimmen. Wenn die Ressourcengruppe keinen UltraServer Kapazitätsblock mit passenden Attributen und verfügbarer Kapazität hat, schlägt der Instance-Start fehl.

Wenn ein UltraServer Kapazitätsblock aus einer Ressourcengruppe entfernt wird, während dort Instances laufen, werden diese Instances weiterhin im Kapazitätsblock ausgeführt. Wenn ein UltraServer Kapazitätsblock in einer Gruppe endet, während Instances laufen, werden die Instances beendet.

Sie können einer Ressourcengruppe keine Instance-Kapazitätsblöcke hinzufügen.

Verwenden Sie eine der folgenden Methoden, um eine Ressourcengruppe für UltraServer Capacity Blocks zu erstellen.

AWS CLI

Um eine Ressourcengruppe für UltraServer Capacity Blocks zu erstellen

Verwenden Sie den AWS CLI -Befehl create-group und geben Sie für `--configuration` Folgendes an:

```
{
  "Configuration": [
    {
      "Type": "AWS::EC2::CapacityReservationPool",
      "Parameters": [
        {
          "Name": "instance-type",
          "Values": [
            "instance_type"
          ]
        },
        {
```

```
          "Name": "reservation-type",
          "Values": [
            "capacity-block"
          ]
        }
      ]
    },
    {
      "Type": "AWS::ResourceGroups::Generic",
      "Parameters": [
        {
          "Name": "allowed-resource-types",
          "Values": [
            "AWS::EC2::CapacityReservation"
          ]
        }
      ]
    }
  ]
}
```

PowerShell

Um eine Ressourcengruppe für UltraServer Kapazitätsblöcke zu erstellen

Verwenden Sie das RGGroup Cmdlet New-. Geben Sie für `-Configuration` Folgendes an:

```
{
  "Configuration": [
    {
      "Type": "AWS::EC2::CapacityReservationPool",
      "Parameters": [
        {
          "Name": "instance-type",
          "Values": [
            "instance_type"
          ]
        },
        {
          "Name": "reservation-type",
          "Values": [
            "capacity-block"
          ]
        }
```

```
      ]
    },
    {
      "Type": "AWS::ResourceGroups::Generic",
      "Parameters": [
        {
          "Name": "allowed-resource-types",
          "Values": [
            "AWS::EC2::CapacityReservation"
          ]
        }
      ]
    }
  ]
}
```

Nachdem Sie eine Ressourcengruppe für UltraServer Capacity Block erstellt haben, verwenden Sie eine der folgenden Methoden, um ihr vorhandene UltraServer Capacity-Blöcke hinzuzufügen.

AWS CLI

Um einer Ressourcengruppe einen UltraServer Kapazitätsblock hinzuzufügen

Verwenden Sie den Befehl group-resources. Geben Sie für `--group` den Namen der von Ihnen erstellten Ressourcengruppe an. Geben Sie für die UltraServer Kapazitätsblöcke ARNs an `--resource-arns`, die hinzugefügt werden sollen.

```
aws resource-groups group-resources \
--group MyCRGroup \
--resource-arns capacity_block_arn
```

PowerShell

Um einen UltraServer Kapazitätsblock zu einer Ressourcengruppe hinzuzufügen

Verwenden Sie das RGResource Cmdlet Add-. Geben Sie für `-Group` den Namen der von Ihnen erstellten Ressourcengruppe an. Geben Sie für die UltraServer Kapazitätsblöcke ARNs an `-ResourceArn` , die hinzugefügt werden sollen.

Mit dem folgenden Befehl werden beispielsweise zwei Kapazitätsreservierungen zur angegebenen Gruppe hinzugefügt.

```
Add-RGResource `
-Group MyCRGroup `
-ResourceArn capacity_block_arn
```

Überwachen Sie Kapazitätsblöcke mit EventBridge

Wenn Ihre Kapazitätsblock-Reservierung beginnt, EC2 sendet Amazon ein Ereignis, EventBridge das darauf hinweist, dass Ihre Kapazität einsatzbereit ist. Vierzig Minuten vor Ende Ihrer Kapazitätsblock-Reservierung erhalten Sie ein weiteres EventBridge Ereignis, das Sie darüber informiert, dass alle Instances, die im Rahmen der Reservierung laufen, in 10 Minuten beendet werden. Weitere Informationen zu EventBridge Veranstaltungen finden Sie unter Amazon EventBridge Events.

Die folgenden Ereignisstrukturen für von Kapazitätsblöcken ausgegebene Ereignisse:

Kapazitätsblock bereitgestellt

Das folgende Beispiel zeigt ein Ereignis für Kapazitätsblock bereitgestellt.

```
{
  "customer_event_id": "[Capacity Reservation Id]-delivered",
  "detail_type": "Capacity Block Reservation Delivered",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Warnung vor Ablauf des Kapazitätsblocks

Das folgende Beispiel zeigt ein Ereignis für die Warnung Kapazitätsblockablauf.

```
{
  "customer_event_id": "[Capacity Reservation Id]-approaching-expiry",
  "detail_type": "Capacity Block Reservation Expiration Warning",
  "source": "aws.ec2",
```

```
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Kapazität protokollieren Blockiert API-Aufrufe mit AWS CloudTrail

Capacity Blocks ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in Capacity Blocks ausgeführt wurden. CloudTrail erfasst API-Aufrufe für Capacity Blocks als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Kapazitätsblocks-Konsole und Cdeaufrufe der Kapazitätsblocks-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Kapazitätsblöcke. Auch wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail-Konsole in Event history (Ereignisverlauf) anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Capacity Blocks gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Kapazität: Blockiert Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn Aktivitäten in Kapazitätsblöcken auftreten, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem System AWS-Konto, einschließlich der Ereignisse für Kapazitätsblöcke, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS -Partition und stellt die Protokolldateien in dem von Ihnen angegebenen

Amazon-S3-Bucket bereit. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle Capacity Blocks-Aktionen werden von der Amazon EC2 API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert. Beispielsweise generieren Aufrufe von und `CapacityBlockActive` Aktionen Einträge in den CloudTrail Protokolldateien. `CapacityBlockScheduled`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlegendes zu den Protokolldateieinträgen für Kapazitätsblöcke

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis ist eine einzelne Anforderung aus einer beliebigen Quelle und enthält Informationen zur angeforderten Aktion, zu Datum und Uhrzeit der Aktion, zu den Anforderungsparametern usw. CloudTrail -Protokolldateien stellen kein geordnetes Stack-Trace der öffentlichen API-Aufrufe dar. Daher werden sie nicht in einer bestimmten Reihenfolge angezeigt.

Die folgenden Beispiele zeigen CloudTrail Protokolleinträge für:

- TerminateCapacityBlocksInstances

- CapacityBlockPaymentFailed
- CapacityBlockScheduled
- CapacityBlockActive
- CapacityBlockFailed
- CapacityBlockExpired

> **Note**
>
> Aus Datenschutzgründen wurden einige Felder aus den Beispielen geschwärzt.

TerminateCapacityBlocksInstances


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "TerminateCapacityBlockInstances",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
    }
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws:ec2:us-east-1:123456789012:instance/i-0598c7d356eba48d7"
    }
```

```
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      }
}
```

CapacityBlockPaymentFailed

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockPaymentFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "payment-failed"
      }
}
```

CapacityBlockScheduled


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockScheduled",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "scheduled"
      }
}
```


CapacityBlockActive


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
```

```
  "eventName": "CapacityBlockActive",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "active"
      }
 }
```


CapacityBlockFailed


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
```

```
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "failed"
      }
 }
```

CapacityBlockExpired

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockExpired",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "expired"
```

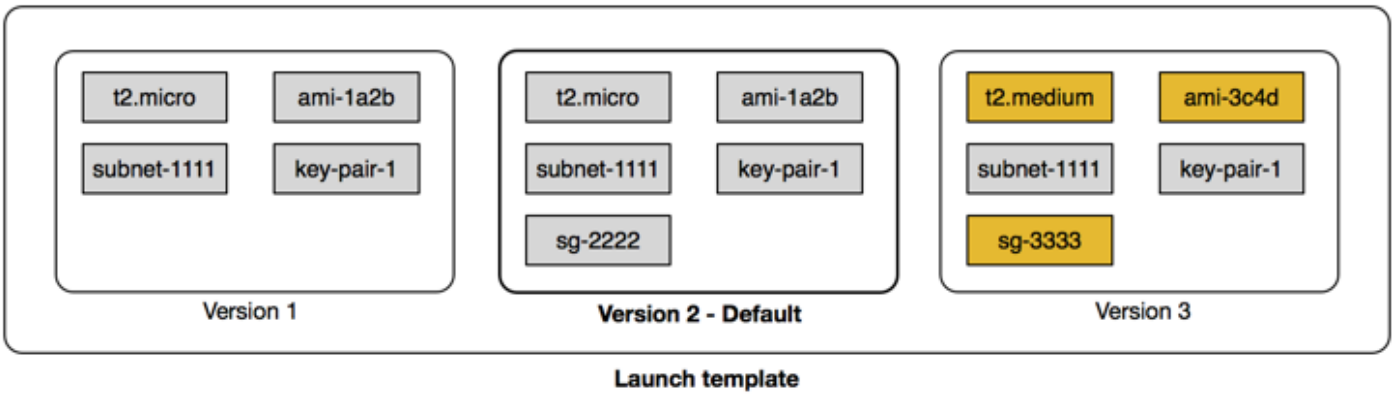
```
        }
}
```

Instance-Startparameter in EC2 Amazon-Startvorlagen speichern

Sie können eine EC2 Amazon-Startvorlage verwenden, um Instance-Startparameter zu speichern, sodass Sie sie nicht bei jedem Start einer EC2 Amazon-Instance angeben müssen. Sie können zum Beispiel eine Startvorlage erstellen, welche die AMI-ID, den Instance-Typ und die Netzwerkeinstellungen speichert, die Sie normalerweise zum Starten von Instances verwenden. Wenn Sie eine Instance mit der EC2 Amazon-Konsole, einem AWS SDK oder einem Befehlszeilentool starten, können Sie die Startvorlage angeben, anstatt die Parameter erneut einzugeben.

Sie können für jede Startvorlage eine oder mehrere nummerierte Startvorlagenversionen erstellen. Jede Version kann unterschiedliche Startparameter besitzen. Wenn Sie eine Instance von einer Startvorlage aus starten, können Sie eine beliebige Version der Startvorlage verwenden. Wenn Sie keine Version angeben, wird die Standardversion verwendet. Sie können eine beliebige Version der Startvorlage als Standardvorlage festlegen — standardmäßig ist dies die erste Version der Startvorlage.

Im folgenden Diagramm ist eine Startvorlage mit drei Versionen dargestellt. Die erste Version gibt den Instancetyp, die AMI-ID, das Subnetz und das Schlüsselpaar an, mit denen die Instance geladen werden soll. Die zweite Version basiert auf der ersten Version und gibt zudem eine Sicherheitsgruppe für die Instance an. Die dritte Version verwendet für einige der Parameter andere Werte. Version 2 wird als Standardversion festgelegt. Wenn über diese Startvorlage eine Instance gestartet werden würde, würden die Startparameter von Version 2 verwendet werden, sofern keine andere Version angegeben wurde.



Inhalt

- Einschränkungen für EC2 Amazon-Startvorlagen
- Für EC2 Amazon-Startvorlagen sind IAM-Berechtigungen erforderlich
- Verwenden Sie EC2 Amazon-Startvorlagen, um den Start von EC2 Amazon-Instances zu steuern
- Erstellen Sie eine EC2 Amazon-Startvorlage
- Ändern einer Startvorlage (Verwalten von Startvorlagenversionen)
- Eine Startvorlage oder Startvorlagenversion löschen

Einschränkungen für EC2 Amazon-Startvorlagen

Die folgenden Einschränkungen gelten für Startvorlagen und Startvorlagenversionen:

- Kontingente — Um die Kontingente für Ihre Startvorlagen und Startvorlagenversionen anzuzeigen, öffnen Sie die Service Quotas Quotas-Konsole oder verwenden Sie den list-service-quotas AWS CLI Befehl. Jedes AWS Konto kann bis zu 5.000 Startvorlagen pro Region und bis zu 10.000 Versionen pro Startvorlage haben. Ihre Konten können je nach Alter und Nutzungsverlauf über unterschiedliche Kontingente verfügen.
- Parameter sind optional – Startvorlagenparameter sind optional. Sie müssen jedoch sicherstellen, dass Ihre Aufforderung zum Starten einer Instance alle erforderlichen Parameter enthält. Wenn Ihre Startvorlage z. B. keine AMI-ID enthält, müssen Sie eine AMI-ID eingeben, wenn Sie eine Instance mit dieser Startvorlage starten.
- Parameter nicht validiert – Die Parameter der Startvorlage werden nicht vollständig validiert, wenn Sie die Startvorlage erstellen. Wenn Sie falsche Werte für Parameter angeben oder nicht unterstützte Parameterkombinationen verwenden, können keine Instances unter Verwendung dieser Startvorlage gestartet werden. Um Probleme zu vermeiden, stellen Sie sicher, dass Sie die richtigen Werte angeben, und verwenden Sie unterstützte Parameterkombinationen. Um beispielsweise eine Instance in einer Platzierungsgruppe zu starten, müssen Sie einen unterstützten Instance-Typ angeben.
- Tags – Sie können eine Startvorlage, jedoch nicht die Version einer Startvorlage markieren.
- Unveränderlich – Startvorlagen sind unveränderlich. Um eine Startvorlage zu ändern, müssen Sie eine neue Version der Startvorlage erstellen.
- Versionsnummern – Die Startvorlagenversionen werden in der Reihenfolge nummeriert, in der sie erstellt werden. Wenn Sie eine Startvorlagenversion erstellen, können Sie die Versionsnummer nicht selbst angeben.

Für EC2 Amazon-Startvorlagen sind IAM-Berechtigungen erforderlich

Mit IAM-Berechtigungen können Sie steuern, ob Benutzer Startvorlagen oder Versionen von Startvorlagen auflisten, anzeigen, erstellen oder löschen können.

> **Important**
>
> Sie können Berechtigungen auf Ressourcenebene nicht verwenden, um die Ressourcen einzuschränken, die Benutzer in einer Startvorlage angeben können, wenn sie eine Startvorlage oder eine Startvorlagenversion erstellen. Stellen Sie daher sicher, dass nur vertrauenswürdigen Administratoren die Berechtigung zum Erstellen von Startvorlagen und Startvorlagenversionen gewährt wird.

Sie müssen allen Personen, die eine Startvorlage verwenden, die erforderlichen Berechtigungen zum Erstellen und Zugreifen auf die in der Startvorlage angegebenen Ressourcen gewähren. Zum Beispiel:

- Um eine Instance aus einem freigegebenen privaten Amazon Machine Image (AMI) zu starten, muss der Benutzer über die Startberechtigung für das AMI verfügen.
- Um EBS-Volumes mit Tags aus vorhandenen Snapshots zu erstellen, muss der Benutzer über Lesezugriff auf die Snapshots sowie über Berechtigungen zum Erstellen und Markieren von Volumes verfügen.

Inhalt

- ec2: CreateLaunchTemplate
- ec2: DescribeLaunchTemplates
- ec2: DescribeLaunchTemplateVersions
- ec2: DeleteLaunchTemplate
- Steuern von Berechtigungen für Versionsverwaltung
- Steuern des Zugriffs auf Tags in Startvorlagen

ec2: CreateLaunchTemplate

Um eine Startvorlage in der Konsole oder mithilfe von zu erstellen APIs, muss der Principal über die `ec2:CreateLaunchTemplate` entsprechende Berechtigung in einer IAM-Richtlinie verfügen.

Verwenden Sie nach Möglichkeit Tags, um den Zugriff auf die Startvorlagen in Ihrem Konto zu steuern.

Beispielsweise gewährt die folgende IAM-Richtlinienanweisung dem Prinzipal nur dann die Berechtigung, Startvorlagen zu erstellen, wenn die Vorlage das angegebene Tag verwendet (*purpose*=*testing*).

```
{
    "Sid": "IAMPolicyForCreatingTaggedLaunchTemplates",
    "Action": "ec2:CreateLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

Prinzipale, die Schlüssel erstellen, benötigen möglicherweise einige verwandte Berechtigungen, wie beispielsweise:

- ec2: CreateTags — Um der Startvorlage während des `CreateLaunchTemplate` Vorgangs Tags hinzuzufügen, muss der `CreateLaunchTemplate` Aufrufer über die `ec2:CreateTags` entsprechende Berechtigung in einer IAM-Richtlinie verfügen.
- ec2: RunInstances — Um EC2 Instances von der Startvorlage aus zu starten, die sie erstellt haben, muss der Principal auch über die `ec2:RunInstances` entsprechende Berechtigung in einer IAM-Richtlinie verfügen.

Bei Aktionen zur Ressourcenerstellung, die Tags anwenden, müssen Benutzer über `ec2:CreateTags`-Berechtigungen verfügen. Die folgende IAM-Richtlinienanweisung verwendet den Bedingungsschlüssel `ec2:CreateAction`, um Benutzern das Erstellen von Tags nur im Kontext von `CreateLaunchTemplate` zu ermöglichen. Die Benutzer können keine vorhandenen Startvorlagen oder andere Ressourcen kennzeichnen. Weitere Informationen finden Sie unter Erteilen Sie die Erlaubnis, EC2 Amazon-Ressourcen während der Erstellung zu taggen.

```
{
    "Sid": "IAMPolicyForTaggingLaunchTemplatesOnCreation",
    "Action": "ec2:CreateTags",
```

```
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": "CreateLaunchTemplate"
        }
    }
}
```

Der IAM-Benutzer, der eine Startvorlage erstellt, verfügt nicht automatisch über die Berechtigung, die von ihm erstellte Startvorlage zu verwenden. Wie jeder andere Prinzipal muss der Ersteller der Startvorlage eine Berechtigung über eine IAM-Richtlinie erhalten. Wenn ein IAM-Benutzer eine EC2 Instance von einer Startvorlage aus starten möchte, muss er über die entsprechende Genehmigung verfügen. `ec2:RunInstances` Wenn Sie diese Berechtigungen gewähren, können Sie angeben, dass Benutzer nur Startvorlagen mit bestimmten oder bestimmten IDs Tags verwenden können. Sie können auch das AMI und andere Ressourcen steuern, auf die jeder, der Startvorlagen verwendet, beim Starten von Instances verweisen und diese verwenden kann, indem Sie Berechtigungen auf Ressourcenebene für den `RunInstances`-Aufruf angeben. Beispiele für Richtlinien finden Sie unter Startvorlagen.

ec2: DescribeLaunchTemplates

Um Startvorlagen im Konto anzuzeigen und aufzulisten, muss der Prinzipal über die `ec2:DescribeLaunchTemplates`-Berechtigung in einer IAM-Richtlinie verfügen. Da `Describe`-Aktionen keine Berechtigungen auf Ressourcenebene unterstützen, müssen sie Sie ohne Bedingungen angeben, und der Wert des Ressourcenelements in der Richtlinie muss `"*"` sein.

Beispielsweise gewährt die folgende IAM-Richtlinienanweisung dem Prinzipal die Berechtigung, alle Startvorlagen im Konto anzuzeigen und aufzulisten.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplates",
    "Action": "ec2:DescribeLaunchTemplates",
    "Effect": "Allow",
    "Resource": "*"
}
```

ec2: DescribeLaunchTemplateVersions

Prinzipale, die Startvorlagen aufrufen, sollten auch über die `ec2:DescribeLaunchTemplateVersions`-Berechtigung verfügen, den gesamten Satz von Attributen abzurufen, aus denen die Startvorlagen bestehen.

Um Startvorlagenversionen im Konto anzuzeigen und aufzulisten, muss der Prinzipal über die `ec2:DescribeLaunchTemplateVersions`-Berechtigung in einer IAM-Richtlinie verfügen. Da `Describe`-Aktionen keine Berechtigungen auf Ressourcenebene unterstützen, müssen sie Sie ohne Bedingungen angeben, und der Wert des Ressourcenelements in der Richtlinie muss `"*"` sein.

Beispielsweise gewährt die folgende IAM-Richtlinienanweisung dem Prinzipal die Berechtigung, alle Startvorlagenversionen im Konto anzuzeigen und aufzulisten.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplateVersions",
    "Effect": "Allow",
    "Action": "ec2:DescribeLaunchTemplateVersions",
    "Resource": "*"
}
```

ec2: DeleteLaunchTemplate

> **Important**
>
> Seien Sie vorsichtig, wenn Sie Prinzipalen die Berechtigung zum Löschen einer Ressource gewähren. Das Löschen einer Startvorlage kann zu einem Fehler in einer AWS Ressource führen, die auf der Startvorlage basiert.

Um eine Startvorlage zu löschen muss der Prinzipal über die `ec2:DeleteLaunchTemplate`-Berechtigung in einer IAM-Richtlinie verfügen. Wann immer möglich, verwenden Sie Bedingungsschlüssel, um die Berechtigungen einzuschränken.

Die folgende IAM-Richtlinienanweisung gewährt dem Prinzipal beispielsweise nur dann die Berechtigung, Startvorlagen zu löschen, wenn die Vorlage das angegebene Tag verwendet (*purpose*=*testing*).

```
{
```

```
    "Sid": "IAMPolicyForDeletingLaunchTemplates",
    "Action": "ec2:DeleteLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

Alternativ können Sie sie verwenden, ARNs um die Startvorlage zu identifizieren, für die die IAM-Richtlinie gilt.

Eine Startvorlage verfügt über den folgenden ARN.

```
"Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/lt-09477bcd97b0d310e"
```

Sie können mehrere angeben, ARNs indem Sie sie in eine Liste einschließen, oder Sie können den `Resource` Wert `"*"` ohne das `Condition` Element angeben, damit der Prinzipal jede Startvorlage im Konto löschen kann.

Steuern von Berechtigungen für Versionsverwaltung

Vertrauenswürdigen Administratoren können Sie Zugriff zum Erstellen und Löschen von Versionen einer Startvorlage sowie zum Ändern der Standardversion einer Startvorlage gewähren, indem Sie IAM-Richtlinien ähnlich den folgenden Beispielen verwenden.

> **Important**
>
> Seien Sie vorsichtig, wenn Sie Prinzipalen die Berechtigung gewähren, Versionen von Startvorlagen zu erstellen oder Startvorlagen zu ändern.
>
> - Wenn Sie eine Startvorlagenversion erstellen, wirken Sie sich auf alle AWS Ressourcen aus, die es Amazon EC2 ermöglichen, Instances in Ihrem Namen mit der `Latest` Version zu starten.
> - Wenn Sie eine Startvorlage ändern, können Sie die Version ändern `Default` und sich somit auf alle AWS Ressourcen auswirken, die es Amazon ermöglichen, Instances in Ihrem Namen mit dieser modifizierten Version EC2 zu starten.

Sie müssen auch vorsichtig sein, wenn Sie mit AWS Ressourcen umgehen, die mit der Vorlagenversion interagieren `Latest` oder diese `Default` starten, wie EC2 Fleet und Spot-Flotte. Wenn eine andere Version der Startvorlage für `Latest` oder verwendet wird`Default`, überprüft Amazon die Benutzerberechtigungen EC2 nicht erneut auf auszuführende Aktionen, wenn neue Instances gestartet werden, um die Zielkapazität der Flotte zu erreichen, da keine Benutzerinteraktion mit der AWS Ressource stattfindet. Indem einem Benutzer die Berechtigung zum Aufrufen von `CreateLaunchTemplateVersion` und erteilt wird `ModifyLaunchTemplate` APIs, wird dem Benutzer die `iam:PassRole` Berechtigung auch erteilt, wenn er die Flotte auf eine andere Version der Startvorlage weiterleitet, die ein Instance-Profil (einen Container für eine IAM-Rolle) enthält. Dies bedeutet, dass ein Benutzer potenziell eine Startvorlage aktualisieren kann, um eine IAM-Rolle an eine Instance zu übergeben, auch wenn er nicht über die entsprechende `iam:PassRole`-Berechtigung verfügt. Sie können dieses Risiko kontrollieren, indem Sie bei der Vergabe von Berechtigungen für die Erstellung und Verwaltung von Startvorlagenversionen vorsichtig vorgehen.

ec2: CreateLaunchTemplateVersion

Um eine neue Version einer Startvorlage zu erstellen, muss der Prinzipal über die `ec2:CreateLaunchTemplateVersion`-Berechtigung für die Startvorlage in einer IAM-Richtlinie verfügen.

Die folgende IAM-Richtlinienerklärung gewährt dem Prinzipal beispielsweise nur dann die Berechtigung, Startvorlagenversionen zu erstellen, wenn die Version das angegebene Tag verwendet (*`environment`*=*`production`*). Alternativ können Sie eine oder mehrere Startvorlagen angeben ARNs, oder Sie können den `Resource` Wert `"*"` ohne das `Condition` Element angeben, damit der Principal Versionen jeder Startvorlage im Konto erstellen kann.

```
{
    "Sid": "IAMPolicyForCreatingLaunchTemplateVersions",
    "Action": "ec2:CreateLaunchTemplateVersion",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
```

```
    }
}
```

ec2: DeleteLaunchTemplateVersion

> **Important**
>
> Wie immer sollten Sie Vorsicht walten lassen, wenn Sie Prinzipalen die Berechtigung zum Löschen einer Ressource erteilen. Das Löschen einer Version der Startvorlage kann zu einem Fehler in einer AWS Ressource führen, die auf der Version der Startvorlage basiert.

Um eine neue Version einer Startvorlagenversion zu erstellen, muss der Prinzipal über die `ec2:DeleteLaunchTemplateVersion`-Berechtigung für die Startvorlage in einer IAM-Richtlinie verfügen.

Die folgende IAM-Richtlinienerklärung gewährt dem Prinzipal beispielsweise nur dann die Berechtigung, Startvorlagenversionen zu löschen, wenn die Version das angegebene Tag verwendet (*`environment`*=*`production`*). Alternativ können Sie eine oder mehrere Startvorlagen angeben ARNs, oder Sie können den `Resource` Wert `"*"` ohne das `Condition` Element angeben, damit der Prinzipal Versionen aller Startvorlagen im Konto löschen kann.

```
{
    "Sid": "IAMPolicyForDeletingLaunchTemplateVersions",
    "Action": "ec2:DeleteLaunchTemplateVersion",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

ec2: ModifyLaunchTemplate

Um die mit einer Startvorlage zugeordnete `Default`-Version zu ändern, muss der Prinzipal über die `ec2:ModifyLaunchTemplate`-Berechtigung für die Startvorlage in einer IAM-Richtlinie verfügen.

Die folgende IAM-Richtlinienerklärung gewährt dem Prinzipal beispielsweise nur dann die Berechtigung, Startvorlagen zu ändern, wenn die Vorlage das angegebene Tag verwendet (*environment*=*production*). Alternativ können Sie eine oder mehrere Startvorlagen angeben ARNs, oder Sie können den `Resource` Wert `"*"` ohne das `Condition` Element angeben, damit der Principal jede Startvorlage im Konto ändern kann.

```
{
    "Sid": "IAMPolicyForModifyingLaunchTemplates",
    "Action": "ec2:ModifyLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

Steuern des Zugriffs auf Tags in Startvorlagen

Sie können Bedingungsschlüssel verwenden, um Tagging-Berechtigungen einzuschränken, wenn es sich bei der Ressource um eine Startvorlage handelt. Die folgende IAM-Richtlinie erlaubt beispielsweise nur das Entfernen des Tags mit dem *temporary*-Schlüssel aus Startvorlagen im angegebenen Konto und in der angegebenen Region.

```
{
    "Sid": "IAMPolicyForDeletingTagsOnLaunchTemplates",
    "Action": "ec2:DeleteTags",
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
    "Condition": {
        "ForAllValues:StringEquals": {
            "aws:TagKeys": ["temporary"]
        }
    }
}
```

Weitere Informationen zu Bedingungsschlüsseln, mit denen Sie die Tagschlüssel und -werte steuern können, die auf EC2 Amazon-Ressourcen angewendet werden können, finden Sie unterKontrollieren des Zugriffs auf bestimmte Tags (Markierungen).

Verwenden Sie EC2 Amazon-Startvorlagen, um den Start von EC2 Amazon-Instances zu steuern

Sie können die Konfiguration Ihrer EC2 Amazon-Instances steuern, indem Sie angeben, dass Benutzer Instances nur starten können, wenn sie eine Startvorlage verwenden, und dass sie nur eine bestimmte Startvorlage verwenden können. Sie können auch festlegen, wer Startvorlagen und Versionen von Startvorlagen erstellen, ändern, beschreiben und löschen darf.

Verwenden von Startvorlagen zum Steuern von Startparametern

Eine Startvorlage kann alle oder einige der Parameter zum Starten einer Instance beim Start enthalten. Wenn Sie eine Instance über eine Startvorlage starten, können Sie jedoch Parameter außer Kraft setzen, die in der Startvorlage angegeben werden. Sie können auch zusätzliche Parameter angeben, die nicht in der Startvorlage enthalten sind.

> **Note**
>
> Sie können während des Starts keine Startvorlagenparameter entfernen (Sie können beispielsweise keinen Nullwert für den Parameter angeben). Um einen Parameter zu entfernen, erstellen Sie eine neue Version der Startvorlage ohne den Parameter und starten Sie die Instance mit dieser Version.

Zum Starten von Instances müssen Benutzer über die Berechtigung zur Verwendung der `ec2:RunInstances`-Aktion verfügen. Benutzer müssen außerdem über Berechtigungen zum Erstellen oder Verwenden der Ressourcen verfügen, die mit der Instance erstellt oder ihr zugewiesen werden. Sie können für die Aktion `ec2:RunInstances` Berechtigungen auf Ressourcenebene verwenden, um die Startparameter zu steuern, die die Benutzer festlegen können. Alternativ können Sie Benutzern gestatten, eine Instance unter Nutzung einer Startvorlage zu starten. Auf diese Weise können Sie Startparameter über eine Startvorlage anstatt über eine IAM-Richtlinie verwalten und eine Startvorlage als Autorisierungsmethode für das Starten von Instances einsetzen. Sie können z. B. festlegen, dass Benutzer Instances nur über eine Startvorlage starten und dass sie nur eine bestimmte Startvorlage verwenden können. Sie können auch steuern, welche Startparameter Benutzer in der Startvorlage außer Kraft setzen dürfen. Beispiele für Richtlinien finden Sie unter Startvorlagen.

Steuern der Nutzung von Startvorlagen

Standardmäßig sind -Benutzer nicht zum Arbeiten mit Startvorlagen berechtigt. Sie können eine Richtlinie erstellen, über die Benutzer Berechtigungen zum Erstellen, Ändern, Beschreiben und Löschen von Startvorlagen und Startvorlagenversionen erhalten. Sie können auf einige Startvorlagen-Aktionen auch Berechtigungen auf Ressourcenebene anwenden, mit denen Sie steuern können, welche Ressourcen Benutzer für diese Aktionen nutzen können. Weitere Informationen erhalten Sie in den folgenden Beispielrichtlinien: Beispiel: Arbeiten mit Startvorlagen.

Überlegen Sie sorgfältig, wenn Sie Benutzern Berechtigungen zur Verwendung der Aktionen `ec2:CreateLaunchTemplate` und `ec2:CreateLaunchTemplateVersion` erteilen. Mit Berechtigungen auf Ressourcenebene können Sie nicht steuern, welche Ressourcen Benutzer in der Startvorlage angeben können. Um einzuschränken, welche Ressourcen zum Starten einer Instance verwendet werden, achten Sie darauf, nur die betreffenden Administratoren zum Erstellen von Startvorlagen und Startvorlagenversionen zu berechtigen.

Wichtige Sicherheitsbedenken bei der Verwendung von Startvorlagen mit EC2 Fleet oder Spot Fleet

Zur Verwendung von Startvorlagen müssen Sie Ihren Benutzern auch Berechtigungen zum Erstellen, Ändern, Beschreiben und Löschen von Startvorlagen und Startvorlagenversionen erteilen. Sie können steuern, wer Startvorlagen und Startvorlagenversionen erstellen kann, indem Sie den Zugriff auf die Aktionen `ec2:CreateLaunchTemplate` und `ec2:CreateLaunchTemplateVersion` steuern. Sie können auch steuern, wer Startvorlagen ändern kann, indem Sie den Zugriff auf die Aktion `ec2:ModifyLaunchTemplate` steuern.

> **Important**
>
> Wenn eine EC2 Flotte oder Spot-Flotte so konfiguriert ist, dass sie die neueste Version oder die Standardversion der Startvorlage verwendet, weiß die Flotte nicht, ob Latest oder Standard später so geändert werden, dass sie auf eine andere Version der Startvorlage verweisen. Wenn eine andere Version der Startvorlage für Latest oder Standard verwendet wird, überprüft Amazon beim Start neuer Instances zur Erfüllung der Zielkapazität der Flotte EC2 nicht erneut die Berechtigungen für auszuführende Aktionen. Dies ist ein wichtiger Aspekt bei der Erteilung von Berechtigungen für die Erstellung und Verwaltung von Startvorlagenversionen, insbesondere bei der Aktion `ec2:ModifyLaunchTemplate`, die es einem Benutzer ermöglicht, die Standardversion der Startvorlage zu ändern.

Wenn einem Benutzer die Erlaubnis erteilt wird, die EC2 Aktionen für die Startvorlage zu verwenden APIs, erhält der Benutzer faktisch auch die `iam:PassRole` Erlaubnis, wenn er eine EC2 Flotte oder Spot-Flotte erstellt oder aktualisiert, sodass er auf eine andere Version der Startvorlage verweist, die ein Instance-Profil (einen Container für eine IAM-Rolle) enthält. Dies bedeutet, dass ein Benutzer potenziell eine Startvorlage aktualisieren kann, um eine IAM-Rolle an eine Instance zu übergeben, auch wenn er nicht über die entsprechende `iam:PassRole`-Berechtigung verfügt. Weitere Informationen und ein Beispiel für eine IAM-Richtlinie finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden.

Weitere Informationen erhalten Sie unter Steuern der Nutzung von Startvorlagen und Beispiel: Arbeiten mit Startvorlagen.

Erstellen Sie eine EC2 Amazon-Startvorlage

Sie können eine EC2 Amazon-Startvorlage erstellen, indem Sie Ihre eigenen Werte für die Instance-Konfigurationsparameter angeben oder die Werte aus einer vorhandenen Startvorlage oder EC2 Amazon-Instance abrufen.

Sie müssen nicht für jeden Parameter in der Startvorlage einen Wert angeben. Sie müssen nur einen Instance-Konfigurationsparameter angeben, um eine Startvorlage zu erstellen. Um Parameter anzugeben, die Sie nicht angeben möchten, wählen Sie bei Verwendung der Konsole die Option Nicht in die Startvorlage aufnehmen aus. Wenn Sie ein Befehlszeilentool verwenden, geben Sie die Parameter nicht mit an, um anzuzeigen, dass Sie sie nicht in der Startvorlage angeben möchten.

Wenn Sie in der Startvorlage ein AMI angeben möchten, können Sie entweder ein AMI auswählen oder einen Systems-Manager-Parameter angeben, der beim Start der Instance auf ein AMI verweist.

Wenn eine Instance mit einer Startvorlage gestartet wird, werden die in der Startvorlage angegebenen Werte verwendet, um die entsprechenden Instance-Parameter zu konfigurieren. Wenn in der Startvorlage kein Wert angegeben ist, wird der Standardwert für den entsprechenden Instance-Parameter verwendet.

Aufgaben

- Startvorlage durch Angabe von Parametern erstellen
- Erstellen einer Startvorlage anhand einer vorhandenen Startvorlage
- Erstellen einer Startvorlage aus einer Instance
- Verwenden eines Systems-Manager-Parameters anstelle einer AMI-ID

Startvorlage durch Angabe von Parametern erstellen

Um eine Launchvorlage zu erstellen, müssen Sie den Namen der Launchvorlage und mindestens einen Instance-Konfigurationsparameter angeben.

Eine Beschreibung jedes Parameters finden Sie unter Referenz für EC2 Amazon-Instance-Konfigurationsparameter.

Console

Eine Startvorlage erstellen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates (Startvorlagen) und dann Create launch template (Startvorlage erstellen) aus.
3. Gehen Sie unter Name und Beschreibung der Startvorlage folgendermaßen vor:
   a. Geben Sie für Launch template name (Startvorlagenname) einen aussagekräftigen Namen für die Startvorlage ein.
   b. Geben Sie unter Template version description (Beschreibung der Vorlagenversion) eine kurze Beschreibung dieser Version der Startvorlage ein.
   c. Um die Startvorlage bei der Erstellung zu markieren, erweitern Sie Vorlagen-Tags und wählen Sie Tag hinzufügen aus. Geben Sie dann einen Tag-Schlüssel und ein Wert-Paar ein. Wählen Sie für jede weitere Markierung Neue Markierung hinzufügen aus.

   > **Note**
   >
   > Um die Ressourcen zu markieren, die beim Start einer Instance erstellt werden, müssen Sie die Tags unter Resource tags (Ressourcen-Tags) angeben. Weitere Informationen finden Sie im Schritt 9 in diesem Vorgehen.

4. Unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image) können Sie entweder die Option Nicht in Startvorlage aufnehmen ausgewählt lassen oder das Betriebssystem (OS) für die Instance und dann ein AMI auswählen. Alternativ können Sie einen Systems-Manager-Parameter angeben, anstatt ein AMI anzugeben. Weitere Informationen finden Sie unter Verwenden eines Systems-Manager-Parameters anstelle einer AMI-ID.

Ein AMI ist eine Vorlage, die das Betriebssystem und die Software enthält, die zum Starten einer Instance erforderlich sind.

5. Unter Instance-Typ können Sie entweder die Option Nicht in Startvorlage einbeziehen aktiviert lassen oder einen Instance-Typ auswählen oder Instance-Attribute angeben und Amazon die Instance-Typen anhand dieser Attribute EC2 identifizieren lassen.

> **Note**
>
> Die Angabe von Instance-Attributen wird nur unterstützt, wenn die Startvorlage von Amazon EC2 Auto Scaling Scaling-Gruppen, EC2 Fleet und Spot Fleet zum Starten von Instances verwendet wird. Weutere Informationen finden Sie unter Erstellen einer gemischten Instances-Gruppe mit attributbasierter Auswahl des Instance-Typs und Geben Sie Attribute für die Auswahl von Instance-Typen für EC2-Flotte oder Spot-Flotte an.
> Wenn Sie die Startvorlage im Launch-Instance-Assistenten oder mit der RunInstances API verwenden möchten, können Sie keine Instance-Typ-Attribute angeben.

Der Instance-Typ bestimmt die Hardware-Konfiguration (CPU, Arbeitsspeicher, Speicher und Netzwerkkapazität) und die Größe des Host-Computers, der für eine Instance verwendet wird.

Wenn Sie sich nicht sicher sind, welchen Instance-Typ Sie auswählen sollen, gehen Sie folgendermaßen vor:

- Wählen Sie Instance-Typen vergleichen, um verschiedene Instance-Typen anhand der folgenden Attribute zu vergleichen: Anzahl von vCPUs, Architektur, Speichergröße (GiB), Speichermenge (GB), Speichertyp und Netzwerkleistung.
- Wählen Sie Rat einholen, um Anleitungen und Vorschläge für Instance-Typen vom EC2 Instance-Typ-Finder zu erhalten. Weitere Informationen finden Sie unter Holen Sie sich Empfehlungen vom EC2-Instance-Typ-Finder.

> **Note**
>
> Je nachdem, wann Sie Ihr Konto erstellt haben, sind Sie möglicherweise berechtigt, Amazon EC2 im Rahmen des kostenlosen Kontingents zu nutzen.
> Wenn Sie Ihre AWS-Konto vor dem 15. Juli 2025 erstellt haben und sie weniger als 12 Monate alt ist, können Sie Amazon im EC2 Rahmen des kostenlosen Kontingents nutzen, indem Sie den Instance-Typ t2.micro oder in Regionen, in denen t2.micro nicht verfügbar ist, den Instance-Typ t3.micro auswählen. Beachten Sie, dass beim Starten einer t3.micro-Instance standardmäßig der Modus Unlimited verwendet wird, wodurch je nach CPU-Auslastung zusätzliche Gebühren anfallen können. Wenn ein Instance-Typ unter dem kostenlosen Kontingent berechtigt ist, ist er als Für das kostenlose Kontingent berechtigt gekennzeichnet.
> Wenn Sie Ihre Instance-Typen AWS-Konto am oder nach dem 15. Juli 2025 erstellt haben, können Sie die Instance-Typen t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large und m7i-flex.large für 6 Monate oder bis Ihr Guthaben aufgebraucht ist verwenden.
> Weitere Informationen finden Sie unter Vorteile des kostenlosen Kontingents vor und nach dem 15. Juli 2025.

6. Lassen Sie unter Schlüsselpaar (Anmeldung) für Schlüsselpaar-Name entweder die Option Nicht in Startvorlage aufnehmen ausgewählt, wählen Sie ein vorhandenes Schlüsselpaar oder erstellen Sie ein neues.
7. Unter Netzwerkeinstellungen können Sie entweder die Option Nicht in Startvorlage aufnehmen aktiviert lassen oder Werte für die verschiedenen Netzwerkeinstellungen angeben.
8. Wenn Sie unter Speicher konfigurieren in der Startvorlage ein AMI angegeben haben, enthält das AMI ein oder mehrere Speicher-Volumes, einschließlich des Root-Volumes (Volume 1 (AMI Root)). Sie können optional zusätzliche Volumes angeben, die an die Instance angefügt werden sollen. Um ein neues Volume hinzuzufügen, wählen Sie Add new volume (Neues Volume hinzufügen).
9. Unter Ressourcen-Tags, um die Ressourcen, die beim Start einer Instance erstellt werden mit Tags zu versehene, wählen Sie Tag hinzufügen und geben dann ein Tag-Schlüssel- und Wertepaar ein. Geben Sie unter Resource types (Ressourcentypen) die Ressourcen an, die bei der Erstellung markiert werden sollen. Sie können den gleichen Tag für alle Ressourcen

spezifizieren oder verschiedene Tags für verschiedene Ressourcen angeben. Wählen Sie für jedes weitere Tag Add another Tag (Weiteres Tag hinzufügen) aus.

Sie können Tags für die folgenden Ressourcen angeben, die erstellt werden, wenn eine Startvorlage verwendet wird:

- Instances
- Datenträger
- Elastic Graphics
- Spot-Instance-Anforderungen
- Netzwerkschnittstellen

> **Note**
>
> Um die Startvorlage selbst zu markieren, müssen Sie die Tags unter Template tags (Vorlagen-Tags) angeben. Weitere Informationen finden Sie im Schritt 3 in diesem Vorgehen.

10. Erweitern Sie für Erweiterte Details den Bereich zur Ansicht der Felder und geben Sie zusätzliche Parameter für die Instance an.
11. Verwenden Sie die Schaltfläche Zusammenfassung, um die Konfiguration Ihrer Startvorlage zu überprüfen. Sie können zu einem beliebigen Abschnitt navigieren, indem Sie den entsprechenden Link auswählen und dann die erforderlichen Änderungen vornehmen.
12. Wenn Sie bereit sind, Ihre Launchvorlage zu erstellen, wählen Sie Create launch template (Launchvorlage erstellen) aus.

AWS CLI

Eine Startvorlage erstellen

Verwenden Sie den Befehl create-launch-template.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --version-description WebVersion1 \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
```

```
    --launch-template-data file://template-data.json
```

Im Folgenden finden Sie eine Beispiel-JSON-Datei, welche die Startvorlagen-Daten für die Instance-Konfiguration enthält. Speichern Sie den JSON-Code in einer Datei und fügen Sie ihn in den `--launch-template-data`-Parameter ein, wie im Beispielbefehl gezeigt.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-0abcdef1234567890"
    }],
    "ImageId": "ami-0abcdef1234567890",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":4,
        "ThreadsPerCore":2
    }
}
```

Es folgt eine Beispielausgabe.

```
{
    "LaunchTemplate": {
        "LatestVersionNumber": 1,
        "LaunchTemplateId": "lt-01238c059e3466abc",
        "LaunchTemplateName": "TemplateForWebServer",
        "DefaultVersionNumber": 1,
        "CreatedBy": "arn:aws:iam::123456789012:root",
        "CreateTime": "2017-11-27T09:13:24.000Z"
    }
}
```

PowerShell

Eine Startvorlage erstellen

Verwenden Sie das cmdlet New-EC2LaunchTemplate.

```
$launchTemplateData = [Amazon.EC2.Model.RequestLaunchTemplateData]@{
    ImageId = 'ami-0abcdef1234567890'
    InstanceType = 'r5.4xlarge'
    NetworkInterfaces = @(

 [Amazon.EC2.Model.LaunchTemplateInstanceNetworkInterfaceSpecificationRequest]@{
            AssociatePublicIpAddress = $true
            DeviceIndex = 0
            Ipv6AddressCount = 1
            SubnetId = 'subnet-0abcdef1234567890'
        }
    )
    TagSpecifications = @(
        [Amazon.EC2.Model.LaunchTemplateTagSpecificationRequest]@{
            ResourceType = 'instance'
            Tags = [Amazon.EC2.Model.Tag]@{
                Key = 'Name'
                Value = 'webserver'
            }
        }
    )
    CpuOptions = [Amazon.EC2.Model.LaunchTemplateCpuOptionsRequest]@{
        CoreCount = 4
        ThreadsPerCore = 2
    }
}
$tagSpecificationData = [Amazon.EC2.Model.TagSpecification]@{
    ResourceType = 'launch-template'
    Tags = [Amazon.EC2.Model.Tag]@{
        Key = 'purpose'
        Value = 'production'
    }
}
New-EC2LaunchTemplate -LaunchTemplateName 'TemplateForWebServer' `
    -VersionDescription 'WebVersion1' `
    -LaunchTemplateData $launchTemplateData `
    -TagSpecification $tagSpecificationData
```

Es folgt eine Beispielausgabe.

```
CreatedBy            : arn:aws:iam::123456789012:root
CreateTime           : 9/19/2023 16:57:55
DefaultVersionNumber : 1
LatestVersionNumber  : 1
LaunchTemplateId     : lt-01238c059eEXAMPLE
LaunchTemplateName   : TemplateForWebServer
Tags                 : {purpose}
```

Erstellen einer Startvorlage anhand einer vorhandenen Startvorlage

Sie können eine vorhandene Startvorlage klonen und dann die Parameter anpassen, um eine neue Startvorlage zu erstellen. Sie können dies jedoch nur tun, wenn Sie die EC2 Amazon-Konsole verwenden. Das AWS CLI unterstützt das Klonen einer Vorlage nicht. Eine Beschreibung jedes Parameters finden Sie unter Referenz für EC2 Amazon-Instance-Konfigurationsparameter.

Console

So erstellen Sie eine Startvorlage anhand einer vorhandenen Startvorlage

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates (Startvorlagen) und dann Create launch template (Startvorlage erstellen) aus.
3. Geben Sie für Launch template name (Startvorlagenname) einen aussagekräftigen Namen für die Startvorlage ein.
4. Geben Sie unter Template version description (Beschreibung der Vorlagenversion) eine kurze Beschreibung dieser Version der Startvorlage ein.
5. Um die Startvorlage bei der Erstellung mit einem Tag zu versehen, erweitern Sie Vorlagen-Tags, wählen Sie Neues Tag hinzufügen und geben Sie ein Tag-Schlüssel- und Wertepaar ein.
6. Erweitern Sie Source template (Quellvorlage). Wählen Sie in Launch template name (Name der Startvorlage) die Startvorlage aus, auf der die neue Startvorlage basieren soll.
7. Wählen Sie für Source template version die Version der Startvorlage aus, auf der die neue Startvorlage basieren soll.
8. Passen Sie alle Startparameter wie erforderlich an und wählen Sie Create launch template (Startvorlage erstellen).

Erstellen einer Startvorlage aus einer Instance

Sie können die Parameter einer vorhandenen EC2 Amazon-Instance klonen und dann die Parameter anpassen, um eine Startvorlage zu erstellen. Eine Beschreibung jedes Parameters finden Sie unter Referenz für EC2 Amazon-Instance-Konfigurationsparameter.

Console

So erstellen Sie eine Startvorlage aus einer Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance und anschließend Aktionen, Image und Vorlagen, Vorlage aus einer Instance erstellen aus.
4. Geben Sie einen Namen, eine Beschreibung und Tag (Markierung) an und passen Sie die Startparameter wie erforderlich an.

> **Note**
>
> Wenn Sie eine Startvorlage aus einer Instance erstellen, sind die Netzwerkschnittstelle IDs und die IP-Adressen der Instance nicht in der Vorlage enthalten.

5. Wählen Sie Startvorlage erstellen.

AWS CLI

Sie können die verwenden AWS CLI , um eine Startvorlage aus einer vorhandenen Instance zu erstellen, indem Sie zuerst die Startvorlagendaten von einer Instance abrufen und dann mithilfe der Startvorlagendaten eine Startvorlage erstellen.

So erhalten Sie Startvorlagendaten von einer Instance

- Verwenden Sie den Befehl get-launch-template-data und geben Sie die Instance-ID an. Sie können die Ausgabe als Basis zum Erstellen einer neuen Startvorlage oder einer neuen Version der Startvorlage verwenden. Die Ausgabe umfasst standardmäßig ein `LaunchTemplateData`-Objekt der obersten Ebene, das nicht in den Daten der

Startvorlage angegeben werden kann. Verwenden Sie die Option `--query`, um dieses Objekt auszuschließen.

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData"
```

Es folgt eine Beispielausgabe.

```
    {
        "Monitoring": {},
        "ImageId": "ami-8c1be5f6",
        "BlockDeviceMappings": [
            {
                "DeviceName": "/dev/xvda",
                "Ebs": {
                    "DeleteOnTermination": true
                }
            }
        ],
        "EbsOptimized": false,
        "Placement": {
            "Tenancy": "default",
            "GroupName": "",
            "AvailabilityZone": "us-east-1a"
        },
        "InstanceType": "t2.micro",
        "NetworkInterfaces": [
            {
                "Description": "",
                "NetworkInterfaceId": "eni-35306abc",
                "PrivateIpAddresses": [
                    {
                        "Primary": true,
                        "PrivateIpAddress": "10.0.0.72"
                    }
                ],
                "SubnetId": "subnet-7b16de0c",
                "Groups": [
                    "sg-7c227019"
                ],
                "Ipv6Addresses": [
```

```
                    {
                        "Ipv6Address": "2001:db8:1234:1a00::123"
                    }
                ],
                "PrivateIpAddress": "10.0.0.72"
            }
        ]
    }
```

Sie können die Ausgabe direkt in eine Datei schreiben, z. B.:

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData" >> instance-data.json
```

So erstellen Sie eine Startvorlage mithilfe von Startvorlagendaten

- Verwenden Sie den create-launch-templateBefehl, um mithilfe der Ausgabe des vorherigen Verfahrens eine Startvorlage zu erstellen. Weitere Informationen zum Erstellen einer Startvorlage mit dem AWS CLI finden Sie unterStartvorlage durch Angabe von Parametern erstellen.

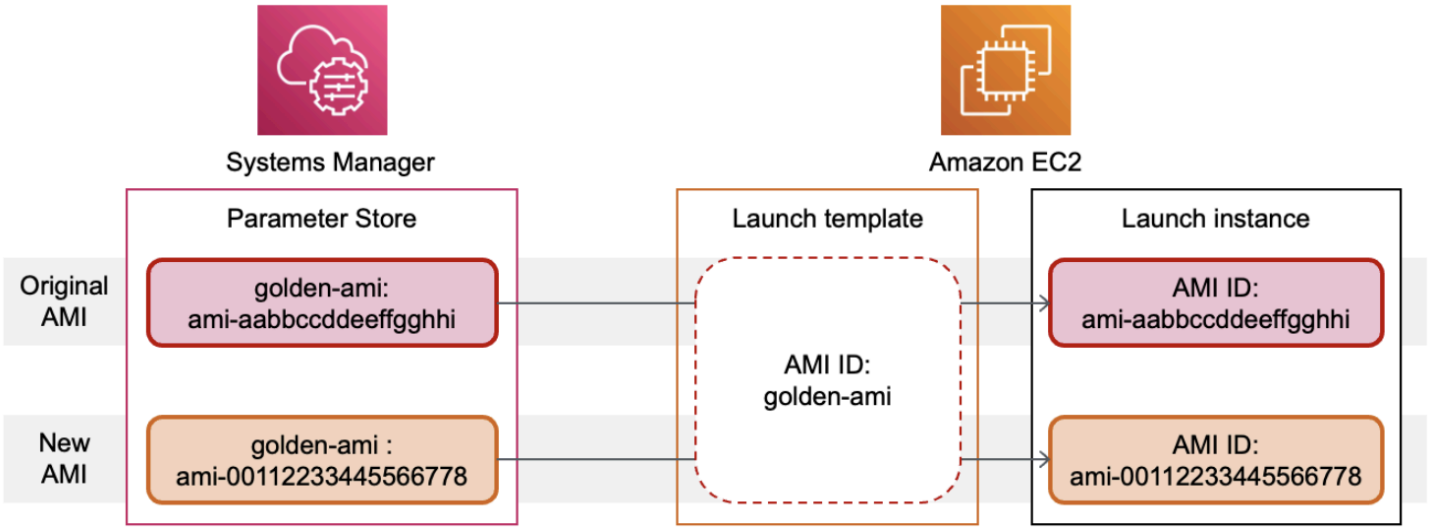
Verwenden eines Systems-Manager-Parameters anstelle einer AMI-ID

Sie können anstelle einer AMI-ID in Ihren Startvorlagen auch einen AWS Systems Manager -Parameter angeben. Wenn sich die AMI-ID ändert, können Sie die AMI-ID an einem Ort aktualisieren, indem Sie den Systems-Manager-Parameter im Systems-Manager-Parameterspeicher aktualisieren. Parameter können auch mit anderen geteilt werden AWS-Konten. Sie können AMI-Parameter zentral in einem Konto speichern und verwalten und sie für jedes andere Konto freigeben, das auf sie verweisen muss. Mithilfe eines Systems-Manager-Parameters können alle Ihre Startvorlagen in einer einzigen Aktion aktualisiert werden.

Ein Systems-Manager-Parameter ist ein benutzerdefiniertes Schlüssel-Wert-Paar, das Sie im AWS Systems Manager -Parameterspeicher erstellen. Der Parameterspeicher bietet einen zentralen Ort zum Speichern Ihrer Anwendungskonfigurationswerte.

Im folgenden Diagramm wird der `golden-ami`-Parameter zuerst dem ursprünglichen AMI `ami-aabbccddeeffgghhi` im Parameterspeicher zugeordnet. In der Startvorlage lautet der Wert für die AMI-ID `golden-ami`. Wenn eine Instance mit dieser Startvorlage gestartet wird, wird die AMI-ID zu

`ami-aabbccddeeffgghhi` aufgelöst. Später wird das AMI aktualisiert, was zu einer neuen AMI-ID führt. Im Parameter Store wird der `golden-ami`-Parameter dem neuen `ami-00112233445566778` zugeordnet. Die Startvorlage bleibt unverändert. Wenn eine Instance mit dieser Startvorlage gestartet wird, wird die AMI-ID in das neue `ami-00112233445566778` aufgelöst.



Systems Manager Manager-Parameterformat für AMI IDs

Startvorlagen erfordern, dass benutzerdefinierte Systems-Manager-Parameter das folgende Format einhalten, wenn sie anstelle einer AMI-ID verwendet werden:

- Parametertyp: `String`
- Parameterdatentyp: `aws:ec2:image` – Dadurch wird sichergestellt, dass der Parameterspeicher überprüft, ob der von Ihnen eingegebene Wert das richtige Format für eine AMI-ID hat.

Weitere Informationen zum Erstellen eines gültigen Parameters für eine AMI-ID finden Sie unter Erstellen von Systems-Manager-Parametern im AWS Systems Manager -Benutzerhandbuch.

Systems-Manager-Parameterformat in Startvorlagen

Um einen Systems-Manager-Parameter anstelle einer AMI-ID in einer Startvorlage zu verwenden, müssen Sie beim Angeben des Parameters in der Startvorlage eines der folgenden Formate verwenden:

So verweisen Sie auf einen öffentlichen Parameter:

- `resolve:ssm:`*`public-parameter`*

So verweisen Sie auf einen Parameter, der im selben Konto gespeichert ist:

- `resolve:ssm:parameter-name`
- `resolve:ssm:parameter-name:version-number` – Die Versionsnummer selbst ist eine Standardbezeichnung
- `resolve:ssm:parameter-name:label`

So verweisen Sie auf einen von einem anderen AWS-Konto freigegebenen Parameter:

- `resolve:ssm:parameter-ARN`
- `resolve:ssm:parameter-ARN:version-number`
- `resolve:ssm:parameter-ARN:label`

Parameter-Versionen

Systems-Manager-Parameter sind versionierte Ressourcen. Wenn Sie einen Parameter aktualisieren, erstellen Sie neue, aufeinander folgende Versionen des Parameters. Systems Manager unterstützt Parameterbezeichnungen, die Sie bestimmten Versionen eines Parameters zuordnen können.

Der `golden-ami`-Parameter kann beispielsweise drei Versionen haben: `1`, `2` und `3`. Sie können eine Parameterbezeichnung `beta` erstellen, die Version 2 zugeordnet ist, und eine Parameterbezeichnung `prod`, die Version `3` zugeordnet ist.

In einer Startvorlage können Sie Version 3 des `golden-ami`-Parameters angeben, indem Sie eines der folgenden Formate verwenden:

- `resolve:ssm:golden-ami:3`
- `resolve:ssm:golden-ami:prod`

Die Angabe der Version oder Bezeichnung ist optional. Wenn keine Version oder Bezeichnung angegeben ist, wird die neueste Version des Parameters verwendet.

Angeben eines Systems-Manager-Parameters in einer Startvorlage

Sie können einen Systems-Manager-Parameter in einer Startvorlage anstelle einer AMI-ID angeben, wenn Sie eine Startvorlage oder eine neue Version einer Startvorlage erstellen.

Console

So geben Sie einen Systems-Manager-Parameter in einer Startvorlage an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates (Startvorlagen) und dann Create launch template (Startvorlage erstellen) aus.
3. Geben Sie für Launch template name (Startvorlagenname) einen aussagekräftigen Namen für die Startvorlage ein.
4. Wählen Sie unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image) die Option Mehr durchsuchen aus AMIs.
5. Wählen Sie die Pfeiltaste rechts neben der Suchleiste und wählen Sie dann Benutzerdefinierten Wert/Systems-Manager-Parameter angeben aus.
6. Gehen Sie im Dialogfeld Benutzerdefinierten Wert oder Systems-Manager-Parameter angeben wie folgt vor:

   a. Geben Sie für AMI-ID oder Systems-Manager-Parameterzeichenfolge den Systems-Manager-Parameternamen in einem der folgenden Formate ein:

      So verweisen Sie auf einen öffentlichen Parameter:

      - **resolve:ssm:*public-parameter***

      So verweisen Sie auf einen Parameter, der im selben Konto gespeichert ist:

      - **resolve:ssm:*parameter-name***
      - **resolve:ssm:*parameter-name*:*version-number***
      - **resolve:ssm:*parameter-name*:*label***

      So verweisen Sie auf einen von einem anderen AWS-Konto freigegebenen Parameter:

      - **resolve:ssm:*parameter-ARN***
      - **resolve:ssm:*parameter-ARN*:*version-number***
      - **resolve:ssm:*parameter-ARN*:*label***

   b. Wählen Sie Speichern.

7. Geben Sie nach Bedarf weitere Startvorlagenparameter an und wählen Sie dann Startvorlage erstellen aus.

Weitere Informationen finden Sie unter Startvorlage durch Angabe von Parametern erstellen.

AWS CLI

So geben Sie einen Systems-Manager-Parameter in einer Startvorlage an

- Verwenden Sie den create-launch-templateBefehl, um die Startvorlage zu erstellen. Um das zu verwendende AMI anzugeben, geben Sie den Systems-Manager-Parameternamen in einem der folgenden Formate ein:

  So verweisen Sie auf einen öffentlichen Parameter:

  - **resolve:ssm:*public-parameter***

  So verweisen Sie auf einen Parameter, der im selben Konto gespeichert ist:

  - **resolve:ssm:*parameter-name***
  - **resolve:ssm:*parameter-name*:*version-number***
  - **resolve:ssm:*parameter-name*:*label***

  So verweisen Sie auf einen von einem anderen AWS-Konto freigegebenen Parameter:

  - **resolve:ssm:*parameter-ARN***
  - **resolve:ssm:*parameter-ARN*:*version-number***
  - **resolve:ssm:*parameter-ARN*:*label***

  Das folgende Beispiel erstellt eine Startvorlage, die Folgendes festlegt:

  - Ein Name für die Startvorlage (*TemplateForWebServer*)
  - Ein Tag für die Launchvorlage (*purpose*=*production*)
  - Die Daten für die Instance-Konfiguration, die in einer JSON-Datei angegeben sind:
    - Das zu verwendende AMI (`resolve:ssm:`*golden-ami*)
    - Der zu startende Instance-Typ (*m5.4xlarge*)

- Ein Tag für die Instance (*Name*=*webserver*)

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

Im Folgenden finden Sie eine Beispiel-JSON-Datei, die die Launchvorlagen-Daten für die Instance-Konfiguration enthält. Der Wert für `ImageId` ist der Systems-Manager-Parametername, der im erforderlichen Format `resolve:ssm:golden-ami` eingegeben wird.

```
{"LaunchTemplateData": {
    "ImageId": "resolve:ssm:golden-ami",
    "InstanceType": "m5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }]
  }
}
```

Sicherstellen, dass eine Startvorlage die richtige AMI-ID erhält

So lösen Sie den Systems-Manager-Parameter in die tatsächliche AMI-ID auf

Verwenden Sie den describe-launch-template-versionsBefehl und fügen Sie den `--resolve-alias` Parameter hinzu.

```
aws ec2 describe-launch-template-versions \
    --launch-template-name my-launch-template \
    --versions $Default \
    --resolve-alias
```

Die Antwort enthält die AMI-ID für `ImageId`. Wenn in diesem Beispiel eine Instance mit dieser Startvorlage gestartet wird, wird die AMI-ID zu `ami-0ac394d6a3example` aufgelöst.

```
{
    "LaunchTemplateVersions": [
        {
            "LaunchTemplateId": "lt-089c023a30example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
            "CreateTime": "2022-12-28T19:52:27.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Bob",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0ac394d6a3example",
                "InstanceType": "t3.micro",
            }
        }
    ]
}
```

Zugehörige Ressourcen

Weitere Informationen zum Arbeiten mit Systems-Manager-Parametern finden Sie in den folgenden Referenzmaterialien in der Systems-Manager-Dokumentation.

- Informationen zum Nachschlagen der öffentlichen AMI-Parameter, die von Amazon unterstützt werden EC2, finden Sie unter Öffentliche AMI-Parameter aufrufen.
- Informationen zur gemeinsamen Nutzung von Parametern mit anderen AWS Konten oder über AWS Organizations finden Sie unter Arbeiten mit gemeinsam genutzten Parametern.
- Informationen zur Überwachung, ob Ihre Parameter erfolgreich erstellt wurden, finden Sie unter Native Parameterunterstützung für Amazon Machine Image IDs.

Einschränkungen

- Nur EC2 Flotten des Typs `instant` unterstützen die Verwendung einer Startvorlage, bei der anstelle einer AMI-ID ein Systems Manager Manager-Parameter angegeben ist.
- EC2 Flotten des Typs `maintain` und und `request` Spot-Flotten unterstützen nicht die Verwendung einer Startvorlage, bei der anstelle einer AMI-ID ein Systems Manager Manager-

Parameter angegeben ist. Wenn Sie für EC2 Flotten des Typs `maintain` und `request` und für Spot-Flotten ein AMI in der Startvorlage angeben, müssen Sie die AMI-ID angeben.

- Wenn Sie in Ihrer EC2 Flotte die attributbasierte Instance-Auswahl verwenden, können Sie keinen Systems Manager Manager-Parameter anstelle einer AMI-ID angeben. Wenn Sie die attributbasierte Instanceauswahl verwenden, müssen Sie die AMI-ID angeben.
- Amazon EC2 Auto Scaling bietet weitere Einschränkungen. Weitere Informationen finden Sie unter Verwenden von AWS Systems Manager Parametern anstelle von AMI IDs in Startvorlagen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Ändern einer Startvorlage (Verwalten von Startvorlagenversionen)

Startvorlagen sind unveränderlich; nach der Erstellung einer Startvorlage können Sie sie nicht ändern. Stattdessen können Sie eine neue Version der Startvorlage erstellen, die alle erforderlichen Änderungen enthält.

Sie können verschiedene Versionen einer Startvorlage erstellen, die Standardversion festlegen, eine Startvorlagenversion beschreiben und nicht mehr benötigte Versionen löschen.

Aufgaben

- Erstellen einer Startvorlagenversion
- Festlegen einer Standardversion der Startvorlage
- Beschreiben einer Startvorlagenversion

Erstellen einer Startvorlagenversion

Wenn Sie eine Startvorlagenversion erstellen, können Sie neue Startparameter angeben oder eine vorhandene Version als Grundlage für die neue Version verwenden. Eine Beschreibung jedes Parameters finden Sie unter Referenz für EC2 Amazon-Instance-Konfigurationsparameter.

Console

So erstellen Sie eine Startvorlagenversion

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates aus.
3. Wählen Sie eine Startvorlage aus, und wählen Sie dann Actions (Aktionen), Modify template (Create new version) ((Vorlage ändern) (Neue Version erstellen)).

4. Geben Sie unter Template version description (Beschreibung der Vorlagenversion) eine Beschreibung für diese Version der Startvorlage ein.
5. (Optional) Erweitern Sie die Source template (Quellvorlage) und wählen Sie eine Version der Startvorlage aus, die als Basis für die neue Version der Startvorlage dienen soll. Die neue Startvorlagenversion erbt die Startparameter von dieser Startvorlagenversion.
6. Ändern Sie die Startparameter nach Bedarf.
7. Wählen Sie Startvorlage erstellen.

AWS CLI

So erstellen Sie eine Startvorlagenversion

Verwenden Sie den Befehl create-launch-template-version. Sie können eine Quellversion angeben, auf der die neue Version basieren soll. Die neue Startvorlagenversion erbt die Startparameter von dieser Startvorlagenversion und Sie können mit `--launch-template-data` Parameter überschreiben. Das folgende Beispiel erstellt eine neue Version, die auf Version 1 der Startvorlage basiert und eine andere AMI-ID angibt.

```
aws ec2 create-launch-template-version \
    --launch-template-id lt-0abcd290751193123 \
    --version-description WebVersion2 \
    --source-version 1 \
    --launch-template-data "ImageId=ami-0abcdef1234567890"
```

PowerShell

So erstellen Sie eine Startvorlagenversion

Verwenden Sie das New-EC2LaunchTemplateVersionCmdlet. Sie können eine Quellversion angeben, auf der die neue Version basieren soll. Die neue Startvorlagenversion erbt die Startparameter von dieser Startvorlagenversion und Sie können mit `LaunchTemplateData` Parameter überschreiben. Das folgende Beispiel erstellt eine neue Version, die auf Version 1 der Startvorlage basiert und eine andere AMI-ID angibt.

```
New-EC2LaunchTemplateVersion `
    -LaunchTemplateId lt-0abcd290751193123 `
    -VersionDescription WebVersion2 `
    -SourceVersion 1 `
```

```
    -LaunchTemplateData (
        New-Object `
            -TypeName Amazon.EC2.Model.RequestLaunchTemplateData `
            -Property @{ImageId = 'ami-0abcdef1234567890'}
    )
```

Festlegen einer Standardversion der Startvorlage

Sie können die Standardversion für die Startvorlage festlegen. Wenn Sie eine Instance über eine Startvorlage starten, ohne eine Version anzugeben, wird die Instance unter Verwendung der Parameter der Standardversion gestartet.

Console

So legen Sie eine Standardversion der Startvorlage fest

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates aus.
3. Wählen Sie die Startvorlage und anschließend Actions (Aktionen), Set default version (Standardversion festlegen) aus.
4. Wählen Sie unter Template version (Vorlagenversion) die Versionsnummer aus, die als Standardversion festgelegt werden soll, und wählen Sie Set as default version (Als Standardversion festlegen).

AWS CLI

So legen Sie eine Standardversion der Startvorlage fest

Verwenden Sie den Befehl modify-launch-template.

```
aws ec2 modify-launch-template \
    --launch-template-id lt-0abcd290751193123 \
    --default-version 2
```

PowerShell

So legen Sie eine Standardversion der Startvorlage fest

Verwenden Sie das cmdlet Edit-EC2LaunchTemplate.

```
Edit-EC2LaunchTemplate `
    -LaunchTemplateId lt-0abcd290751193123 `
    -DefaultVersion 2
```

Beschreiben einer Startvorlagenversion

Über die Konsole können Sie alle Versionen der ausgewählten Startvorlage anzeigen oder eine Liste der Startvorlagen abrufen, deren neueste Version oder Standardversion mit einer bestimmten Versionsnummer übereinstimmt. Mithilfe von können Sie alle Versionen, einzelne Versionen oder eine Reihe von Versionen einer bestimmten Startvorlage beschreiben. AWS CLI Sie können auch alle aktuellen Versionen oder alle Standardversionen aller Startvorlagen in Ihrem Konto beschreiben.

Console

So beschreiben Sie eine Startvorlagenversion

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates aus.
3. Sie können eine Version einer bestimmten Startvorlage anzeigen oder eine Liste der Startvorlagen abrufen, deren neueste Version oder Standardversion mit einer bestimmten Versionsnummer übereinstimmt.
   - So zeigen Sie eine Version einer Startvorlage an: Wählen Sie die Startvorlage aus. Wählen Sie auf der Registerkarte Versionen unter Version eine Version aus, um deren Details anzuzeigen.
   - So rufen Sie eine Liste aller Startvorlagen ab, deren neueste Version mit einer bestimmten Versionsnummer übereinstimmt: Wählen Sie in der Suchleiste die Option Aktuelle Version aus und wählen Sie dann eine Versionsnummer aus.
   - So rufen Sie eine Liste aller Startvorlagen ab, deren Standardversion mit einer bestimmten Versionsnummer übereinstimmt: Wählen Sie in der Suchleiste die Option Standardversion aus und wählen Sie dann eine Versionsnummer aus.

AWS CLI

So beschreiben Sie eine Startvorlagenversion

Verwenden Sie den describe-launch-template-versionsBefehl und geben Sie die Versionsnummern an. Im folgenden Beispiel werden die Versionen *1* und *3* angegeben.

```
aws ec2 describe-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1 3
```

So beschreiben Sie die neuesten und standardmäßigen Versionen der Startvorlagen in Ihrem Konto

Verwenden Sie den describe-launch-template-versionsBefehl und geben Sie `$Latest``$Default`, oder beides an. Sie müssen die Startvorlagen-ID und den Namen in dem Aufruf weglassen. Sie können keine Versionsnummern angeben.

```
aws ec2 describe-launch-template-versions \
    --versions "$Latest,$Default"
```

PowerShell

So beschreiben Sie eine Startvorlagenversion

Verwenden Sie das Get-EC2TemplateVersionCmdlet und geben Sie die Versionsnummern an. Im folgenden Beispiel werden die Versionen *1* und *3* angegeben.

```
Get-EC2TemplateVersion `
    -LaunchTemplateId lt-0abcd290751193123 `
    -Version 1,3
```

So beschreiben Sie die neuesten und standardmäßigen Versionen der Startvorlagen in Ihrem Konto

Verwenden Sie das Get-EC2TemplateVersionCmdlet und geben Sie`$Latest`, `$Default` oder beides an. Sie müssen die Startvorlagen-ID und den Namen in dem Aufruf weglassen. Sie können keine Versionsnummern angeben.

```
Get-EC2TemplateVersion `
    -Version '$Latest','$Default'
```

Eine Startvorlage oder Startvorlagenversion löschen

Wenn eine Startvorlage nicht mehr benötigt wird, können Sie sie löschen. Beim Löschen einer Startvorlage werden alle ihre Versionen gelöscht. Wenn Sie nur eine bestimmte Version einer

Startvorlage löschen möchten, können Sie dies tun und dabei die anderen Versionen der Startvorlage beibehalten.

Das Löschen einer Startvorlage wirkt sich das nicht auf Instances aus, die Sie über die Startvorlage gestartet haben.

Eine Startvorlage und alle ihre Versionen löschen

Wenn eine Startvorlage, einschließlich aller ihrer Versionen, nicht mehr benötigt wird, können Sie die Startvorlage löschen. Beim Löschen einer Startvorlage werden alle ihre Versionen gelöscht.

Console

So löschen Sie eine Startvorlage und alle ihre Versionen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates aus.
3. Wählen Sie die Startvorlage und anschließend Actions (Aktionen), Delete template (Vorlage löschen) aus.
4. Geben Sie **`Delete`** ein, um das Löschen zu bestätigen, und wählen Sie dann Löschen.

AWS CLI

So löschen Sie eine Startvorlage und alle ihre Versionen

Verwenden Sie den delete-launch-templateBefehl und geben Sie die Startvorlage an.

```
aws ec2 delete-launch-template --launch-template-id lt-01238c059e3466abc
```

PowerShell

So löschen Sie eine Startvorlage und alle ihre Versionen

Verwenden Sie den Befehl Remove-EC2LaunchTemplate(AWS -Tools für PowerShell) und geben Sie die Startvorlage an. Wenn `-Force` es weggelassen wird, PowerShell werden Sie zur Bestätigung aufgefordert.

```
Remove-EC2LaunchTemplate -LaunchTemplateId lt-0123456789example -Force
```

Löschen einer Startvorlagenversion

Wenn eine Startvorlagenversion nicht mehr benötigt wird, können Sie sie löschen.

Überlegungen

- Sie können die Versionsnummer nach dem Löschen nicht mehr ersetzen.
- Sie können die Standardversion der Startvorlage nicht löschen. Sie müssen zunächst eine andere Version als Standard zuweisen. Wenn die Standardversion die einzige Version für die Startvorlage ist, müssen Sie die gesamte Startvorlage löschen.
- Bei Verwendung der Konsole können Sie jeweils eine Startvorlagenversion löschen. Wenn Sie den verwenden AWS CLI, können Sie bis zu 200 Versionen der Startvorlage in einer einzigen Anfrage löschen. Um mehr als 200 Versionen in einer einzigen Anfrage zu löschen, können Sie die Startvorlage löschen, wodurch auch alle zugehörigen Versionen gelöscht werden.

Console

So löschen Sie eine Startvorlagenversion

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates aus.
3. Wählen Sie die Startvorlage und anschließend Actions (Aktionen), Delete template version (Vorlagenversion löschen) aus.
4. Wählen Sie die zu löschende Version aus und wählen Sie Delete (Löschen).

AWS CLI

So löschen Sie eine Startvorlagenversion

Verwenden Sie den delete-launch-template-versionsBefehl und geben Sie die Versionsnummern an, die gelöscht werden sollen. Wenn Sie die verwenden, können Sie bis zu 200 Startvorlagenversionen in einer einzigen Anfrage löschen.

```
aws ec2 delete-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1
```

PowerShell

So löschen Sie eine Startvorlagenversion

Verwenden Sie das Remove-EC2TemplateVersionCmdlet und geben Sie die Versionsnummern an, die gelöscht werden sollen. Wenn Sie die verwenden, können Sie bis zu 200 Startvorlagenversionen in einer einzigen Anfrage löschen.

```
Remove-EC2TemplateVersion `
    -LaunchTemplateId lt-0abcd290751193123 `
    -Version 1
```

Starten Sie eine EC2 Amazon-Instance

Eine Instanz ist ein virtueller Server in der AWS Cloud. Sie starten eine Instance von einem Amazon Machine Image (AMI) aus. Das AMI stellt das Betriebssystem, den Anwendungsserver und Anwendungen für Ihre Instance bereit.

Wenn Sie Ihre erstellen AWS-Konto, können Sie EC2 kostenlos mit Amazon beginnen, indem Sie die verwenden Kostenloses AWS-Kontingent. Die Vorteile des kostenlosen Kontingents hängen davon ab, wann Sie Ihr AWS-Konto erstellt haben. Wenn Sie Ihr AWS-Konto vor dem 15. Juli 2025 erstellt haben und das Konto weniger als 12 Monate alt ist, können Sie das kostenlose Kontingent verwenden, um eine `t2.micro`-Instance kostenlos zu starten und zu verwenden (in Regionen, in denen `t2.micro` nicht verfügbar ist, können Sie eine `t3.micro`-Instance im Rahmen des kostenlosen Kontingents verwenden).Es fallen für Ihre Instance oder Nutzung Gebühren an, die auf die Limits Ihres kostenlosen -Kontingents angerechnet werden, während die Instance ausgeführt wird. Weitere Informationen finden Sie unter EC2 Amazon-Preise. Wenn Sie Ihr AWS-Konto am oder nach dem 15. Juli 2025 erstellt haben, können Sie die Instance-Typen `t3.micro`, `t3.small`, `t4g.micro`, `t4g.small`, `c7i-flex.large` und `m7i-flex.large` 6 Monate lang verwenden oder bis Ihr Guthaben aufgebraucht ist. Weitere Informationen finden Sie unter Vorteile des kostenlosen Kontingents vor und nach dem 15. Juli 2025.

Wenn Sie die Instance starten, können Sie die Instance in einem Subnetz starten, das einer der folgenden Ressourcen zugeordnet ist:

- Eine Availability Zone – diese Option ist die Standardeinstellung.

- Eine Local Zone – Um eine Instance in einer Local Zone zu starten, müssen Sie sich bei der Local Zone anmelden und dann ein Subnetz in der Zone erstellen. Weitere Informationen finden Sie unter Erste Schritte mit Local Zones.
- Eine Wavelength-Zone – Um eine Instance in einer Wavelength-Zone zu starten, müssen Sie sich für die Wavelength-Zone anmelden und dann ein Subnetz in der Zone erstellen. Weitere Informationen zum Starten einer Instance in einer Wavelength-Zone finden Sie unter Erste Schritte mit AWS Wavelength.
- Einem Outpost – um eine Instance in einem Outpost zu starten, müssen Sie einen Outpost erstellen. Informationen zum Erstellen eines Outposts finden Sie unter Erste Schritte mit AWS Outposts.

Nachdem Sie Ihre Instance gestartet haben, können Sie eine Verbindung zu ihr herstellen und sie verwenden. Zu Beginn lautet der Status der Instance `pending`. Wenn der Status der Instance `running` lautet, hat die Instance mit dem Hochfahren begonnen. Es kann möglicherweise kurz dauern, bis Sie eine Verbindung zur Instance herstellen können. Beachten Sie, dass der Start von Bare Metal-Instance-Typen möglicherweise länger dauern kann.

Je nachdem, wie Sie eine Verbindung zu Ihrer Instance planen, sollten Sie beim Starten Ihrer Instance möglicherweise bestimmte Konfigurationen vornehmen. Diese Konfigurationen könnten die Angabe von Sicherheitsgruppenregeln für eingehenden Datenverkehr oder die Zuweisung einer Instance-Profil-Rolle beinhalten. Weitere Informationen zu den Verbindungsmethoden, mit denen Sie eine Verbindung herstellen können, und zu den jeweiligen Anforderungen finden Sie unter Connect zu Ihrer EC2 Instance her.

Die Instance erhält einen öffentlichen DNS-Namen, den Sie verwenden können, um über das Internet auf die Instance zuzugreifen. Außerdem erhält die Instance einen privaten DNS-Namen, den andere Instances innerhalb desselben VPC zum Herstellen der Verbindung zur Instance verwenden können.

Wenn Sie eine Instance nicht mehr benötigen, müssen Sie sie beenden, um unnötige Kosten zu vermeiden. Weitere Informationen finden Sie unter EC2 Amazon-Instances beenden.

Die folgenden Methoden sind einige der Möglichkeiten, wie Sie eine Instance starten können.

Methode	Tool	Dokumentation
Verwenden Sie den Launch Instance Wizard zur Angabe der Startparameter.	EC2 Amazon-Konsole	EC2-Instance mit dem Launch Instance Wizard in der Konsole starten
Erstellen Sie eine Startvorlage und starten Sie die Instance über die Startvorlage.	EC2 Amazon-Konsole	Starten Sie EC2 Instances mithilfe einer Startvorlage
Verwenden Sie eine vorhandene Instance als Basis.	EC2 Amazon-Konsole	Starten Sie eine EC2 Instance mit Details aus einer vorhandenen Instance
Verwenden Sie ein im AWS Marketplace erworbenes AMI.	EC2 Amazon-Konsole	Starten einer Amazon-EC 2-Instance von einem AWS Marketplace-AMI
Verwenden Sie ein von Ihnen angegebenes AMI.	AWS CLI	EC2 Amazon-Instances starten, auflisten und löschen in der AWS CLI
Verwenden Sie ein von Ihnen angegebenes AMI.	AWS Tools for Windows PowerShell	Starten Sie eine EC2 Amazon-Instance mit Windows PowerShell
Verwenden Sie EC2 Fleet, um Kapazität für verschied ene EC2 Instance-Typen und Availability Zones sowie für die Kaufoptionen On-Demand -Instance, Reserved Instance und Spot-Instance bereitzus tellen.	AWS CLI	EC2 Flotte und Spot-Flotte
Verwenden Sie eine CloudFormation Vorlage, um eine Instanz anzugeben.	AWS CloudFormation	AWS::EC2::Instance im AWS CloudFormation -Benutzer handbuch

Methode	Tool	Dokumentation
Verwenden Sie ein sprachspezifisches AWS SDK, um eine Instanz zu starten.	AWS SDK	AWS SDK for .NET AWS SDK for C++ AWS SDK for Go AWS SDK für Java AWS SDK für JavaScript AWS SDK for PHP V3 AWS SDK für Python AWS SDK for Ruby V3

Tutorials zum Starten von EC2-Instances

Es gibt verschiedene Methoden, um eine Amazon-EC2-Instance zu starten und zu konfigurieren. Die Methode und Konfiguration, die Sie verwenden, hängen von Ihrem speziellen Anwendungsfall ab.

In den folgenden Tutorials erfahren Sie, wie Sie EC2-Instances starten. Wenn Amazon EC2 neu für Sie ist, empfehlen wir Ihnen, mit dem ersten Tutorial zu beginnen. Die Tutorials beginnen mit einer Einführung in die Grundlagen und helfen Ihnen, auf den Grundlagen aufzubauen, indem weitere Konfigurationsoptionen vorgestellt werden.

Ziel	Link zum Tutorial
Meine allererste EC2-Instance starten Erfahren Sie, wie Sie eine Amazon-EC2-Instance mithilfe der Standardeinstellungen im Launch Instance Wizard von Amazon-EC2 schnell starten. Erfahren Sie auch, wie Sie die Felder für die Instance-Konfiguration überprüfen und die Instance beenden.	Tutorial 1: Starten meiner allerersten Amazon-EC2-Instance

Ziel	Link zum Tutorial
Dauer: 10 Minuten	
Starten Sie eine Test-EC2-Instance und stellen Sie eine Verbindung zu ihr her So starten Sie eine Amazon-EC2 Instance, die Sie zu Testzwecken verwenden können. Diese Instance hat keine erweiterte Konfiguration und speichert keine vertraulichen Informationen. Außerdem erfahren Sie mehr über die grundlegenden Einstellungen für die Instancekonfiguration und darüber, wie Sie eine Verbindung zur Instance herstellen und wie Sie sie beenden können. Dauer: 30 Minuten	Tutorial 2: Starten einer EC2-Test-Instance und Verbindung zu ihr herstellen

Suchen Sie nach anderen Tutorials?

- Tutorial: Installieren eines LAMP-Webservers in AL2023
- Tutorial: SSL/TLS in AL2023 konfigurieren
- Tutorial: Hosten eines WordPress-Blogs in AL2023
- Tutorial: Vervollständigen Sie die Konfiguration, die für die Verbindung mit Ihrer Instance mithilfe von EC2 Instance Connect erforderlich ist
- Tutorial: Verbinden einer Amazon-EC2-Instance mit einer Amazon-RDS-Datenbank

Tutorial 1: Starten meiner allerersten Amazon-EC2-Instance

Tutorial-Ziel	Erfahren Sie, wie Sie eine Amazon-EC2-Instance mithilfe der Standardeinstellungen im Launch Instance Wizard von Amazon-EC2 schnell starten. Erfahren Sie auch, wie Sie die

	Felder für die Instance-Konfiguration überprüfen und die Instance beenden.
EC2-Erfahrung	Einsteiger
Dauer	10 Minuten

Kosten	Für das kostenlose Kontingent berechtigt Wenn Sie Ihr AWS-Konto erstellen, können Sie kostenlos mit der Verwendung von Amazon EC2 beginnen, indem Sie das Kostenloses AWS-Kontingent nutzen. Wenn Sie Ihr AWS-Konto vor dem 15. Juli 2025 erstellt haben und das Konto weniger als 12 Monate alt ist, und Sie das kostenlose Kontingent für Amazon EC2 noch nicht ausgeschöpft haben, ist das Absolvieren dieses Tutorials für Sie kostenlos, da wir Ihnen helfen, Optionen auszuwählen, die in das kostenlose Kontingent fallen. Andernfalls fallen die üblichen Amazon-EC2-Nutzungsgebühren an, und zwar ab dem Zeitpunkt, an dem Sie die Instance starten (auch wenn sie im Leerlauf bleibt), bis Sie sie beenden. Wenn Sie Ihr AWS-Konto vor dem 15. Juli 2025 erstellt haben und das Konto weniger als 6 Monate alt ist, und Sie Ihr Guthaben noch nicht ausgeschöpft haben, ist das Absolvieren dieses Tutorials für Sie kostenlos, da wir Ihnen helfen, Optionen auszuwählen, die in das kostenlose Kontingent fallen. Informationen darüber, wie Sie feststellen können, ob Sie für das kostenlose Kontingent in Frage kommen, finden Sie unter the section called “Ihre Nutzung des kostenlosen Kontingents nachverfolgen”.

Voraussetzungen	• Sie müssen über ein AWS Konto verfügen, einen Benutzer mit Administratorzugriff konfigurieren und sich mit dem Administr atorbenutzer bei AWS-Managementkons ole anmelden. Sie sind sich nicht sicher, wie das geht? Probieren Sie dieses Tutorial aus: Einrichtung Ihrer AWS-Umgebung • Sie müssen mit der AWS-Konsole allgemein vertraut sein. Sie sind sich nicht sicher, wo Sie anfangen sollen? Probieren Sie diesen Leitfaden für die ersten Schritte aus: Erste Schritte mit dem AWS-Managementkonsole

Tutorial-Übersicht

Dieses Tutorial richtet sich an Anfänger ohne vorherige Erfahrung mit Amazon EC2. Wir führen Sie durch die Schritte zum Erstellen – wir nennen das Starten – Ihrer allerersten EC2-Instance mithilfe der EC2-Konsole. Eine Instance ist im Grunde ein Webserver in der AWS Cloud. Nachdem Sie Ihre Instance gestartet haben, zeigen wir Ihnen, wie Sie sie in der Konsole finden. Um Ihnen bei der Kostenkontrolle zu helfen, zeigen wir Ihnen abschließend, wie Sie Ihre Instance löschen – wir nennen das Beenden.

Diese Anleitung ist in die folgenden kurzen Schritte unterteilt. Sie müssen jede Aufgabe abschließen, bevor Sie mit der nächsten fortfahren können.

- Aufgabe 1: Ihre Instance starten
- Aufgabe 2: Ihre Instance finden
- Aufgabe 3: Ihre Instance-Konfiguration anzeigen
- Schritt 4: Ihre Instance beenden

Aufgabe 1: Ihre Instance starten

In dieser Aufgabe gehen Sie am schnellsten zum Starten Ihrer Instance vor, indem Sie nur das Wesentliche erledigen. Wir verwenden den Launch Instance Wizard von EC2, ein webbasiertes Formular, das alle Felder für die Konfiguration und den Start Ihrer Instance enthält. Es vereinfacht den Prozess, indem es Standardwerte für die Instance-Konfigurationsfelder bereitstellt.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie die in der obigen Tabelle aufgeführten Voraussetzungen erfüllt haben, einschließlich der Anmeldung in der AWS-Managementkonsole mit Ihrem Administratorbenutzer.

Führen Sie die folgenden Schritte aus, um Ihre Instance schnell zu starten

1. Öffnen Sie die Amazon-EC2-Konsole:

   Gehen Sie zu https://console.aws.amazon.com/ec2/.

2. Öffnen Sie den EC2-Launch-Instance-Wizard:

   Wählen Sie im EC2-Dashboard Instance starten aus.

   Das webbasierte Formular Eine Instance starten wird geöffnet. Das ist der Launch Instance Wizard von EC2.

3. Benennung Ihrer Instance:

   Geben Sie unter Name und Tags bei Name einen beschreibenden Namen wie **`My first EC2 instance`** ein.

   Die Benennung Ihrer Instance ist zwar nicht erforderlich, hilft aber dabei, Ihre Instance später zu identifizieren.

4. Ohne Schlüsselpaar fortfahren:

   Wählen Sie unter Schlüsselpaar (Anmeldung) für Name des Schlüsselpaars die Option Ohne Schlüsselpaar fortfahren (nicht empfohlen) aus.

   Ein Schlüsselpaar kann für die sichere Anmeldung verwendet werden. Da wir uns in diesem Tutorial jedoch nicht bei der Instance anmelden, benötigen Sie vorerst kein Schlüsselpaar.

5. Starten Ihrer Instance:

   Wählen Sie im Bereich Summary (Zusammenfassung) rechts Launch instance (Instance starten) aus.

   Amazon EC2 startet Ihre Instance schnell mit den Standardeinstellungen. Ein Erfolgsbanner bestätigt den Start.

Herzlichen Glückwunsch!Sie haben Ihre allererste EC2-Instance erfolgreich gestartet!

Aufgabe 2: Ihre Instance finden

In dieser Aufgabe lokalisieren Sie die Instance, die Sie gerade in der EC2-Konsole gestartet haben.

Gehen Sie wie folgt vor, um Ihre Instance in der EC2-Konsole zu finden

1. Öffnen Sie die Instances-Seite:

   Wenn Sie sich immer noch auf der Erfolgsseite befinden, wählen Sie im Breadcrumb oben auf dem Bildschirm Instances aus. Möglicherweise müssen Sie zuerst die drei Ellipsen wählen, um darauf zuzugreifen.

   Wenn Sie die Seite verlassen haben, wählen Sie im Navigationsbereich Instances aus.
2. Ihre Instance suchen:

   Suchen Sie in der Spalte Name Ihre Instance anhand des Namens, den Sie ihr gegeben haben.

Aufgabe 3: Ihre Instance-Konfiguration anzeigen

In dieser Aufgabe machen Sie sich mit der Anzeige der Konfigurationsdetails Ihrer Instance vertraut.

Gehen Sie folgendermaßen vor, um die Konfiguration Ihrer Instance anzuzeigen

1. Lokalisieren Sie die Instance-ID:

   Notieren Sie sich in der Spalte Instance-ID die eindeutige ID Ihrer Instance. Sie beginnt mit i–, gefolgt von 17 alphanumerischen Zeichen, zum Beispiel i-01aeed690c9fb5322.

   Die Instance-ID wird Ihrer Instance automatisch zugewiesen, wenn sie gestartet wird.
2. Öffnen Sie die Seite mit den Instance-Details:

   Wählen Sie in der Spalte Instance-ID den ID-Link aus, um die Seite mit den Instance-Details zu öffnen, auf der Sie die Konfiguration überprüfen können.
3. Erkunden Sie die Einzelheiten der Instance-Konfiguration:

   Nehmen Sie sich ein paar Minuten Zeit, um die Konfigurationsdetails Ihrer Instance zu erkunden. Im nächsten Tutorial werden wir uns eingehender mit der Konfiguration befassen. Nutzen Sie diese Zeit zunächst, um sich mit der Seite mit den Instance-Details vertraut zu machen.

   Tipp: Um schnell ein Feld zu finden, drücken Sie Strg+F oder Befehlstaste+F auf Ihrer Tastatur.

a. Instance-Typ: Können Sie den Instance-Typ finden? Es könnte zum Beispiel t3.micro sein.

b. Öffentliche IPv4-Adresse: Können Sie die öffentliche IPv4-Adresse finden, die Ihrer Instance zugewiesen wurde? Sie hat ein Format, das dem folgenden Beispiel ähnelt: 34.242.148.128.

c. Instance-Besitzer: Können Sie den Besitzer dieser Instance identifizieren? Sie sind es! Ihre AWS-Konto-Nummer ist im Feld Eigentümer aufgeführt.

d. Instance-Tags: Der Name, den Sie Ihrer Instance gegeben haben, ist eigentlich ein Tag. Können Sie Ihre Instance-Tags finden? Wählen Sie die Registerkarte Tags aus. Der Schlüssel ist Name, und der Wert ist der Name, den Sie angegeben haben.

e. Startzeit: Können Sie herausfinden, wann Sie Ihre Instance gestartet haben? Wählen Sie die Registerkarte Details aus und suchen Sie das Feld Startzeit.

f. Instance-Status: Können Sie den Status Ihrer Instance überprüfen? Sie sollte Wird ausgeführt sein.

Nehmen Sie sich ein paar Minuten Zeit, um die Konfigurationsdetails Ihrer Instance zu erkunden. Wenn Sie bereit sind, fortzufahren, gehen Sie zur nächsten Aufgabe.

Schritt 4: Ihre Instance beenden

> **Warning**
>
> Das Beenden einer Instance ist dauerhaft und irreversibel.
> Nachdem Sie eine Instance beendet haben, können Sie keine Verbindung mehr zu ihr herstellen und sie kann nicht wiederhergestellt werden. Alle angehängten Amazon-EBS-Volumes, die so konfiguriert sind, dass sie beim Beenden gelöscht werden, werden ebenfalls dauerhaft gelöscht und können nicht wiederhergestellt werden. Alle auf den Instance-Speicher-Volumes gespeicherten Daten gehen dauerhaft verloren. Weitere Informationen finden Sie unter Wie die Kündigung von Instances funktioniert.
> Bevor Sie eine Instance beenden, stellen Sie sicher, dass Sie alle Daten, die Sie nach der Beendigung behalten müssen, im persistenten Speicher gesichert haben.

In dieser Aufgabe löschen Sie Ihre Instance, um die Vorteile des kostenlosen Kontingents beizubehalten. In EC2 ist Beenden der Begriff, der für das Löschen einer Instance verwendet wird.

Gehen Sie wie folgt vor, um Ihre Instance zu beenden

1. Beendigung einleiten:

   Wenn Sie sich immer noch auf der Seite mit den Instance-Details befinden, wählen Sie das Menü Instance-Status (oben rechts) und dann Instance beenden (löschen).

   Wenn Sie die Seite verlassen haben, wählen Sie im Navigationsbereich Instances aus. Aktivieren Sie dann auf der Seite Instances das Kontrollkästchen neben dem Namen Ihrer Instance, wählen Sie dann das Menü Instance-Status (oben rechts) und wählen Sie Instance beenden (löschen) aus.
2. Bestätigen Sie die Beendigung:

   Wählen Sie im sich öffnenden Fenster Instance beenden (löschen) die Schaltfläche Beenden (löschen), um zu bestätigen, dass Sie Ihre Instance beenden möchten.
3. Instance-Status überwachen:

   Überprüfen Sie auf der Seite Instances die Spalte Instance-Status. Der Status Ihrer Instance ändert sich in Fährt herunter. Wenn Sie nicht den vollständigen Text sehen, versuchen Sie, die Spalte zu erweitern.

   Sobald die Instance heruntergefahren wurde, löscht Amazon EC2 die Instance und sie verschwindet von der Instance-Seite.

Die wichtigsten Erkenntnisse

In diesem Tutorial haben Sie die folgenden Schlüsselkonzepte behandelt:

- Instance bezieht sich auf einen Amazon-EC2-Webserver in der AWS Cloud.
- Start bezieht sich auf die Erstellung einer EC2-Instance.
- Beenden bezieht sich auf das Löschen einer EC2-Instance.
- Der Launch Instance Wizard von EC2 enthält Standardwerte für die Instance-Konfiguration, die einen schnellen und einfachen Instance-Start ermöglichen.
- Die Instance-ID ist eine eindeutige Kennung, die Ihrer Instance automatisch zugewiesen wird, während der Instance-Name ein optionales Tag ist, das Sie zur leichteren Identifizierung zuweisen können.

Nächste Schritte

Um Vertrauen beim Starten und Beenden von Instances aufzubauen, sollten Sie die Schritte in diesem Tutorial wiederholen. Stellen Sie sicher, dass Sie alle Instances, die Sie starten, beenden, um die Vorteile des kostenlosen Kontingents beizubehalten.

Sobald Sie mit diesen Grundlagen vertraut sind, fahren Sie mit dem nächsten Tutorial fort, das einen tieferen Einblick in die wichtigsten Felder der Instance-Konfiguration bietet.

Tutorial 2: Starten einer EC2-Test-Instance und Verbindung zu ihr herstellen

Tutorial-Ziel	So starten Sie eine Amazon-EC2-Instance, die Sie zu Testzwecken verwenden können. Diese Instance hat keine erweiterte Konfiguration und speichert keine vertraulichen Informationen. Außerdem erfahren Sie mehr über die grundlegenden Einstellungen für die Instancekonfiguration und darüber, wie Sie eine Verbindung zur Instance herstellen und wie Sie sie beenden können.
EC2-Erfahrung	Einsteiger
Dauer	30 Minuten
Kosten	Für das kostenlose Kontingent berechtigt Wenn Sie Ihr AWS-Konto erstellen, können Sie kostenlos mit der Verwendung von Amazon EC2 beginnen, indem Sie das Kostenloses AWS-Kontingent nutzen. Wenn Sie Ihr AWS-Konto vor dem 15. Juli 2025 erstellt haben und das Konto weniger als 12 Monate alt ist, und Sie das kostenlose Kontingent für Amazon EC2 noch nicht ausgeschöpft haben, ist das Absolvieren dieses Tutorials für Sie kostenlos, da wir Ihnen helfen, Optionen auszuwählen, die in das kostenlos

	e Kontingent fallen. Andernfalls fallen die üblichen Amazon-EC2-Nutzungsgebühren an, und zwar ab dem Zeitpunkt, an dem Sie die Instance starten (auch wenn sie im Leerlauf bleibt), bis Sie sie beenden. Wenn Sie Ihr AWS-Konto vor dem 15. Juli 2025 erstellt haben und das Konto weniger als 6 Monate alt ist, und Sie Ihr Guthaben noch nicht ausgeschöpft haben, ist das Absolvier en dieses Tutorials für Sie kostenlos, da wir Ihnen helfen, Optionen auszuwählen, die in das kostenlose Kontingent fallen. Informationen darüber, wie Sie feststellen können, ob Sie für das kostenlose Kontingen t in Frage kommen, finden Sie unter the section called “Ihre Nutzung des kostenlosen Kontingents nachverfolgen”.
Voraussetzungen	Schließen Sie ab Tutorial 1: Starten meiner allerersten Amazon-EC2-Instance.

Tutorial-Übersicht

Dieses Tutorial richtet sich an Einsteiger, die eine EC2-Instance starten möchten, die sie zu Testzwecken verwenden können.

Wir erklären die wichtigsten Felder für die Instance-Konfiguration und führen Sie anschließend durch die Schritte zum Starten einer Test-Instance mithilfe der Standardwerte in der EC2-Konsole. Nach dem Start Ihrer Instance zeigen wir Ihnen, wie Sie sich bei Ihrer Instance anmelden – wir nennen das Verbindung zu – Ihrer Instance. In diesem Tutorial zeigen wir Ihnen auch, wie Sie ein Schlüsselpaar erstellen, das für die Verbindung mit Ihrer Instance erforderlich ist. Abschließend zeigen wir Ihnen, wie Sie Ihre Instance beenden können, um Nutzungsgebühren zu vermeiden.

In diesem Tutorial starten Sie eine Linux-Instance. Die Schritte in diesem Tutorial können zwar zum Starten von Instances mit anderen Betriebssystemen verwendet werden, die Anweisungen zum Herstellen einer Verbindung zu einer Instance sind jedoch spezifisch für Linux-Instances.

Diese Anleitung ist in die folgenden kurzen Schritte unterteilt. Sie müssen jede Aufgabe abschließen, bevor Sie mit der nächsten fortfahren können.

- Aufgabe 1: Machen Sie sich mit den wichtigsten Komponenten für den Start einer Instance vertraut
- Aufgabe 2: Ein technisches Diagramm überprüfen
- Schritt 3: Erstellen eines Schlüsselpaares
- Aufgabe 4: Ihre Test-Instance starten
- Aufgabe 5: Ihre Instance finden
- Aufgabe 6: Anzeigen Ihrer Instance-Konfiguration
- Aufgabe 7: Machen Sie sich mit den wichtigsten Komponenten für die Verbindung zu einer Instance vertraut
- Aufgabe 8: Verbindung mit Ihrer Instance herstellen
- Aufgabe 9: Ihre Instance anhalten

Aufgabe 1: Machen Sie sich mit den wichtigsten Komponenten für den Start einer Instance vertraut

In dieser Aufgabe erkunden Sie die wichtigsten Komponenten, die zum Starten einer EC2-Instance erforderlich sind. Dies sind das AMI, der Instance-Typ, ein Schlüsselpaar, die Sicherheitsgruppe, das Netzwerk (VPC und Subnetz) und das Amazon-EBS-Volume. Sie werden sich auch mit einer optionalen Komponente, dem Name-Tag, befassen.

Stellen Sie sich zur besseren Veranschaulichung dieser Komponenten eine Instance wie ein Miethaus vor. So wie Sie durch die Anmietung eines Hauses eine Wohnung erhalten, ohne dass Sie die Immobilie besitzen und verwalten müssen, bieten EC2-Instances Rechenleistung, ohne dass Sie die zugrunde liegende Infrastruktur besitzen und verwalten müssen.

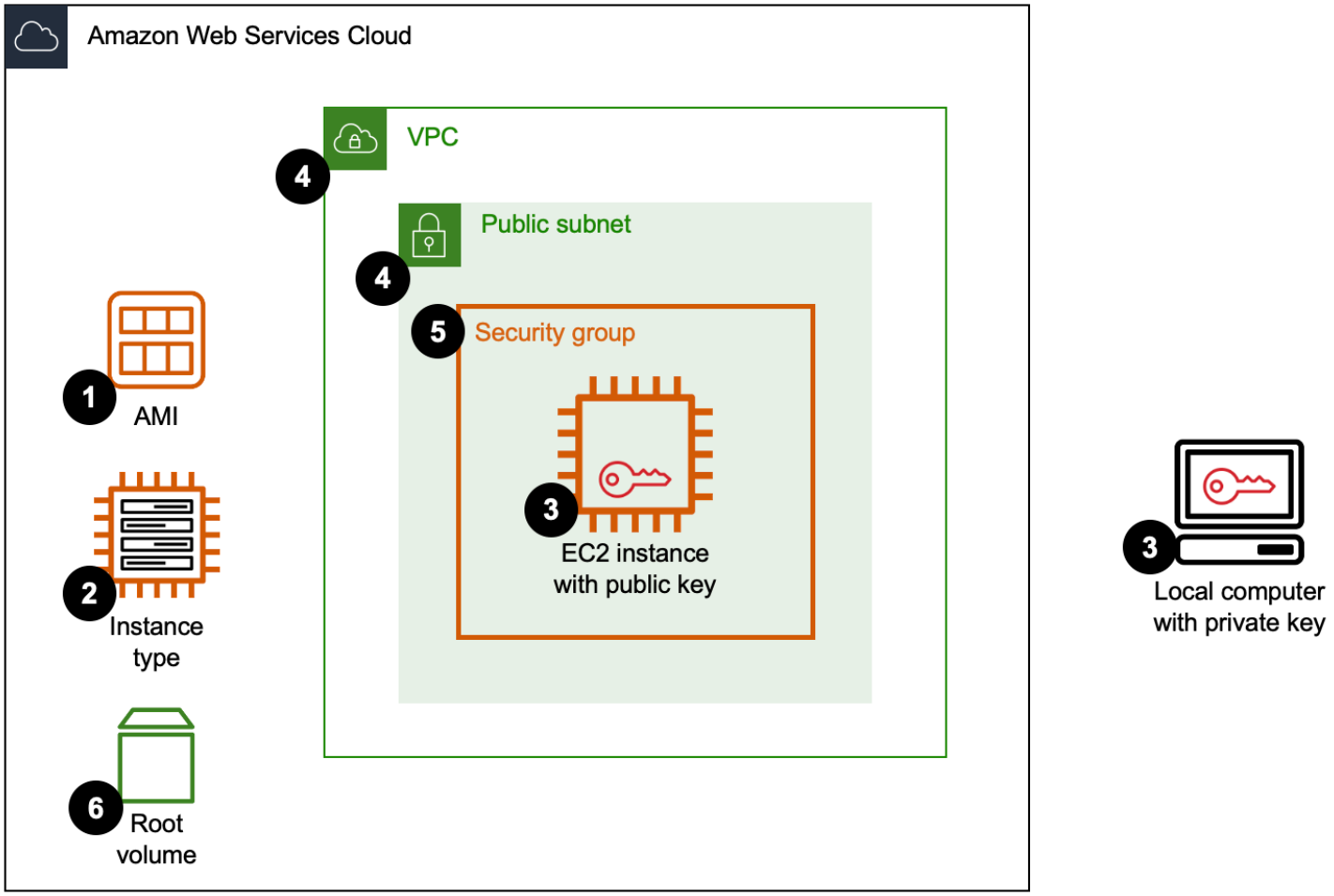
Bei der Entscheidung, welche Art von Instance gestartet werden soll, berücksichtigen Sie die Konfigurationskriterien für die Instance, genauso wie Sie die Kriterien berücksichtigen würden, die Sie von einem Haus erwarten. Diese Analogie vereinfacht zwar die Dinge, bietet aber eine hilfreiche Möglichkeit, die Komponenten zu visualisieren, bis Sie mit ihnen besser vertraut sind.

- AMI – Baumaterialien und Ausstattungen für Häuser: Das Amazon Machine Image (AMI) bestimmt, mit welchem Betriebssystem und welchen Anwendungen Ihre Instance gestartet wird. Dies entspricht der Auswahl der Baumaterialien (wie Ziegel, Stahl oder Holz) und der Ausstattung (wie Geräte und Einrichtungsgegenstände) Ihres Hauses. Ein Basis-AMI ist wie ein unmöbliertes Haus mit Basisgeräten, während ein benutzerdefiniertes AMI mit vorinstallierter Software einem komplett eingerichteten Haus ähnelt.

- Instance-Typ – Hausgröße und Leistung: Der Instance-Typ definiert die Größe und die Funktionen Ihrer EC2-Instance, ähnlich wie die Wahl der Größe eines Hauses, der Anzahl der Räume und der Energiekapazität. Jeder Instance-Typ bestimmt die Menge an CPU, Arbeitsspeicher, Speicher und Netzwerkkapazität Ihrer Instance. Das ausgewählte AMI schränkt möglicherweise ein, welche Instance-Typen Sie wählen können.
- Schlüsselpaar – Haustürschlüssel: Ein Schlüsselpaar ist wie Schloss und Schlüssel für die Haustür Ihres Hauses. Der öffentliche Schlüssel fungiert als Schloss für Ihre Instance, während der private Schlüssel der Schlüssel ist, den Sie sicher auf Ihrem lokalen Computer aufbewahren müssen. Wenn jemand anderes in die Hände Ihres privaten Schlüssels gelangt, kann diese Person auf Ihre Instance zugreifen, ähnlich wie jemand mit Ihrem Haustürschlüssel Ihr Haus betreten kann.
- Netzwerk (VPC und Subnetz) – Grundstücksgrenze, abgeteilte Bereiche und Hausnummer: Ihre Virtual Private Cloud (VPC) ist wie das gesamte Grundstück, auf dem sich Ihr Haus befindet, und das Subnetz ist der abgetrennte Bereich rund um das Haus. Wenn Sie mehrere Häuser (Instances) auf Ihrem Grundstück haben, sollten Sie diese je nach Verwendungszweck in unterschiedliche Bereiche (verschiedene Subnetze) unterteilen. Einige Häuser ermöglichen es Besuchern, sich frei durch die Gärten zu bewegen (öffentliche Subnetze mit Internetzugang), während andere über eingezäunte Gärten verfügen, um den Zutritt zu beschränken (private Subnetze ohne Internetzugang). Jedes Subnetz enthält, ähnlich wie Hausnummern, eine Reihe von IP-Adressen, die Instances innerhalb des Subnetzes zugewiesen werden können.
- Sicherheitsgruppe – Der Pförtner: Die Sicherheitsgruppe agiert wie ein Pförtner und kontrolliert, wer Ihr Haus besuchen darf. Sie setzt eine Reihe von Regeln durch, die kontrollieren, welcher Datenverkehr Ihre Instance erreichen darf. Eine Regel, die SSH-Verkehr von einer bestimmten IP-Adresse zulässt, ist beispielsweise so, als würde der Pförtner nur eine bestimmte Person für die Lieferung von Lebensmitteln zulassen. In ähnlicher Weise ist das Zulassen von HTTPS-Verkehr von überall aus so, als ob die Öffentlichkeit kommen und sich das Äußere Ihres Hauses ansehen würde.
- Amazon-EBS-Volumen – Speichereinheiten: EBS-Volumes sind wie Lagereinheiten, in denen Sie Ihre Sachen lagern können. Jede Instance hat ein Root-Volume (auf dem das AMI gespeichert ist), und Sie können bei Bedarf jederzeit weitere Volumes (Speicher) hinzufügen.
- Name-Tag – Der Hausname: Das Name-Tag funktioniert wie ein Schild an einem Haus, sodass Sie leicht erkennen können, wer dort wohnt. Das Name-Tag erleichtert zwar die Unterscheidung zwischen Instances, ist aber beim Starten einer Instance nicht erforderlich.

Aufgabe 2: Ein technisches Diagramm überprüfen

In dieser Aufgabe machen Sie sich mit einem typischen technischen Diagramm vertraut, das wir in der AWS-Dokumentation verwenden. Das folgende Diagramm zeigt die Konfiguration für die Test-Instance, die Sie in diesem Tutorial starten. In der vorherigen Aufgabe haben wir diese Komponenten anhand der Analogie eines Miethauses vorgestellt. Jetzt konzentrieren wir uns auf die eigentlichen EC2-Komponenten selbst. Die nummerierten Etiketten entsprechen den folgenden Beschreibungen.



1. AMI – Das AMI ist das Image, das Sie beim Starten einer Instance auswählen. Das ist eine Vorlage, die das Betriebssystem und die Software enthält, die auf Ihrer Instance ausgeführt werden sollen. Wenn Sie beispielsweise eine Linux-Instance starten möchten, können Sie das Amazon Linux 2023 AMI wählen. Oder, wenn Sie eine Windows-Instance starten möchten, können Sie das Microsoft-Windows-Server-2022-Base-AMI wählen. Der AMI-Katalog in der Amazon-EC2-Konsole enthält Tausende von Bildern, aus denen Sie wählen können.
2. Instance-Typ – Der Instance-Typ ist die Hardware, die die CPU, den Arbeitsspeicher, die Speicher und die Netzwerkkapazität des Host-Computers für die Instance bestimmt. Amazon EC2 bietet

über 600 Instance-Typen zur Auswahl, die sich jeweils in Hardwarekonfiguration und Größe unterscheiden, sodass Sie die für Ihre Anwendung am besten geeignete Variante auswählen können.

3. Schlüsselpaar – Ein Schlüsselpaar ist eine Reihe von Sicherheitsanmeldeinformationen, mit denen Sie elektronisch Ihre Identität nachweisen, wenn Sie sich mit einer -Instance verbinden. Der private Schlüssel ist auf dem lokalen Computer gespeichert und ein öffentlicher Schlüssel ist in der Instance gespeichert.

   In EC2 bezieht sich die Verbindung zu Ihrer Instance auf die Anmeldung bei Ihrer Instance von Ihrem lokalen Computer aus. Es gibt zwar andere Möglichkeiten, eine sichere Verbindung zu Ihrer Instance herzustellen, aber in diesem Tutorial verwenden wir ein Schlüsselpaar.
4. Netzwerk – Das Netzwerk besteht aus einer VPC und einem oder mehreren Subnetzen. Eine VPC ist ein isoliertes virtuelles Netzwerk in AWS Cloud. Jeder AWS-Kunde hat seine eigene VPC, die dem AWS-Konto gewidmet ist. Sie werden Ihre Instance in einem Subnetz in Ihrer VPC starten. Ein Subnetz ist ein Bereich von IP-Adressen in einer VPC. Ihr Standardsubnetz ist ein öffentliches Subnetz, was bedeutet, dass es eine öffentliche IP-Adresse zuweist und Ihrer Instance von außerhalb des Amazon-Netzwerks Internetzugang ermöglicht.
5. Sicherheitsgruppe – Eine Sicherheitsgruppe fungiert als Firewall zur Steuerung des Datenverkehrs zu Ihrer Instance. Eine Sicherheitsgruppe enthält Regeln, die bestimmten Arten von Datenverkehr den Zugang zu Ihrer Instance ermöglichen. Um eine SSH-Verbindung von Ihrem lokalen Computer zu Ihrer Instance herzustellen (mithilfe Ihres Schlüsselpaars), benötigen Sie eine Regel, die SSH-Verkehr von Ihrem lokalen Computer aus zulässt.
6. EBS-Volume – Ein Amazon-EBS-Volume ist ein Speichergerät, das wie eine physische Festplatte funktioniert. Ihre Instance verfügt über ein Root-Volume, bei dem es sich um ein spezielles EBS-Volume handelt, das das AMI mit dem Betriebssystem und der Software speichert, die zum Starten Ihrer Instance benötigt werden. Sie können optional Daten-Volumes hinzufügen. Da Ihre Test-Instance jedoch keine vertraulichen Daten speichert, benötigen Sie keine zusätzlichen verschlüsselten Daten-Volumes.

Herzlichen Glückwunsch! Sie haben die konzeptionellen Aufgaben in diesem Tutorial abgeschlossen. In den folgenden Aufgaben verwenden Sie die Amazon-EC2-Konsole, um die Komponenten zu erstellen, über die Sie sich informiert haben.

Schritt 3: Erstellen eines Schlüsselpaares

In dieser Aufgabe erstellen Sie ein Schlüsselpaar. Ein Schlüsselpaar besteht aus zwei Teilen: einem öffentlichen Schlüssel, den Sie Ihrer Instance hinzufügen, und einem passenden privaten

Schlüssel, mit dem Sie eine sichere Verbindung zu Ihrer Instance herstellen. In der nächsten Aufgabe wählen Sie dieses Schlüsselpaar beim Starten Ihrer Instance aus, wodurch der öffentliche Schlüssel automatisch zur Instance hinzugefügt wird. Es ist wichtig, den privaten Schlüssel sicher auf Ihrem lokalen Computer zu speichern, da jeder, der Zugriff darauf hat, eine Verbindung zu Ihrer Instance herstellen kann.

Wenn Sie beim Starten Ihrer Test-Instance lieber ein vorhandenes Schlüsselpaar verwenden möchten, können Sie diese Aufgabe gerne überspringen. Erstellen Sie andernfalls ein neues Schlüsselpaar.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie die in der obigen Tabelle aufgeführten Voraussetzungen erfüllt haben, einschließlich der Anmeldung in der AWS-Managementkonsole mit Ihrem Administratorbenutzer.

So erstellen Sie ein Schlüsselpaar

1. Öffnen Sie die Amazon-EC2-Konsole:

   Gehen Sie zu https://console.aws.amazon.com/ec2/.
2. Navigieren Sie zur Seite der Schlüsselpaarkonsole:

   Wählen Sie im Navigationsbereich unter Network & Security die Option Key Pairs aus.

   - Wenn Sie zuvor Schlüsselpaare erstellt haben, werden diese in der Tabelle angezeigt.
   - Wenn keine Schlüsselpaarname vorhanden ist, ist die Tabelle leer.
3. Erstellen Sie ein neues Schlüsselpaar:

   Klicken Sie auf die Schaltfläche Schlüsselpaar erstellen (oben rechts), um das webbasierte Formular Schlüsselpaar erstellen zu öffnen, und geben Sie Ihre Schlüsselpaardetails wie folgt ein:

   a. Benennen Sie Ihr Schlüsselpaar: Geben Sie unter Name einen Namen ein, anhand dessen Sie das Schlüsselpaar leichter erkennen können, z. B **`test-instance-key-pair`**.

      Der Name kann bis zu 255 ASCII-Zeichen enthalten. Er darf keine führenden oder nachfolgenden Leerzeichen enthalten.

   b. Wählen Sie den Schlüsselpaartyp: Wählen Sie als Schlüsselpaartyp ED25519.

Linux-Instances unterstützen sowohl RSA- als auch ED25519-Schlüsseltypen, während Windows-Instances nur RSA unterstützen. Da Sie in diesem Tutorial eine Linux-Instance starten, können Sie einen ED25519-Schlüssel verwenden.

c. Privatschlüsselformat wählen: Wählen Sie unter Dateiformat des privaten Schlüssels .pem.

Dies ist das Format, in dem Ihre private Schlüsseldatei gespeichert wird.

4. Speichern Sie den öffentlichen Schlüssel in Amazon EC2 und laden Sie den privaten Schlüssel herunter:

Wählen Sie die Schaltfläche Schlüsselpaar erstellen (unten rechts).

Amazon EC2 speichert den öffentlichen Schlüssel, während Ihr Browser die private Schlüsseldatei automatisch auf Ihren lokalen Computer herunterlädt. Die Datei wird nach dem Namen benannt, den Sie für das Schlüsselpaar angegeben haben und die Erweiterung ist das ausgewählte Dateiformat. Verschieben Sie die private Schlüsseldatei an einen sicheren Speicherort auf Ihrem Computer.

> **Important**
>
> Dies ist die einzige Möglichkeit, die Sie haben, die private Schlüsseldatei zu speichern.

5. Legen Sie die Berechtigungen für den Schlüssel fest (für MacOS- und Linux-Benutzer):

Wenn Sie über SSH auf einem macOS- oder Linux-Computer eine Verbindung zu Ihrer Instance herstellen möchten, müssen Sie die richtigen Berechtigungen für Ihre private Schlüsseldatei festlegen. Öffnen Sie ein Terminal-Fenster und führen Sie den folgenden Befehl aus, wobei Sie *test-instance-key-pair* durch den Namen Ihres Schlüsselpaars ersetzen:

```
chmod 400 test-instance-key-pair.pem
```

Dieser Befehl stellt sicher, dass nur Sie die private Schlüsseldatei lesen können, die für den Aufbau einer sicheren Verbindung zu Ihrer Instance erforderlich ist. Ohne diese Berechtigungen können Sie mit diesem Schlüsselpaar keine Verbindung herstellen.

Herzlichen Glückwunsch! Sie haben erfolgreich ein Schlüsselpaar erstellt!

Aufgabe 4: Ihre Test-Instance starten

In dieser Aufgabe starten Sie schnell eine Test-Instance mit dem Launch Instance Wizard von EC2. Sie konfigurieren die wichtigsten Instance-Konfigurationseinstellungen für eine Linux-Instance und verwenden die Standardwerte für die anderen Felder.

Um Ihnen das Kostenmanagement zu erleichtern, empfehlen wir Ihnen, die für das kostenlose Kontingent infrage kommenden Komponenten zu wählen.

Die folgenden Schritte ausführen, um eine Test-Instance zu starten

1. Öffnen Sie die Amazon-EC2-Konsole:

   Gehen Sie zu https://console.aws.amazon.com/ec2/.
2. Öffnen Sie den EC2-Launch-Instance-Wizard:

   Wählen Sie im EC2-Dashboard Instance starten aus.

   Das webbasierte Formular Eine Instance starten wird geöffnet. Das ist der Launch Instance Wizard von EC2.
3. Benennung Ihrer Instance:

   Geben Sie unter Name und Tags bei Name einen beschreibenden Namen wie **`Test instance`** ein.

   Der Instance-Name ist ein Tag, wobei der Schlüssel Name ist und es sich bei dem Wert um den von Ihnen angegebenen Namen handelt.

   Tipp: Für Test-Instances ist ein Namens-Tag ausreichend. Für Produktions-Instances empfiehlt es sich jedoch, eine Tagging-Richtlinie festzulegen, um das Tagging für all Ihre Ressourcen zu standardisieren.
4. Wählen Sie Ihr Betriebssystem und Ihre Software – das Amazon Machine Image (AMI):

   Unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image) ist die Standardauswahl für Amazon Machine Image (AMI) die Standardauswahl Amazon Linux 2023 AMI. Diese AMIs sind als Zur kostenlosen Nutzung berechtigt gekennzeichnet. In diesem Tutorial starten Sie eine Linux-Instance. Behalten Sie also die Standardeinstellung bei, um innerhalb des kostenlosen Kontingents zu bleiben.
5. Wählen Sie Ihre Hardware – den Instance-Typ:

Behalten Sie für dieses Tutorial unter Instance-Typ für Instance-Typ die Standardauswahl bei. Der Standard-Instance-Typ kann mit dem kostenlosen Kontingent verwendet werden und seine Hardware ist für Ihre Test-Instance geeignet.

6. Bereiten Sie sich auf die sichere Anmeldung mit einem Schlüsselpaar vor:

   Wählen Sie unter Schlüsselpaar (Anmeldung) bei Schlüsselpaarname das Schlüsselpaar aus, das Sie bei der Einrichtung erstellt haben. Wenn Ihr Schlüsselpaar nicht in der Liste angezeigt wird, wählen Sie das Aktualisierungssymbol (rechts neben der Liste).

   Wenn Ihre Instance gestartet wird, platziert sie den öffentlichen Schlüssel auf der Instance. Um nach dem Start eine Verbindung zu Ihrer Instance herzustellen, verwenden Sie den entsprechenden privaten Schlüssel, den Sie in der vorherigen Aufgabe heruntergeladen haben.

7. Konfigurieren Sie die Netzwerkeinstellungen, um den Internetzugang zu aktivieren:

   Unter Netzwerkeinstellungen sind die Felder Netzwerk (Ihre VPC) und Subnetz standardmäßig konfiguriert. Behalten Sie die Standardeinstellungen für dieses Tutorial bei, um Ihnen den schnellen Einstieg zu erleichtern. Wenn Sie Ihr Standard-Subnetz nicht geändert haben, verfügt Ihre Instance über Internetzugang.

   Tipp: Ihr Standardsubnetz ist ein öffentliches Subnetz, was bedeutet, dass es eine öffentliche IP-Adresse zuweist und Ihrer Instance von außerhalb des Amazon-Netzwerks Internetzugang ermöglicht. Für Test-Instances ist es in Ordnung, die Standard-Subnetzeinstellungen zu verwenden, die den Internetzugang ermöglichen. Für Produktions-Instances empfiehlt es sich jedoch, nur eine öffentliche IP-Adresse zuzuweisen und ein Subnetz mit Internetzugang zu verwenden, wenn dies unbedingt erforderlich ist.

8. Richten Sie die Instance-Firewall (Sicherheitsgruppe) ein):

   Lassen Sie unter Netzwerkeinstellungen unter Firewall (Sicherheitsgruppen) das Kontrollkästchen SSH-Verkehr von überall zulassen (0.0.0.0) aktiviert. Dadurch wird eine neue Sicherheitsgruppe für Ihre Test-Instance erstellt, die SSH-Datenverkehr von einer beliebigen IP-Adresse aus zulässt.

   Eine Sicherheitsgruppe fungiert als Firewall zur Steuerung des Datenverkehrs zu Ihrer Instance. Um eine SSH-Verbindung von Ihrem lokalen Computer zu Ihrer Instance herzustellen, benötigen Sie eine Regel, die SSH-Verkehr von Ihrem lokalen Computer aus zulässt.

   Tipp: Die IP-Adresse Ihres lokalen Computers kann sich im Laufe der Zeit ändern, wenn Ihr Internet-Service-Anbieter dynamische IP-Zuweisung verwendet. Wir gehen davon aus, dass

Sie, wenn Sie eine Instance zu Testzwecken verwenden, die Instance nicht zum Speichern vertraulicher Informationen verwenden. Daher können die Sicherheitsmaßnahmen weniger restriktiv sein. Für Test-Instances ist es generell akzeptabel, Datenverkehr von einer beliebigen IP-Adresse (`0.0.0.0/0`) aus zuzulassen, sodass Sie immer eine Verbindung herstellen können, auch wenn sich Ihre IP-Adresse ändert. Für Produktions-Instances, insbesondere solche mit vertraulichen Daten, hat es sich jedoch bewährt, nur Datenverkehr von bekannten IP-Adressen zuzulassen.

9. Konfigurieren Sie den Instance-Speicher:

   Unter Speicher konfigurieren sind die Felder Root-Volume (verschlüsselt) standardmäßig konfiguriert. Lassen Sie die Einstellungen unverändert, um innerhalb der Limits des kostenlosen Kontingents zu bleiben.

   Da Ihre Test-Instance jedoch keine vertraulichen Daten speichert, benötigen Sie keine zusätzlichen verschlüsselten Daten-Volumes.

10. Überprüfen Sie die Instance-Konfiguration:

    Im Übersichtsbereich auf der rechten Seite können Sie Ihre allgemeinen Einstellungen überprüfen, bevor Sie Ihre Instance starten.

11. Starten Ihrer Instance:

    Wenn Sie bereit sind, Ihre Instance in der Zusammenfassungsbereich zu starten, wählen Sie Instance starten aus.

    Amazon EC2 startet Ihre Instance schnell mit den Einstellungen, die Sie angegeben haben. Wenn Sie keine Einstellung angegeben haben, wird die Standardeinstellung verwendet. Ein Erfolgsbanner bestätigt den Start.

Herzlichen Glückwunsch! Sie haben Ihre Test Instance erfolgreich gestartet!

Aufgabe 5: Ihre Instance finden

In dieser Aufgabe lokalisieren Sie die Instance, die Sie gerade in der EC2-Konsole gestartet haben.

Gehen Sie wie folgt vor, um Ihre Instance in der EC2-Konsole zu finden

1. Öffnen Sie die Instances-Seite:

Wenn Sie sich immer noch auf der Erfolgsseite befinden, wählen Sie die Instance-ID im Erfolgsbanner aus.

Wenn Sie die Seite verlassen haben, wählen Sie im Navigationsbereich Instances aus.

2. Ihre Instance suchen:

   Suchen Sie in der Spalte Name Ihre Instance anhand des Namens, den Sie ihr gegeben haben.

Aufgabe 6: Anzeigen Ihrer Instance-Konfiguration

In dieser Aufgabe machen Sie sich mit der Anzeige der Konfigurationsdetails Ihrer Instance vertraut.

Gehen Sie folgendermaßen vor, um die Konfiguration Ihrer Instance anzuzeigen

1. Ihre Instance suchen:

   Suchen Sie in der Spalte Name Ihre Instance anhand des Namens, den Sie ihr gegeben haben.

2. Öffnen Sie die Seite mit den Instance-Details:

   Aktivieren Sie das Kontrollkästchen neben dem Namen Ihrer Instance, wählen Sie dann das Menü Aktionen (oben rechts) und wählen Sie Details anzeigen, um die Seite mit den Instance-Details zu öffnen, auf der Sie die Konfiguration überprüfen können.

   Im vorherigen Tutorial haben Sie den ID-Link der Instance ausgewählt, um die Instance-Detailseite zu öffnen. Sie werden feststellen, dass es mehrere Möglichkeiten gibt, eine Aufgabe in der EC2-Konsole zu erledigen.

3. Erkunden Sie die Einzelheiten der Instance-Konfiguration:

   Nehmen Sie sich ein paar Minuten Zeit, um die Konfigurationsdetails Ihrer Instance zu erkunden.

   Tipp: Um schnell ein Feld zu finden, drücken Sie Strg+F oder Befehlstaste+F auf Ihrer Tastatur.

   a. AMI: Können Sie das AMI finden, mit dem Sie Ihre Instance gestartet haben? Sie finden die Informationen unter AMI-ID und AMI-Name auf der Registerkarte Details.
   b. Instance-Typ: Können Sie den Instance-Typ finden? Es könnte zum Beispiel t3.micro sein.
   c. Schlüsselpaar: Finden Sie das Schlüsselpaar, das Sie beim Starten Ihrer Instance angegeben haben? Es ist für das beim Start zugewiesene Schlüsselpaar angegeben.

Beachten Sie, dass sich der Wert hier nicht ändert, wenn Sie das Schlüsselpaar in Zukunft ändern.

d. VPC: Können Sie die ID Ihrer VPC finden? Sie finden alle netzwerkbezogenen Konfigurationseinstellungen auf der Registerkarte Netzwerk. Die VPC-ID hat ein Format, das dem folgenden Beispiel ähnelt: vpc-1a2b3c4d

e. Subnetz: Können Sie die ID des Subnetzes finden, in dem Sie Ihre Instance gestartet haben? Sie hat ein Format, das dem folgenden Beispiel ähnelt: subnet-1a2b3c4d

f. Öffentliche IPv4-Adresse: Können Sie die öffentliche IPv4-Adresse finden, die Ihrer Instance zugewiesen wurde? Sie hat ein Format, das dem folgenden Beispiel ähnelt: 34.242.148.128.

g. Sicherheitsgruppe: Können Sie die Regel für eingehenden Datenverkehr finden, die erstellt wurde, um SSH-Verkehr von überall aus zuzulassen (0.0.0.0./0)? Sie finden alle sicherheitsrelevanten Konfigurationseinstellungen auf der Registerkarte Sicherheit.

h. Speicher: Können Sie das Volume finden, das für diese Instance erstellt wurde? Sie finden alle sicherheitsrelevanten Konfigurationseinstellungen auf der Registerkarte Speicher.

i. Instance-Tags: Der Name, den Sie Ihrer Instance gegeben haben, ist eigentlich ein Tag. Können Sie Ihre Instance-Tags finden? Wählen Sie die Registerkarte Tags aus. Der Schlüssel ist Name, und der Wert ist der Name, den Sie angegeben haben.

j. Instance-Status: Können Sie den Status Ihrer Instance überprüfen? Sie sollte Wird ausgeführt sein.

Nehmen Sie sich ein paar Minuten Zeit, um die Konfigurationsdetails Ihrer Instance zu erkunden. Wenn Sie bereit sind, fortzufahren, gehen Sie zur nächsten Aufgabe.

Aufgabe 7: Machen Sie sich mit den wichtigsten Komponenten für die Verbindung zu einer Instance vertraut

In dieser Aufgabe erkunden Sie die wichtigsten Komponenten, die zum Starten einer EC2-Instance erforderlich sind. Dies sind das Verbindungsprotokoll, das öffentliche DNS, die Sicherheitsgruppe, das Schlüsselpaar und der Instance-Benutzername.

Um diese Komponenten besser zu visualisieren, stellen Sie sich vor, eine Verbindung zu einer Instance herzustellen, z. B. zu Ihnen nach Hause zu gehen:

- Verbindungsprotokoll – Ihr Transportmittel: So wie Sie entscheiden, wie Sie nach Hause kommen, wählen Sie auch das Verbindungsprotokoll, das Sie zu Ihrer Instance führt. In diesem Tutorial

verwenden wir SSH (Secure Shell), das einen sicheren Tunnel für die Verbindung Ihres Computers mit Ihrer Instance über das Internet erstellt.

- Öffentliches DNS – Die Hausadresse: So wie Ihr Haus eine eindeutige Adresse hat, hat auch Ihre EC2-Instance ihren eigenen öffentlichen DNS-Namen (z. B. `ec2-18-201-118-201.eu-west-1.compute.amazonaws.com`). Dieser öffentliche DNS-Name ermöglicht es SSH, eine direkte Verbindung zu Ihrer Instance herzustellen.
- Sicherheitsgruppe – Der Pförtner: Stellen Sie sich vor, Ihr Haus hat einen Pförtner, der kontrolliert, wer rein oder raus darf. In ähnlicher Weise verfügt die EC2-Instance über eine Sicherheitsgruppe, die wie ein Pförtner agiert und kontrolliert, welche Arten von Netzwerkverkehr in Ihre Instance hinein oder aus Ihrer Instance heraus zugelassen sind. Nur der Datenverkehr, den Sie ausdrücklich zulassen (z. B. SSH-Verkehr von der IP-Adresse Ihres Computers), ist zugelassen.
- Privater Schlüssel – Ihr Haustürschlüssel: Als Sie die Instance gestartet haben, haben Sie ein Schlüsselpaar angegeben. Der private Schlüssel ist auf dem lokalen Computer gespeichert und ein öffentlicher Schlüssel ist in der Instance gespeichert. Der private Schlüssel fungiert als Ihr Haustürschlüssel – ohne ihn können Sie nicht auf Ihre Instance zugreifen.
- Benutzername der Instance – Der Bewohner: Wenn Sie bei Ihnen zu Hause ankommen, müssen Sie sich ausweisen, um nachzuweisen, dass Sie dort ansässig sind. Wenn Sie eine Verbindung zu einer Instance herstellen, geben Sie ebenfalls einen Benutzernamen an. Verschiedene Instances haben je nach Betriebssystem unterschiedliche Standardbenutzernamen. Amazon-Linux-Instances verwenden beispielsweise `ec2-user` als den Standardbenutzernamen.

Der Verbindungsbefehl

Um eine Verbindung zu Ihrer EC2-Instance herzustellen, verwenden Sie den folgenden Befehl in einem Terminal-Fenster:

```
ssh -i "test-instance-key-pair.pem" ec2-user@ec2-18-201-118-201.eu-
west-1.compute.amazonaws.com
```

Im Folgenden finden Sie eine Aufschlüsselung der Funktionen des Befehls:

- `ssh` – Dieser Befehl gibt das Verbindungsprotokoll an, das eine SSH-Verbindung (Secure Shell) zu Ihrer Instance initiiert.
- `-i "test-instance-key-pair.pem"` – Das `-i`-Flag gibt die private Schlüsseldatei an, die zur Authentifizierung der Verbindung benötigt wird. Diese private Schlüsseldatei muss mit dem Schlüsselpaar übereinstimmen, das Sie beim Starten der Instance angegeben haben. Wenn Ihre

private Schlüsseldatei in einem bestimmten Ordner gespeichert ist, geben Sie den vollständigen Pfad zur Datei an.

- `ec2-user` – Dies ist der Benutzername für die Anmeldung bei der Instance. Bei Amazon-Linux-Instances lautet der Standard-Benutzername `ec2-user`. Andere AMIs verwenden möglicherweise andere Standardbenutzernamen, z. B. `ubuntu` für Ubuntu-Instances.
- `@` – Dieses Symbol trennt den Benutzernamen von der Adresse der Instance.
- `ec2-18-201-118-201.eu-west-1.compute.amazonaws.com` – Dies ist die öffentliche Adresse Ihrer Instance (das öffentliche DNS), zu der die öffentliche IPv4-Adresse und die AWS-Region gehören. Sie identifiziert die Instance eindeutig.

Was geschieht, wenn Sie den Befehl ausführen

Nachdem Sie den Befehl ausgeführt haben, richtet SSH einen sicheren Tunnel ein und authentifiziert sich mit Ihrem privaten Schlüssel. Wenn die Sicherheitsgruppe der Instance den Datenverkehr zulässt, erhalten Sie Zugriff auf Ihre EC2-Instance. Sie können die Instance jetzt von Ihrem Computer aus steuern, als ob Sie direkt davor sitzen würden. Sie können Befehle ausführen, Software installieren und Dateien verwalten – genau wie auf Ihrem lokalen Computer.

Aufgabe 8: Verbindung mit Ihrer Instance herstellen

In dieser Aufgabe stellen Sie über einen SSH-Client auf Ihrem Computer eine Verbindung zu Ihrer Instance her. In der vorherigen Aufgabe haben wir die Komponenten für die Verbindung mit einer Instance anhand der Analogie vorgestellt, dass Sie zu Ihnen nach Hause gehen. Jetzt konzentrieren wir uns auf die Verbindung zur eigentlichen EC2 Instance.

Es gibt verschiedene Methoden, eine Verbindung zu einer Instance herzustellen. Die Methode, mit der Sie eine Verbindung herstellen, hängt vom Betriebssystem der Instance ab. Da Sie eine Linux-Instance gestartet haben, verwenden Sie einen SSH-Client auf Ihrem lokalen Computer.

Überprüfen Sie zunächst, ob auf Ihrem Computer ein SSH-Client installiert ist

Auf den meisten Computern ist ein SSH-Client vorinstalliert. Um dies zu überprüfen, öffnen Sie ein Terminal-Fenster auf Ihrem Computer und führen Sie den folgenden Befehl aus:

```
ssh
```

Wenn der Befehl erkannt wird, können Sie eine Verbindung herstellen.

Wenn Ihr Computer den Befehl nicht erkennt, müssen Sie einen SSH-Client installieren. Anweisungen zur Installation eines SSH-Clients würden den Rahmen dieses Tutorials sprengen. Wenn Sie Hilfe benötigen, lesen Sie Voraussetzungen für eine SSH-Verbindung in diesem Benutzerhandbuch nach oder suchen Sie online nach Anweisungen zur Installation eines SSH-Clients auf Ihrem Betriebssystem.

Folgen Sie diesen Schritten, um eine Verbindung mit Ihrer Instance herzustellen

1. Verbindung herstellen:

   Wenn Sie sich in der Amazon-EC2-Konsole auf der Seite mit den Instance-Details befinden, wählen Sie die Schaltfläche Verbinden (oben rechts).

   Wenn Sie die Seite verlassen haben, wählen Sie im Navigationsbereich Instances aus. Aktivieren Sie dann auf der Seite Instances das Kontrollkästchen neben dem Namen Ihrer Instance und klicken Sie auf die Schaltfläche Verbinden (oben rechts).

   Dadurch wird die Seite Mit Verbinden zur Instance geöffnet.
2. Wählen Sie die Verbindungsmethode:

   Auf der Seite Verbindung mit Instance herstellen wählen Sie die Registerkarte SSH-Client aus.

   Nehmen Sie sich einen Moment Zeit, um den Text auf dieser Seite zu lesen, denn dies sind die Schritte, die Sie als Nächstes befolgen werden.
3. SSH-Befehl überprüfen:

   Unter Beispiel sehen Sie einen Befehl, der automatisch generiert und mit den Details Ihrer Instance angepasst wird. Der Name des privaten Schlüssels wird vom Namen des öffentlichen Schlüssels abgeleitet, der beim Start angegeben wurde.

   Das Ergebnis sieht etwa folgendermaßen aus:

   ```
   ssh -i "test-instance-key-pair.pem" ec2-user@ec2-18-201-118-201.eu-
   west-1.compute.amazonaws.com
   ```
4. SSH-Befehl kopieren:

   Wählen Sie das Kopiersymbol neben dem SSH-Beispielbefehl.
5. Öffnen Sie ein Terminal-Fenster:

Öffnen Sie ein Terminal-Fenster auf Ihrem lokalen Computer.

6. SSH-Befehl einfügen und ausführen:

   Fügen Sie den SSH-Befehl in das Terminal-Fenster ein. Wenn Sie Ihre private Schlüsseldatei in einem bestimmten Ordner gespeichert haben, bearbeiten Sie den Befehl, um den vollständigen Dateipfad anzugeben.

   Drücken Sie Enter auf Ihrer Tastatur.

   Es wird eine Antwort ähnlich dem folgenden Beispiel angezeigt:

   ```
   The authenticity of host 'ec2-18-201-118-201.eu-west-1.compute.amazonaws.com
    (18-201-118-201)' can't be established.
   ED25519 key fingerprint is SHA256:examplehxj9aOr1MogvKOoMNskVVIRBQBoq0example.This
    key is not known by any other names.
   Are you sure you want to continue connecting (yes/no/[fingerprint])?
   ```

7. Die Verbindung fertigstellen:

   Geben Sie **`yes`** ein und drücken Sie die Eingabetaste auf Ihrer Tastatur.

   Die Überprüfung des Fingerabdrucks würde den Rahmen dieses Tutorials sprengen. Weitere Informationen hierzu finden Sie unter (Optional) Anfordern des Instance-Fingerabdrucks.

   Nach einer erfolgreichen Verbindung ändert sich die Terminal-Eingabeaufforderung und zeigt nun den öffentlichen DNS Ihrer Instance an.

Herzlichen Glückwunsch! Sie haben erfolgreich eine Verbindung zu Ihrer Instance hergestellt!

Aufgabe 9: Ihre Instance anhalten

In dieser Aufgabe löschen Sie Ihre Instance, um die Vorteile des kostenlosen Kontingents beizubehalten. Wenn Ihre Instance angehalten wird, fallen für Sie keine Kosten mehr an. Wenn Sie Ihr AWS-Konto vor dem 15. Juli 2025 erstellt haben und Sie für das kostenlose Kontingent berechtigt sind, fallen für Sie weiterhin Kosten für den EBS-Speicher an.

Folgen Sie diesen Schritten, um Ihre Instance zu beenden

1. Starten Sie die Beendigung:

Wenn Sie sich noch auf der Seite Mit Instance verbinden befinden, wählen Sie Instances aus dem Breadcrumb. Wenn Sie die Seite verlassen haben, wählen Sie im Navigationsbereich Instances aus.

Aktivieren Sie dann auf der Seite Instances das Kontrollkästchen neben dem Namen Ihrer Instance, wählen Sie dann das Menü Instance-Status (oben rechts) und wählen Sie Instance beenden aus. Wählen Sie nach Aufforderung die Option Beenden aus.

2. Instance-Status überwachen:

   Überprüfen Sie auf der Seite Instances die Spalte Instance-Status. Der Status Ihrer Instance ändert sich in Am Beenden und dann in Beendet. Wenn Sie nicht den vollständigen Text sehen, versuchen Sie, die Spalte zu erweitern.

   Wenn Sie der Meinung sind, dass sich der Instance-Status von Am Beenden zu Beendet geändert hat, Sie ihn aber noch nicht sehen, wählen Sie das Aktualisierungssymbol (über der Tabelle), um die Tabelle Instances zu aktualisieren.

Die wichtigsten Erkenntnisse

In diesem Tutorial haben Sie die folgenden Schlüsselkonzepte behandelt:

- AMI bezieht sich auf ein Amazon Machine Image, eine Vorlage, die das Betriebssystem und die Software enthält, die zum Starten einer Instance erforderlich sind.
- Der Instance-Typ bestimmt die Hardware des Computers, der für das Hosting Ihrer Instance verwendet wird. Er bestimmt die Menge an CPU, Arbeitsspeicher, Speicher und Netzwerkkapazität Ihrer Instance.
- Das Schlüsselpaar bezieht sich auf den Satz von öffentlichen und privaten Schlüsseln, die Sie für eine sichere Verbindung zu Ihrer Instance verwenden können.
- Netzwerk bezieht sich auf eine VPC (eine virtuelle private Cloud, die Ihrem Konto in der AWS Cloud zugewiesen ist) und ein Subnetz (eine Reihe von IP-Adressen innerhalb Ihrer VPC).
- Sicherheitsgruppe bezieht sich auf eine Reihe von Regeln, die steuern, welcher Datenverkehr Ihre Instance erreichen kann.
- Das EBS-Volume bezieht sich auf den Datenspeicher für Ihre Instance. Jede Instance hat ein Root-Volume zum Speichern des AMI und ein oder mehrere optionale Daten-Volumes.
- Tags sind Metadaten, die Sie Ihrer Instance optional zuweisen können. Der Instance-Name ist ein Tag, dessen Schlüssel Name ist, und der Wert ist Ihre Wahl.

- Eine Verbindung herstellen bezieht sich auf den Zugriff auf Ihre Instance über das Internet.
- SSH bezieht sich auf das Secure Shell-Verbindungsprotokoll, mit dem Sie eine Verbindung zu Ihrer Instance herstellen können.
- Öffentliches DNS ist die eindeutige öffentliche Adresse Ihrer Instance.
- Der Instance-Benutzername wird vom Betriebssystem Ihrer Instance bestimmt und ist für die Verbindung erforderlich.
- Durch das Beenden Ihrer Instance werden die Gebühren für die Instance gestoppt, aber die EBS-Speichergebühren bleiben bestehen.

Nächste Schritte

Um Vertrauen in das Starten, Verbinden und Beenden von Instances aufzubauen, sollten Sie die Schritte dieses Tutorials wiederholen. Stellen Sie sicher, dass Sie alle Instances, die Sie starten, beenden, um die Vorteile des kostenlosen Kontingents beizubehalten.

Sobald Sie mit diesen Grundlagen vertraut sind, können Sie sich die Tutorials für Fortgeschrittene ansehen. Weitere Tutorials finden Sie unter Suchen Sie nach anderen Tutorials?

Wenn Sie Ihr AWS-Konto vor dem 15. Juli 2025 erstellt haben, sollten Sie sich das folgende sechsminütige Video ansehen: Wie kann ich vermeiden, dass mein Konto belastet wird, wenn ich Kostenloses AWS-Kontingent-Services nutze?

Wenn Sie Ihr AWS-Konto am oder nach dem 15. Juli 2025 erstellt haben, sollten Sie sich die folgenden Informationen ansehen: AWS-Services mit dem kostenlosen AWS-Kontingent erkunden im Benutzerhandbuch für AWS Billing.

Referenz für EC2 Amazon-Instance-Konfigurationsparameter

Der Launch-Instance-Assistent und die Startvorlage in der EC2 Amazon-Konsole bieten alle Parameter für die Konfiguration einer EC2 Amazon-Instance.

Mit Ausnahme des Schlüsselpaars stellt der Launch Instance Wizard Standardwerte für alle Parameter bereit. Sie können jede einzelne oder alle Standardeinstellungen akzeptieren oder eine Instance mit Ihren eigenen Werten konfigurieren. Beim Erstellen einer Startvorlage sind die Parameter optional. Wenn Sie eine Startvorlage verwenden, um eine Instance zu starten, überschreiben die in der Startvorlage angegebenen Parameter die Standardwerte im Launch Instance Wizard. Für jeden Parameter, der nicht in der Startvorlage angegeben ist, wird standardmäßig der Wert verwendet, der vom Launch Instance Wizard bereitgestellt wird.

Die Parameter sind im Launch Instance Wizard und der Startvorlage gruppiert. Die folgenden Beschreibungen werden entsprechend den Parametergruppierungen in der Konsole dargestellt.

Parameter für die Instance-Konfiguration

- Name und Tags
- Anwendungs- und Betriebssystem-Images (Amazon Machine Image)
- Instance-Typ
- Schlüsselpaar (Anmeldung)
- Netzwerkeinstellungen
- Speicher konfigurieren
- Erweiterte Details
- Zusammenfassung

Name und Tags

Der Instance-Name ist ein Tag, wobei der Schlüssel Name ist und es sich bei dem Wert um den von Ihnen angegebenen Namen handelt. Sie können die Instance, Volumes und Netzwerkschnittstellen markieren. Bei Spot-Instances können Sie nur die Spot-Instance-Anforderung mit Tags (Markierungen) versehen. Informationen zu Tags siehe Kennzeichnen Sie Ihre EC2 Amazon-Ressourcen.

Die Angabe eines Instance-Namens und zusätzlicher Tags ist optional.

- Geben Sie unter Name einen beschreibenden Namen für die Instance ein. Wenn Sie keinen Namen angeben, kann die Instance anhand der ID identifiziert werden, die beim Starten der Instance automatisch generiert wird.
- Wenn Sie zusätzliche Tags hinzufügen möchten, wählen Sie Add additional tags (Zusätzliche Tags hinzufügen) aus. Klicken Sie auf Tag hinzufügen, geben Sie dann einen Schlüssel und einen Wert ein und wählen Sie den Ressourcentyp aus, den Sie markieren möchten. Wählen Sie für jedes weitere Tag Add another Tag (Weiteres Tag hinzufügen) aus.

Sie können nur den Instance-Namen angeben, wenn Sie die Instance starten. Sie können die Instance nicht benennen, wenn Sie eine Startvorlage erstellen, aber Sie können Tags für die Ressourcen hinzufügen, die beim Start der Instance erstellt werden.

Anwendungs- und Betriebssystem-Images (Amazon Machine Image)

Ein Amazon Machine Image (AMI) enthält die Informationen, die zum Starten einer Instance erforderlich sind. Ein AMI könnte beispielsweise die für die Funktion als Webserver erforderliche Software enthalten, wie Linux, Apache und Ihre Website.

Sie finden wie folgt ein passendes AMI. Bei jeder Option zum Aufrufen eines AMI können Sie Abbrechen (oben rechts) auswählen, um zum Launch Instance Wizard zurückzukehren, ohne ein AMI zu wählen.

Suchleiste

Um alle verfügbaren zu durchsuchen AMIs, geben Sie ein Schlüsselwort in die AMI-Suchleiste ein und drücken Sie dann die Eingabetaste. Wählen Sie Select (Auswählen) zum Auswählen des AMI aus.

Kürzlich gestartet

Die AMIs , die Sie kürzlich verwendet haben.

Wählen Sie Kürzlich gestartet oder Derzeit verwendet aus und wählen Sie dann unter Amazon Machine Image (AMI) ein AMI.

Mein AMIs

Das Private AMIs , das Sie besitzen, oder AMIs das private, das mit Ihnen geteilt wurde.

Klicken Sie auf Im Besitz von mir oder Mit mir geteilt und wählen Sie dann unter Amazon Machine Image (AMI) ein AMI aus.

Schnellstart

AMIs sind nach Betriebssystemen (OS) gruppiert, damit Sie schnell loslegen können.

Wählen Sie zuerst das benötigte Betriebssystem und dann unter Amazon Machine Image (AMI) ein AMI aus. Um ein AMI auszuwählen, das im Rahmen des AWS kostenlosen Kontingents verwendet werden kann, stellen Sie sicher, dass das AMI als für das kostenlose Kontingent in Frage kommt, gekennzeichnet ist.

Weitere Informationen finden AMIs

Wählen Sie Mehr durchsuchen AMIs, um den vollständigen AMI-Katalog zu durchsuchen.

- Um alle verfügbaren zu durchsuchen AMIs, geben Sie ein Schlüsselwort in die Suchleiste ein und drücken Sie dann die Eingabetaste.

- Um mit einem Systems-Manager-Parameter nach einem AMI zu suchen, wählen Sie die Pfeilschaltfläche rechts neben der Suchleiste und dann Search by Systems Manager parameter (Nach Systems-Manager-Parameter suchen) aus. Weitere Informationen finden Sie unter Referenz-AMIs mithilfe von Systems-Manager-Parametern.
- Um nach Kategorien zu suchen, wählen Sie Schnellstart AMIs AMIs AWS Marketplace AMIs, Meine oder Community AMIs.

  Das AWS Marketplace ist ein Online-Shop, in dem Sie Software kaufen können, die unter anderem AMIs läuft. AWS Weitere Informationen zum Starten einer Instance vom AWS Marketplace finden Sie unterStarten einer Amazon-EC2-Instance von einem AWS Marketplace-AMI. In der Community AMIs finden Sie Informationen AMIs , die AWS Community-Mitglieder anderen zur Nutzung zur Verfügung gestellt haben. AMIsvon Amazon oder einem verifizierten Partner sind als Verifizierter Anbieter gekennzeichnet.
- Um die Liste von zu filtern AMIs, aktivieren Sie auf der linken Seite des Bildschirms unter Ergebnisse verfeinern ein oder mehrere Kontrollkästchen. Die Filteroptionen unterscheiden sich in Abhängigkeit von der ausgewählten Suchkategorie.
- Prüfen Sie, welcher Root device type für die einzelnen AMIs aufgeführt ist. Beachten Sie, AMIs welchen Typ Sie benötigen: entweder ebs (unterstützt von Amazon EBS) oder instance-store (unterstützt von Instance Store). Weitere Informationen finden Sie unter Root-Volume-Typ.
- Prüfen Sie, welcher Typ unter Virtualization type für die einzelnen AMIs aufgeführt ist. Beachten Sie, AMIs welchen Typ Sie benötigen: entweder hvm oder paravirtual. Manche Instance-Typen benötigen beispielsweise HVM. Weitere Informationen zu Linux-AMI-Virtualisierungstypen finden Sie unter Virtualisierungstypen.
- Prüfen Sie den für jedes AMI aufgelisteten Startmodus. Beachten AMIs Sie, welcher den von Ihnen benötigten Startmodus verwendet: entweder Legacy-BIOS, UEFI oder UEFI-Preferred. Weitere Informationen finden Sie unter Instance-Startverhalten mit Amazon-EC2-Startmodi.
- Wählen Sie ein AMI aus, das Ihren Anforderungen entspricht, und klicken Sie auf Select.

Warnung beim Wechseln des AMI

Wenn Sie beim Starten einer Instance die Konfiguration von Volumes oder Sicherheitsgruppen ändern, die mit dem ausgewählten AMI verknüpft sind, und dann ein anderes AMI auswählen, öffnet sich ein Fenster, das Sie warnt, dass einige Ihrer aktuellen Einstellungen geändert oder entfernt werden. Sie können die Änderungen an den Sicherheitsgruppen und Volumes überprüfen. Darüber hinaus können Sie entweder anzeigen, welche Volumes hinzugefügt und gelöscht werden oder

nur die hinzugefügten Volumes anzeigen. Diese Warnung wird nicht angezeigt, wenn Sie eine Startvorlage erstellen.

Instance-Typ

Der Instance-Typ definiert die Hardware-Konfiguration und Größe der Instance. Größere Instance-Typen haben mehr CPU und Arbeitsspeicher. Weitere Informationen finden Sie unter EC2Amazon-Instance-Typen.

- Instance type (Instance-Typ): Vergewissern Sie sich, dass der Instance-Typ mit dem von Ihnen angegebenen AMI kompatibel ist. Weitere Informationen finden Sie unter EC2 Amazon-Instance-Typen.

  Kostenloses Kontingent – Sie können Instance-Typen verwenden, die als für das kostenlose Kontingent berechtigt gekennzeichnet sind und kostenlos genutzt werden können. Die spezifischen Instance-Typen hängen davon ab, wann Sie Ihre erstellt haben AWS-Konto.

  Wenn Sie Ihre AWS-Konto vor dem 15. Juli 2025 erstellt haben und sie weniger als 12 Monate alt ist, können Sie Amazon im EC2 Rahmen des kostenlosen Kontingents nutzen, indem Sie den Instance-Typ t2.micro oder in Regionen, in denen t2.micro nicht verfügbar ist, den Instance-Typ t3.micro auswählen. Beachten Sie, dass beim Starten einer t3.micro-Instance standardmäßig der Modus Unlimited verwendet wird, wodurch je nach CPU-Auslastung zusätzliche Gebühren anfallen können.

  Wenn Sie Ihre Instance-Typen AWS-Konto am oder nach dem 15. Juli 2025 erstellt haben, können Sie die Instance-Typen t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large und m7i-flex.large für 6 Monate oder bis Ihr Guthaben aufgebraucht ist verwenden.

  Weitere Informationen finden Sie unter Vorteile des kostenlosen Kontingents vor und nach dem 15. Juli 2025.
- Instance-Typen vergleichen: Sie können verschiedene Instance-Typen anhand der folgenden Attribute vergleichen: Anzahl von vCPUs, Architektur, Speichergröße (GiB), Speichermenge (GB), Speichertyp und Netzwerkleistung.
- Lassen Sie sich beraten: Anleitungen und Vorschläge für Instance-Typen finden Sie im EC2 Instance-Typ-Finder. Weitere Informationen finden Sie unter Holen Sie sich Empfehlungen vom EC2-Instance-Typ-Finder.

- (Nur Startvorlagen) Erweitert: Um Instance-Attribute anzugeben und Amazon die Instance-Typen anhand dieser Attribute EC2 identifizieren zu lassen, wählen Sie Erweitert und dann Instance-Typ-Attribute angeben.
  - Anzahl von v CPUs: Geben Sie die Mindest- und Höchstzahl von v CPUs für Ihre Rechenanforderungen ein. Um keine Limits anzugeben, geben Sie einen Mindestwert von **0** ein und lassen Sie den Höchstwert leer.
  - Speichermenge (MiB): Geben Sie in MiB den minimalen und maximalen Arbeitsspeicher für Ihre Rechenanforderungen ein. Um keine Limits anzugeben, geben Sie einen Mindestwert von **0** ein und lassen Sie den Höchstwert leer.
  - Erweitern Sie Optionale Instance-Typattribute und wählen Sie Attribut hinzufügen aus, um Ihre Rechenanforderungen detaillierter auszudrücken. Informationen zu den einzelnen Attributen finden Sie InstanceRequirementsRequestin der Amazon EC2 API-Referenz.
  - Resultierende Instance-Typen: Sie können eine Vorschau der Instance-Typen anzeigen, die den angegebenen Attributen entsprechen. Um Instance-Typen auszuschließen, wählen Sie Attribut hinzufügen aus und wählen Sie in der Liste Attribut die Option Ausgeschlossene Instance-Typen. Wählen Sie aus der Liste Attributwert die auszuschließenden Instance-Typen aus.

Schlüsselpaar (Anmeldung)

Wählen Sie für Schlüsselpaarname ein vorhandenes Schlüsselpaar aus oder wählen Sie Neues Schlüsselpaar erstellen, um ein neues zu erstellen. Weitere Informationen finden Sie unter EC2 Amazon-Schlüsselpaare und EC2 Amazon-Instances.

> **Important**
>
> Wenn Sie die Option Proceed without key pair (Not recommended) (Ohne Schlüsselpaar fortfahren (Nicht empfohlen)) auswählen, können Sie keine Verbindung zur Instance herstellen, es sei denn, Sie wählen ein AMI aus, das entsprechend konfiguriert ist, um Benutzern eine andere Anmeldemöglichkeit zu erlauben.

Netzwerkeinstellungen

Die Netzwerkeinstellungen definieren die IP-Adressen, Sicherheitsgruppen und Netzwerkschnittstellen für Ihre Instances. Sie können die Standard-Netzwerkeinstellungen verwenden oder sie nach Bedarf konfigurieren.

- (Nur Launch Instance Wizard) VPC: Wählen Sie eine vorhandene VPC für Ihre Instance. Die Standard-VPC für die Region ist standardmäßig ausgewählt. Alternativ können Sie eine VPC auswählen, die Sie erstellt haben oder die mit Ihnen geteilt wurde. Weitere Informationen finden Sie unter Virtual Private Clouds für Ihre EC2-Instances.
- Subnetz: Wählen Sie ein Subnetz für Ihre Instance oder wählen Sie Neues Subnetz erstellen, um mit der Amazon VPC-Konsole ein neues Subnetz zu erstellen.
  - Sie können ein Subnetz in einer Availability Zone, einer Local Zone, einer Wavelength-Zone oder einer Outpost-Zone für die ausgewählte VPC erstellen.
  - Um die Instance IPv6 nur in einem Subnetz zu starten, muss es sich bei der Instance um eine Nitro-basierte Instance handeln.
- (Nur Instanzassistent starten) Öffentliche IP automatisch zuweisen: Aktiviert oder deaktiviert die automatische Zuweisung von öffentlichen IPv4 Adressen. Beim Start von Instances in einem Standard-Subnetz lautet der Standardwert Aktivieren. Beim Start von Instances in einem abweichenden Subnetz lautet der Standardwert Deaktivieren. Weitere Informationen finden Sie unter Öffentliche IPv4-Adressen.

  Sie können diese Option nicht für nicht standardmäßige Subnetze aktivieren, wenn Sie eine sekundäre Netzwerkschnittstelle hinzufügen. Weitere Informationen finden Sie unter the section called “Eine öffentliche IPv4-Adresse beim Start zuweisen”.
- (Nur Instanzassistent starten) IPv6 IP automatisch zuweisen: Aktiviert oder deaktiviert die automatische Zuweisung von IPv6 Adressen. Weitere Informationen finden Sie unter IPv6-Adressen.
- Firewall (Sicherheitsgruppen): Sie können eine vorhandene Sicherheitsgruppe auswählen oder eine neue erstellen. Stellen Sie sicher, dass Ihre Sicherheitsgruppe über Regeln verfügt, die den Datenverkehr zu und von Ihren Instances zulassen. Der gesamte übrige Datenverkehr wird ignoriert.

  Wenn Sie eine neue Sicherheitsgruppe erstellen, erstellen wir automatisch eine eingehende Regel, die es Ihnen ermöglicht, von allen IP-Adressen aus über SSH (Linux-Instances) oder RDP (Windows-Instances) eine Verbindung mit Ihrer Instance herzustellen. Sie können diese Regel nach Bedarf entfernen oder bearbeiten. Sie können Regeln nach Bedarf hinzufügen. Weitere Informationen finden Sie unter Sicherheitsgruppenregeln konfigurieren.

> **Warning**
>
> Regeln, die allen IP-Adressen den Zugriff auf die Instance über SSH oder RDP erlauben, sind akzeptabel, wenn Sie eine Test-Instance kurz starten und bald anhalten oder beenden. Diese Regeln sind für Produktionsumgebungen unsicher. Sie sollten nur einen bestimmten IP-Adressbereich für den Zugriff auf Ihre Instance autorisieren.

Diese Sicherheitsgruppe wird der primären Netzwerkschnittstelle und allen sekundären Netzwerkschnittstellen hinzugefügt. Sie können zusätzliche Sicherheitsgruppen für Ihre Netzwerkschnittstellen auswählen, aber Sie können die hier ausgewählte Gruppe nicht entfernen.

- Erweiterte Netzwerkkonfiguration – Sie können die primäre Netzwerkschnittstelle nach Bedarf konfigurieren. Wählen Sie zum Hinzufügen einer sekundären Netzwerkschnittstelle Netzwerkschnittstelle hinzufügen aus. Die Anzahl der Netzwerkschnittstellen, die Sie hinzufügen können, hängt vom ausgewählten Instance-Typ ab. Beachten Sie, dass dieser Abschnitt nur verfügbar ist, wenn Sie ein Subnetz auswählen.
  - Geräteindex: Der Geräteindex. Die primäre Netzwerkschnittstelle muss dem Index 0 zugewiesen sein.
  - Netzwerkschnittstelle: Die Netzwerkschnittstelle. Wählen Sie Neue Schnittstelle aus, damit Amazon eine neue Schnittstelle EC2 erstellen kann, oder wählen Sie eine vorhandene, verfügbare Netzwerkschnittstelle aus. Wenn Sie eine vorhandene Netzwerkschnittstelle als primäre Netzwerkschnittstelle auswählen, können Sie die automatische Zuweisung öffentlicher IP für nicht-standardmäßige Subnetze nicht aktivieren.
  - Beschreibung: Eine Beschreibung für die neue Netzwerkschnittstelle.
  - Subnet (Subnetz): Das Subnetz, in dem eine neue Netzwerkschnittstelle erstellt werden soll. Die Instance wird im selben Subnetz wie die primäre Netzwerkschnittstelle gestartet.

    Sie müssen ein Subnetz für eine sekundäre Netzwerkschnittstelle aus derselben Availability Zone wie das Subnetz für die primäre Netzwerkschnittstelle auswählen. Wenn Sie ein Subnetz in einer anderen VPC auswählen, wird die Bezeichnung Multi-VPC neben der Netzwerkschnittstelle angezeigt. Auf diese Weise können Sie mehrfach vernetzte Instances VPCs mit unterschiedlichen Netzwerk- und Sicherheitskonfigurationen erstellen.

    Um eine EC2 Instance IPv6 nur in einem Subnetz zu starten, müssen Sie eine Nitro-basierte Instance verwenden. Wenn Sie eine IPv6 Nur-Instance starten, ist es möglich, dass der Instanz

nicht DHCPv6 sofort der DNS-Nameserver zur Verfügung gestellt wird. IPv6 Während dieser anfänglichen Verzögerung kann die Instance möglicherweise keine öffentlichen Domains auflösen. Sie können die Konfigurationsdatei ändern und Ihr AMI neu abbilden, sodass die Datei sofort beim Booten die IPv6 DNS-Nameserveradresse hat.

- Sicherheitsgruppen: Die Sicherheitsgruppen, die der Netzwerkschnittstelle zugeordnet werden sollen. Sie müssen eine Sicherheitsgruppe aus derselben VPC wie dem Subnetz für die Netzwerkschnittstelle auswählen.
- (Nur Startvorlagen) Öffentliche IP automatisch zuweisen: Geben Sie an, ob Ihre Instance eine öffentliche Adresse erhält. IPv4 Standardmäßig erhalten Instances in einem Standardsubnetz eine öffentliche IPv4 Adresse und Instances in einem nicht standardmäßigen Subnetz nicht. Sie können Enable oder Disable auswählen, um die Standardeinstellungen des Subnetzes zu überschreiben. Weitere Informationen finden Sie unter Öffentliche IPv4-Adressen.
- Primäre IP: Eine private IPv4 Adresse aus dem Bereich Ihres Subnetzes. Lassen Sie das Feld leer, damit Amazon eine IPv4 Privatadresse für Sie EC2 auswählt.
- Sekundäre IP: Zusätzliche private IPv4 Adressen aus dem Bereich Ihres Subnetzes. Wählen Sie Manuell zuweisen und geben Sie eine IPv4 Adresse ein. Wählen Sie IP hinzufügen, um eine weitere IPv4 Adresse hinzuzufügen. Wählen Sie alternativ Automatisch zuweisen und geben Sie einen Wert ein, um die Anzahl der IPv4 Adressen anzugeben, die Amazon für Sie EC2 auswählt.
- (IPv6-only) IPv6 IPs: IPv6 Adressen aus dem Bereich des Subnetzes. Wählen Sie Manuell zuweisen und geben Sie eine Adresse ein IPv6 . Wählen Sie IP hinzufügen, um eine weitere IPv6 Adresse hinzuzufügen. Wählen Sie alternativ Automatisch zuweisen und geben Sie einen Wert ein, um die Anzahl der IPv6 Adressen anzugeben, die Amazon für Sie EC2 auswählt.
- IPv4 Präfixe: Die IPv4 Präfixe für die Netzwerkschnittstelle. Wählen Sie Manuell zuweisen und geben Sie ein Präfix ein IPv4. Wählen Sie alternativ Automatisch zuweisen und geben Sie einen Wert ein, um die Anzahl der IPv4 Präfixe anzugeben, die Amazon für Sie EC2 auswählt.
- IPv6 Präfixe: Die IPv6 Präfixe für die Netzwerkschnittstelle. Wählen Sie Manuell zuweisen und geben Sie ein Präfix ein IPv6. Wählen Sie alternativ Automatisch zuweisen und geben Sie einen Wert ein, um die Anzahl der IPv6 Präfixe anzugeben, die Amazon für Sie EC2 auswählt.
- (IPv6Nur Dual-Stack) Primäre IPv6 IP zuweisen: Wenn Sie ein Dual-Stack-Subnetz oder ein IPv6 Nur-Dual-Stack-Subnetz auswählen, weisen Sie eine primäre Adresse zu. IPv6 Auf diese Weise können Störungen des Datenverkehrs zur Instance oder Netzwerkschnittstelle vermieden werden. Aktivieren Sie diese Option, wenn Sie darauf angewiesen sind, dass sich die Adresse nicht ändert. IPv6 Sie können die primäre IPv6 Adresse später nicht entfernen. Wenn Sie eine IPv6 GUA-Adresse als primäre Adresse aktivieren IPv6, wird die erste IPv6 GUA zur primären IPv6 Adresse, bis die Instance beendet oder die Netzwerkschnittstelle getrennt wird. Wenn

Sie mehrere IPv6 Adressen mit einer Netzwerkschnittstelle verknüpft haben und Amazon eine primäre IPv6 Adresse EC2 zuweisen lassen, ist die erste der Netzwerkschnittstelle zugeordnete IPv6 GUA-Adresse die primäre IPv6 Adresse.

- Bei Beenden löschen: Wählen Sie aus, ob die Netzwerkschnittstelle gelöscht werden soll, wenn die Instance gelöscht wird.
- Schnittstellentyp: Der Netzwerkschnittstellentyp:
  - ENA: Eine leistungsstarke Netzwerkschnittstelle, die entwickelt wurde, um hohen Durchsatz und hohe packet-per-second TCP/IP Protokollraten zu bewältigen und gleichzeitig die CPU-Auslastung zu minimieren. Dies ist der Standardwert. Weitere Informationen über ENA finden Sie unter Elastic Network Adapter.
  - EFA mit ENA: Eine Netzwerkschnittstelle, die sowohl ENA- als auch EFA-Geräte für den herkömmlichen Transport sowie für den TCP/IP SRD-basierten Transport unterstützt. Weitere Informationen zu EFA finden Sie unter Elastic Fabric Adapter.
  - Nur EFA: Eine leistungsstarke Netzwerkschnittstelle, die für die Kommunikation zwischen Knoten mit hohem Durchsatz und geringer Latenz für SRD-basierten Transport konzipiert ist und gleichzeitig den Betriebssystemstapel umgeht. Nur-EFA-Netzwerkschnittstellen unterstützen keine IP-Adressen. Weitere Informationen zu EFA finden Sie unter Elastic Fabric Adapter.
- Elastic Fabric Adapter: Gibt an, ob die Netzwerkschnittstelle ein Elastic Fabric Adapter ist. Weitere Informationen finden Sie unter Elastic Fabric Adapter für AI/ML und HPC-Workloads bei Amazon EC2.
- Network card index (Netzwerkkarten-Index): Der Index der Netzwerkkarte. Die primäre Netzwerkschnittstelle muss dem Netzwerkkartenindex 0 zugewiesen sein. Einige Instance-Typen unterstützen mehrere Netzwerkkarten.
- ENA Express: ENA Express basiert auf der SRD-Technologie (AWS Scalable Reliable Datagram). Die SRD-Technologie verwendet einen Paketverteilungsmechanismus, um die Last zu verteilen und Netzwerküberlastungen zu vermeiden. Durch die Aktivierung von ENA Express können unterstützte Instances zusätzlich zu regulärem TCP-Datenverkehr auch SRD für die Kommunikation verwenden (sofern möglich). Der Launch Instance Wizard enthält keine ENA-Express-Konfiguration für die Instance, es sei denn, Sie wählen in der Liste die Option Aktivieren oder Deaktivieren aus.
- ENA Express UDP: Wenn Sie ENA Express aktiviert haben, können Sie es optional für UDP-Datenverkehr verwenden. Der Launch Instance Wizard oder die Startvorlage enthalten keine ENA-Express-Konfiguration für die Instance, es sei denn, Sie wählen in der Liste die Option Aktivieren oder Deaktivieren aus.

Speicher konfigurieren

Die von Ihnen ausgewählte AMI beinhaltet ein oder mehrere Speicher-Volumes, einschließlich eines Root-Volumes. Sie können zusätzliche Volumes angeben, die an die Instance angehängt werden sollen.

(Nur Launch Instance Wizard) Sie können die einfache oder erweiterte Ansicht verwenden. Mit der einfachen Simple-Ansicht legen Sie die Größe und Art des Volumes fest. Um alle Volume-Parameter anzugeben, verwenden Sie die Ansicht Erweitert oben rechts auf der Karte.

In der erweiterten Ansicht können Sie jedes Volume wie folgt konfigurieren:

- Storage type (Speichertyp): Wählen Sie Amazon-EBS- oder Instance-Speicher-Volumes aus, um sie Ihrer Instance zuzuordnen. Die in der Liste verfügbaren Volume-Typen hängen von dem Instance-Typ ab, den Sie ausgewählt haben. Weitere Informationen finden Sie unter Instance-Speicher temporärer Speicher auf Blockebene für EC2-Instances und Amazon-EBS-Volumes.
- Device name (Gerätename): Wählen Sie aus der Liste verfügbarer Gerätenamen für das Volume einen Eintrag aus.
- Snapshot: Wählen Sie den Snapshot aus, von dem das Volume wiederhergestellt werden soll. Sie können nach verfügbaren freigegebenen und öffentlichen Snapshots suchen, indem Sie Text in das Feld Snapshot eingeben.
- Größe (GiB): Sie können für EBS-Volumes eine Speichergröße angeben.
- Volume Type (Volume-Typ): Wählen Sie für die EBS-Volumes einen Volume-Typ aus. Weitere Informationen finden Sie unter Amazon-EBS-Volume-Typen im Amazon-EBS-Benutzerhandbuch.
- IOPS: Wenn Sie den Volumetyp io1, io2 oder gp3 ausgewählt haben, können Sie die Anzahl der I/O Operationen pro Sekunde (IOPS) eingeben, die das Volume unterstützen kann. Erforderlich für io1-, io2- und gp3-Volumes. Wird bei gp2-, st1-, sc1- oder Standard-Volumes nicht unterstützt. Wenn Sie diesen Parameter für die Startvorlage weglassen, müssen Sie einen Wert dafür angeben, wenn Sie eine Instance über die Startvorlage starten.
- Delete on termination (Bei Beendigung löschen): Wählen Sie für Amazon-EBS-Volumes Ja, um das Volume zu löschen, wenn die Instance beendet wird oder wählen Sie Nein, um das Volume beizubehalten. Weitere Informationen finden Sie unter Daten beim Beenden einer Instance aufbewahren.
- Encrypted (Verschlüsselt): Wenn der Instance-Typ die EBS-Verschlüsselung unterstützt, können Sie Ja auswählen, um die Verschlüsselung für das Volume zu aktivieren. Wenn Sie für diese Region die standardmäßige Verschlüsselung aktiviert haben, wird der Standard-CMK für Sie

ausgewählt. Weitere Informationen finden Sie unter Amazon-EBS-Verschlüsselung im Amazon-EBS-Benutzerhandbuch.

- KMS key (KMS-Schlüssel): Wenn Sie Yes (Ja) für Encrypted (Verschlüsselt) ausgewählt haben, müssen Sie einen kundenverwalteten Schlüssel zum Verschlüsseln des Volumes auswählen. Wenn die für diese Region die standardmäßige Verschlüsselung aktiviert haben, wird der Standard-CMK für Sie ausgewählt. Sie können einen anderen Schlüssel auswählen oder den ARN eines Kundenverwaltungsschlüssels angeben, den Sie erstellt haben.
- Durchsatz: Wenn Sie den Volume-Typ gp3 ausgewählt haben, können Sie den Durchsatz, den das Volume unterstützen kann, in MiB/s eingeben.
- Volume-Initialisierungsrate: Wenn Sie einen Snapshot ausgewählt haben, können Sie optional die Volume-Initialisierungsrate in MiB/s angeben, mit der die Snapshot-Blöcke von Amazon S3 auf das Volume heruntergeladen werden sollen. Weitere Informationen finden Sie unter Verwendung einer von Amazon EBS bereitgestellte Rate für die Volume-Initialisierung. Um die Standard-Initialisierungsrate oder die schnelle Snapshot-Wiederherstellung zu verwenden (sofern sie für den ausgewählten Snapshot aktiviert ist), geben Sie keine Rate an.
- Dateisysteme: Hängen Sie ein Amazon EFS- oder FSx Amazon-Dateisystem in die Instance ein. Weitere Informationen zum Bereitstellen eines Amazon-EFS-Dateisystems finden Sie unter Amazon EFS mit Amazon-EC2-Linux-Instances verwenden. Weitere Informationen zum Mounten eines FSx Amazon-Dateisystems finden Sie unter Amazon FSx mit Amazon-EC2-Instances verwenden

Erweiterte Details

Erweitern Sie für Advanced details (Erweiterte Details) den Bereich zur Ansicht der Felder und geben Sie zusätzliche Parameter für die Instance an.

- (Nur beim Assistenten zum Starten von Instances) Domain-Join-Verzeichnis: Wählen Sie das Directory Service Verzeichnis (Domain) aus, zu dem Ihre Instance nach dem Start hinzugefügt wird. Wenn Sie eine Domain auswählen, müssen Sie eine IAM Rolle mit den erforderlichen Berechtigungen auswählen. Weitere Informationen zum Domänenbeitritt finden Sie unter Nahtloses Verbinden einer Amazon EC2 Linux-Instance mit Ihrem AWS verwalteten Microsoft AD-Verzeichnis (Linux-Instances) und Nahtloses Verbinden einer Amazon EC2 Windows-Instance mit Ihrem AWS verwalteten Microsoft AD-Verzeichnis (Windows-Instances).
- IAM-Instance-Profil: Wählen Sie ein IAM-Instance-Profil, das der Instance zugeordnet werden soll. Dies ist ein Container für eine IAM-Rolle. Weitere Informationen finden Sie unter IAM-Rollen für Amazon EC2.

- Hostname type (Hostnamentyp): Wählen Sie aus, ob der Hostname des Gastbetriebssystems der Instance der Ressourcenname oder der IP-Name sein soll. Weitere Informationen finden Sie unter Hostnamen und Domains der EC2-Instance.
- DNS-Hostname: Legt fest, ob die DNS-Abfragen zum Ressourcennamen oder zum IP-Namen (je nachdem, was Sie als Hostnamentyp ausgewählt haben) mit der IPv4 Adresse (A-Eintrag), der IPv6 Adresse (AAAA-Eintrag) oder beidem antworten. Weitere Informationen finden Sie unter Hostnamen und Domains der EC2-Instance.
- Automatische Instance-Wiederherstellung: Wenn diese Option aktiviert ist, wird Ihre Instance wiederhergestellt, falls die Systemstatusprüfungen fehlschlagen. Diese Einstellung ist standardmäßig beim Start für unterstützte Instance-Typen aktiviert. Weitere Informationen finden Sie unter Konfigurieren Sie die vereinfachte automatische Wiederherstellung auf einer EC2 Amazon-Instance.
- Shutdown behavior: Wählen Sie aus, ob die Instance beim Herunterfahren angehalten oder beendet werden soll. Weitere Informationen finden Sie unter Ändern des durch die Instance initiierten Abschaltverhaltens.
- Stop - Hibernate behavior (Stopp – Verhalten im Ruhezustand): Um den Ruhezustand zu aktivieren, wählen Sie Enable (Aktivieren). Dieses Feld ist nur verfügbar, wenn Ihre Instance die Voraussetzungen für den Ruhezustand erfüllt. Weitere Informationen finden Sie unter Versetzen Sie Ihre Amazon-Instance in den Ruhezustand EC2 .
- Termination protection (Beendigungsschutz): Um ein versehentliches Beenden zu verhindern, wählen Sie Aktivieren. Weitere Informationen finden Sie unter Beendigungsschutz für Instances ändern.
- Stop protection (Stoppschutz): Um ein versehentliches Anhalten zu verhindern, wählen Sie Enable (Aktivieren). Weitere Informationen finden Sie unter Aktivieren des Stopp-Schutzes.
- Detaillierte CloudWatch Überwachung: Wählen Sie Aktivieren, um die detaillierte Überwachung Ihrer Instance mithilfe von Amazon zu aktivieren CloudWatch. Es fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter Überwachen Sie Ihre Instances mit CloudWatch.
- Guthabenspezifikation: Wählen Sie Unbegrenzt aus, damit Anwendungen so lange wie nötig über die Baseline hinaus laufen können. Dieses Feld gilt nur für T-Instances. Zusätzliche Gebühren können anfallen. Weitere Informationen finden Sie unter Burstable Performance Instances.
- Platzierungsgruppe: Geben Sie eine Platzierungsgruppe an, in der die Instance gestartet werden soll. Wählen Sie eine vorhandene Platzierungsgruppe aus oder erstellen Sie eine neue. Nicht alle Instance-Typen unterstützen das Starten einer Instance in einer Platzierungsgruppe. Weitere Informationen finden Sie unter Platzierungsgruppen für Ihre Amazon-EC2-Instances.

- EBS-optimierte Instance: Eine Amazon-EBS-optimierte Instance verwendet einen optimierten Konfigurations-Stack und bietet zusätzliche, dedizierte Kapazität für Amazon EBS I/O. Wenn der Instance-Typ dieses Feature unterstützt, wählen Sie Aktivieren, um sie zu aktivieren. Es fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter the section called “EBS-Optimierung”.
- Konfiguration der Instance-Bandbreite: Sie können entweder Ihre Netzwerkbandbreite oder Ihre EBS-Bandbreite erhöhen. Nur für unterstützte Instance-Typen. Weitere Informationen finden Sie unter EC2 Konfiguration der Gewichtung der Instanz-Bandbreite.
- Kaufoption: Wählen Sie Spot Instances, um Spot-Instances zum Spot-Preis anzufordern, der auf den On-Demand-Preis begrenzt ist, und wählen Sie Spot-Instance-Optionen anpassen, um die Standardeinstellungen für Spot Instance zu ändern. Sie können Ihren Höchstpreis festlegen (nicht empfohlen) und den Anforderungstyp, die Anforderungsdauer und das Unterbrechungsverhalten ändern. Wenn Sie keine Spot-Instance anfordern, EC2 startet Amazon standardmäßig eine On-Demand-Instance. Weitere Informationen finden Sie unter Ihre Spot Instances verwalten.
- Capacity Reservation (Kapazitätsreservierung): Geben Sie an, ob die Instance in einer beliebigen offenen Kapazitätsreservierung (Offen), einer bestimmten Kapazitätsreservierung (Ziel nach ID) oder einer Kapazitätsreservierungsgruppe (Ziel nach Gruppe) gestartet werden soll. Um anzugeben, dass keine Kapazitätsreservierung verwendet werden soll, wählen Sie None (Keine) aus. Weitere Informationen finden Sie unter Starten von Instances in einer bestehenden Kapazitätsreservierung.
- Tenancy: Wählen Sie aus, ob Ihre Instance auf einer gemeinsam genutzten (Shared), isolierten oder dedizierten (Dedicated) Hardware oder auf einem dedizierten Host Dedicated Host (Dedicated host) ausgeführt werden soll. Wenn Sie die Instance auf einem Dedicated Host starten möchten, können Sie angeben, ob die Instance in einer Hostressourcengruppe gestartet werden soll oder ob Sie eine bestimmte Dedicated Host verwenden möchten. Es können zusätzliche Gebühren anfallen. Weitere Informationen erhalten Sie unter Amazon-EC2-Dedicated-Instances und EC2 Dedizierte Amazon-Hosts.
- RAM-Disk-ID: (Nur gültig für paravirtual (PV) AMIs) Wählen Sie eine RAM-Disk für die Instance aus. Wenn Sie einen Kernel ausgewählt haben, müssen Sie möglicherweise eine bestimmte RAM-Disk zusammen mit den Treibern auswählen, die diese unterstützen.
- Kernel-ID: (Nur gültig für paravirtual (PV) AMIs) Wählen Sie einen Kernel für die Instanz aus.
- Nitro Enclave: Ermöglicht es Ihnen, isolierte Ausführungsumgebungen, sogenannte Enklaven, aus Amazon-Instances zu erstellen. EC2 Wählen Sie Aktivieren aus, um die Instance für Nitro Enclaves zu aktivieren. AWS Weitere Informationen finden Sie unter Was ist AWS Nitro Enclaves? im AWS Nitro Enclaves-Benutzerhandbuch.

- License configurations (Lizenzkonfigurationen): Sie können Instances für die angegebene Lizenzkonfiguration starten, um die Lizenznutzung nachzuverfolgen. Weitere Informationen finden Sie unter Erstellen einer Lizenzkonfiguration im Benutzerhandbuch zu AWS License Manager.
- CPU-Optionen angeben: Im Launch Instance Wizard ist dieses Feld nur sichtbar, wenn der ausgewählte Instance-Typ die Angabe von CPU-Optionen unterstützt. Wählen Sie „CPU-Optionen angeben“, um beim Start eine benutzerdefinierte Anzahl von v CPUs anzugeben. Legen Sie die Anzahl der CPU-Kerne und -Threads pro Kern fest. Weitere Informationen finden Sie unter CPU-Optionen für EC2 Amazon-Instances.
- Metadatenzugriff: Sie können den Zugriff auf den Instance Metadata Service (IMDS) aktivieren oder deaktivieren. Weitere Informationen finden Sie unter Konfigurieren von Instance-Metadatenoptionen für neue Instances.
- IPv6 Metadaten-Endpunkt: Sie können der Instance ermöglichen, die IPv6 IMDS-Adresse zum Abrufen von Instance-Metadaten `[fd00:ec2::254]` zu verwenden. Diese Option ist nur verfügbar, wenn Sie Nitro-basierte Instances in einem Subnetz starten, das von IPv6 -unterstützt wird (Dual-Stack oder nur). IPv6 Weitere Informationen zum Abrufen von Instance-Metadaten finden Sie unter Auf Instanz-Metadaten für eine EC2 Instanz zugreifen.
- Metadatenversion: Wenn Sie den Zugriff auf den IMDS aktivieren, können Sie festlegen, dass die Verwendung von Instance-Metadatenservice Version 2 beim Anfordern von Instance-Metadaten erforderlich ist. Weitere Informationen finden Sie unter Konfigurieren von Instance-Metadatenoptionen für neue Instances.
- Metadatenantwort-Hop-Limit: Wenn Sie den IMDS aktivieren, können Sie die zulässige Anzahl von Netzwerk-Hops für das Metadaten-Token festlegen. Weitere Informationen finden Sie unter Konfigurieren von Instance-Metadatenoptionen für neue Instances.
- Allow tags in metadata (Tags in Metadaten erlauben): Wenn Sie Enable (Aktivieren) auswählen, erlaubt die Instance den Zugriff auf alle ihre Tags aus ihren Metadaten. Wenn kein Wert angegeben wird, ist der Zugriff auf die Tags in Instance-Metadaten standardmäßig nicht erlaubt. Weitere Informationen finden Sie unter Zugriff auf Tags in Instance-Metadaten ermöglichen .
- User data: Sie können Benutzerdaten so festlegen, dass eine Instance während des Starts konfiguriert wird oder dass ein Konfigurationsskript ausgeführt wird. Weitere Informationen über Benutzerdaten für Linux-Instances finden Sie unter Befehle ausführen, wenn Sie eine EC2 Instance mit Benutzerdateneingabe starten. Weitere Informationen über Benutzerdaten für Windows-Instances finden Sie unter Wie Amazon EC2 mit Benutzerdaten für Windows-Instances umgeht.

Zusammenfassung

Verwenden Sie den Bereich Zusammenfassung, um die Anzahl der zu startenden Instances anzugeben, Ihre Instance-Konfiguration zu überprüfen und Ihre Instances zu starten.

- Number of instances: Geben Sie die Anzahl der Instances ein, die gestartet werden sollen. Alle Instances werden mit derselben Konfiguration gestartet.

  > **Tip**
  >
  > Um sicherzustellen, dass Instances schneller gestartet werden, unterteilen Sie große Anforderungen in kleinere Batches. Erstellen Sie beispielsweise fünf separate Startanforderungen für jeweils 100 Instances anstelle von einer Startanforderung für 500 Instances.

- (Optional) Wenn Sie mehr als eine Instance angeben, können Sie Amazon Auto Scaling zur Erstellung einer Startvorlage und einer EC2 Amazon EC2 Auto Scaling-Gruppe in Betracht ziehen, um sicherzustellen, dass Sie die richtige Anzahl von Instances beibehalten, um den Bedarf an Ihrer Anwendung zu decken. EC2 Amazon EC2 Auto Scaling skaliert die Anzahl der Instances in der Gruppe gemäß Ihren Spezifikationen. Weitere Informationen finden Sie im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

  > **Note**
  >
  > Wenn EC2 Amazon EC2 Auto Scaling eine Instance, die sich in einer Amazon EC2 Auto Scaling Scaling-Gruppe befindet, als fehlerhaft markiert, wird die Instance automatisch als Ersatz eingeplant, wo sie beendet und eine andere gestartet wird, und Sie verlieren Ihre Daten auf der ursprünglichen Instance. Eine Instance wird als fehlerhaft markiert, wenn Sie die Instance beenden oder neu starten oder wenn ein anderes Ereignis die Instance als fehlerhaft markiert. Weitere Informationen finden Sie unter Zustandsprüfungen für Instances in einer Amazon EC2 Auto Scaling Scaling-Gruppe im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

- Überprüfen Sie die Details Ihrer Instance und nehmen Sie ggf. Änderungen vor. Sie können direkt zu einem Abschnitt navigieren, indem Sie den entsprechenden Link im Bereich Zusammenfassung auswählen.
- Wenn Sie bereit sind, Ihre Instance zu starten, wählen Sie Instance starten aus.

EC2-Instance mit dem Launch Instance Wizard in der Konsole starten

Sie können eine Amazon-EC2-Instance mit dem Launch Instance Wizard in der Amazon-EC2-Konsole starten. Der Assistent bietet Standardwerte für die Startparameter, die Sie entweder akzeptieren oder Ihren Anforderungen entsprechend ändern können. Der einzige Parameter, der nicht angegeben ist, ist das Schlüsselpaar. Wenn Sie die Standardwerte akzeptieren, können Sie eine Instance starten, indem Sie nur ein Schlüsselpaar auswählen.

> **Important**
>
> Ihnen werden Gebühren für die Instance berechnet, während sich die Instance im `running`-Zustand befindet, auch wenn sie inaktiv bleibt. Wenn Sie sich jedoch für das kostenlose Kontingent qualifizieren, fallen möglicherweise keine Gebühren an. Weitere Informationen finden Sie unter Verfolgen Sie Ihre Nutzung des kostenlosen Kontingents für Amazon EC2.

Eine Beschreibung der einzelnen Parameter im Launch Instance Wizard finden Sie unter Referenz für EC2 Amazon-Instance-Konfigurationsparameter.

Themen

- Starten Sie schnell eine Instance
- Starten einer Instance mit definierten Parametern

Starten Sie schnell eine Instance

Gehen Sie folgendermaßen vor, um eine Instance zu Testzwecken schnell einzurichten. Sie wählen das Betriebssystem und Ihr Schlüsselpaar aus und akzeptieren die Standardwerte. Mit Ausnahme des Schlüsselpaars stellt der Launch Instance Wizard Standardwerte für alle Parameter bereit. Sie können eine oder alle Standardeinstellungen akzeptieren oder eine Instance konfigurieren, indem Sie für jeden Parameter eigene Werte angeben.

Eine Beschreibung der einzelnen Parameter im Launch Instance Wizard finden Sie unter Referenz für EC2 Amazon-Instance-Konfigurationsparameter.

So führen Sie den Schnellstart einer Instance mithilfe des Launch Instance Wizard durch

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Auf der Navigationsleiste oben im Bildschirm wird die aktuelle AWS-Region angezeigt (beispielsweise USA Ost (Ohio)). Falls benötigt, wählen Sie eine Region aus, in die die Instance gestartet werden soll.
3. Wählen Sie im Dashboard der Amazon EC2-Konsole die Option Instance starten aus.
4. (Optional) Geben Sie unter Name und Tags für Name einen beschreibenden Namen für Ihre Instance ein.
5. Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) Quick Start und dann das Betriebssystem (OS) für Ihre Instance aus.
6. Wählen Sie unter Schlüsselpaar (Anmeldung) für Schlüsselpaarname ein vorhandenes Schlüsselpaar aus oder erstellen Sie ein neues.
7. Wählen Sie in der Übersicht Launch instance (Instance starten) aus.

Starten einer Instance mit definierten Parametern

Wenn Sie eine Instance starten, die Sie in der Produktion verwenden möchten, müssen Sie die Instance entsprechend Ihren Anforderungen konfigurieren. Eine Beschreibung der einzelnen Parameter im Launch Instance Wizard finden Sie unter Referenz für EC2 Amazon-Instance-Konfigurationsparameter.

So starten Sie eine Instance, indem Sie alle Startparameter mit dem Launch Instance Wizard festlegen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Auf der Navigationsleiste oben im Bildschirm wird die aktuelle AWS-Region angezeigt (beispielsweise USA Ost (Ohio)). Falls benötigt, wählen Sie eine Region aus, in die die Instance gestartet werden soll.
3. Wählen Sie im Dashboard der Amazon EC2-Konsole die Option Instance starten aus.
4. (Optional) Geben Sie unter Name and Tags für Name einen beschreibenden Namen für die Instance ein, sodass Sie den Überblick behalten.

   Der Instance-Name ist ein Tag, wobei der Schlüssel Name ist und es sich bei dem Wert um den von Ihnen angegebenen Namen handelt.
5. Wählen Sie unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image) das Betriebssystem (OS) für Ihre Instance aus und wählen Sie dann eine AMI aus.

Ein AMI ist eine Vorlage, die das Betriebssystem und die Software enthält, die zum Starten einer Instance erforderlich sind.

6. Wählen Sie unter EC2 Instance Type (EC2-Instance-Typ) einen Instance-Typ aus.

   Der Instance-Typ bestimmt die Hardware-Konfiguration (CPU, Arbeitsspeicher, Speicher und Netzwerkkapazität) und die Größe des Host-Computers, der für eine Instance verwendet wird.

   Wenn Sie sich nicht sicher sind, welchen Instance-Typ Sie auswählen sollen, gehen Sie folgendermaßen vor:

   - Wählen Sie Instance-Typen vergleichen, um verschiedene Instance-Typen anhand der folgenden Attribute zu vergleichen: Anzahl der vCPUs, Architektur, Arbeitsspeichermenge (GiB), Speichermenge (GB), Speichertyp und Netzwerkleistung.
   - Wählen Sie Beratung einholen, um Anleitungen und Vorschläge für Instance-Typen vom EC2-Instance-Typ-Suche zu erhalten. Weitere Informationen finden Sie unter Holen Sie sich Empfehlungen vom EC2-Instance-Typ-Finder.

   > **Note**
   >
   > Je nachdem, wann Sie Ihr Konto erstellt haben, können Sie Instance-Typen im Rahmen des kostenlosen Kontingents möglicherweise kostenlos nutzen. Diese Instance-Typen sind als Für das kostenlose Kontingent berechtigt gekennzeichnet.
   > Wenn Sie Ihr AWS-Konto vor dem 15. Juli 2025 erstellt haben und es weniger als 12 Monate alt ist, können Sie Amazon EC2 im kostenlosen Kontingent verwenden, indem Sie den Instance-Typ t2.micro auswählen, oder den Instance-Typ t3.micro in Regionen, in denen t2.micro nicht verfügbar ist. Beachten Sie, dass beim Starten einer t3.micro-Instance standardmäßig der Modus Unlimited verwendet wird, wodurch je nach CPU-Auslastung zusätzliche Gebühren anfallen können.
   > Wenn Sie Ihr AWS-Konto am oder nach dem 15. Juli 2025 erstellt haben, können Sie die Instance-Typen t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large und m7i-flex.large 6 Monate verwenden, oder bis Ihr Guthaben aufgebraucht ist.
   > Weitere Informationen finden Sie unter Vorteile des kostenlosen Kontingents vor und nach dem 15. Juli 2025.

7. Wählen Sie unter Schlüsselpaar (Anmeldung) für Schlüsselpaarname ein vorhandenes Schlüsselpaar aus oder erstellen Sie ein neues. Wenn Sie kein Schlüsselpaar benötigen, um

eine Verbindung zu Ihrer Instance herzustellen, können Sie Ohne Schlüsselpaar fortfahren (nicht empfohlen) wählen.

8. Unter Netzwerkeinstellungen können Sie die Standardeinstellungen beibehalten, wenn Sie eine Test-Instance starten. Wenn Sie eine Produktions-Instance starten, empfiehlt es sich, den ein- und ausgehenden Datenverkehr mithilfe der von Ihnen definierten Netzwerkeinstellungen und Sicherheitsgruppen zu kontrollieren.
9. Unter Speicher konfigurieren können Sie die Standardeinstellungen beibehalten oder zusätzlichen Speicher angeben. Die von Ihnen ausgewählte AMI beinhaltet ein oder mehrere Speicher-Volumes, einschließlich eines Root-Volumes. Sie können zusätzliche Volumes angeben, die an die Instance angehängt werden sollen.

   Sie können die Ansicht Einfach oder Erweitert verwenden. Mit der einfachen Simple-Ansicht legen Sie die Größe und Art des Volumes fest. Um alle Volume-Parameter anzugeben, verwenden Sie die Ansicht Erweitert oben rechts auf der Karte.
10. Erweitern Sie für Erweiterte Details den Bereich zur Ansicht der Felder und geben Sie zusätzliche Parameter für die Instance an.
11. Sie können im Bereich Zusammenfassung folgende Aktionen ausführen:

    a. Die Anzahl der zu startenden Instances angeben.

    b. Ihre Instance-Konfiguration überprüfen und direkt zu einem Abschnitt navigieren, indem Sie den entsprechenden Link auswählen.

    c. Wenn Sie bereit sind, Ihre Instance zu starten, wählen Sie Instance starten aus.

    Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Fehlerbehebung bei Amazon-EC2-Instances.
12. (Optional) Sie können eine Abrechnungswarnung für die Instance erstellen. Wählen Sie auf dem Bestätigungsbildschirm unter Next Steps (Nächste Schritte) die Option Create billing alerts (Gebührenlimit-Warnungen erstellen) aus und befolgen Sie die Anweisungen. Gebührenlimit-Warnungen können auch nach dem Start der Instance erstellt werden. Weitere Informationen finden Sie unter Erstellen eines Rechnungsalarms zur Überwachung Ihrer geschätzten AWS-Gebühren im Amazon-CloudWatch-Benutzerhandbuch.

Starten Sie EC2 Instances mithilfe einer Startvorlage

Eine EC2 Amazon-Startvorlage speichert Instance-Startparameter, sodass Sie sie nicht bei jedem Start einer Instance angeben müssen.

Einige Instance-Startservices können beim Starten von Instances optional Startvorlagen verwenden, während bei anderen Services, wie EC2 Fleet, Instances nur gestartet werden können, wenn eine Startvorlage verwendet wird. In diesem Thema wird beschrieben, wie Sie eine Startvorlage verwenden, wenn Sie eine Instance mit dem EC2 Launch-Instance-Assistenten, Amazon EC2 Amazon EC2 Auto Scaling, EC2 Fleet und Spot Fleet starten.

Weitere Informationen zum Erstellen einer Startvorlage finden Sie unter Instance-Startparameter in EC2 Amazon-Startvorlagen speichern.

Themen

- Starten Sie eine EC2 Amazon-Instance mithilfe einer Startvorlage
- Starten Sie Instances in einer Amazon EC2 Auto Scaling Scaling-Gruppe mithilfe einer Startvorlage
- Starten Sie eine EC2 Flotte mithilfe einer Startvorlage
- Eine Spot-Flotte über eine Startvorlage starten

Starten Sie eine EC2 Amazon-Instance mithilfe einer Startvorlage

Sie können die in einer Startvorlage enthaltenen Parameter verwenden, um eine EC2 Amazon-Instance zu starten. Nachdem Sie die Startvorlage ausgewählt haben, aber bevor Sie die Instance starten, können Sie die Startparameter ändern.

Zu Instances, die über eine Startvorlage gestartet werden, werden automatisch zwei Tags mit den Schlüsseln `aws:ec2launchtemplate:id` und `aws:ec2launchtemplate:version` zugewiesen. Diese Tags können nicht entfernt oder bearbeitet werden.

Console

So starten Sie eine Instance mithilfe einer Startvorlage

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie eine der folgenden Optionen, um die Startvorlage auszuwählen:

- Wählen Sie im Dashboard der EC2 Amazon-Konsole den Abwärtspfeil neben Launch Instance aus, wählen Sie Launch Instance from template aus und wählen Sie dann für Source template eine Startvorlage aus.
- Wählen Sie im Navigationsbereich Startvorlagen, wählen Sie die Startvorlage aus und wählen Sie Aktionen, Instance von Vorlage starten aus.

3. Wählen Sie unter Source template version (Quellvorlagenversion) die zu verwendende Startvorlagenversion aus.
4. (Optional) Sie können die Werte für jeden der Startparameter ändern. Wenn Sie einen Wert nicht ändern, wird der in der Startvorlage definierte Wert verwendet. Wenn in der Startvorlage kein Wert angegeben wurde, wird der Standardwert für den Parameter verwendet.
5. Geben Sie im Bereich Zusammenfassung für Anzahl der Instances die Anzahl der Instances ein, die gestartet werden sollen.
6. Wählen Sie Launch Instance (Instance starten) aus.

   Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Fehlerbehebung bei Amazon-EC2-Instances.

AWS CLI

So starten Sie eine Instance über eine Startvorlage

- Geben Sie mit dem Befehl run-instances den Parameter `--launch-template` an. Optional können Sie die zu verwendende Startvorlagenversion angeben. Wenn Sie keine Version angeben, wird die Standardversion verwendet.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123,Version=1
```

- Um einen Parameter der Startvorlage zu übersteuern, geben Sie den Parameter im Befehl run-instances an. Das folgende Beispiel übersteuert den Instance-Typ, der in der Startvorlage angegeben wird (sofern zutreffend).

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --instance-type t2.small
```

- Wenn Sie einen verschachtelten Parameter angeben, der Teil einer komplexen Struktur ist, wird die Instance wie in der Startvorlage angegeben mittels der komplexen Struktur sowie aller zusätzlichen von Ihnen angegebenen verschachtelten Parameter gestartet.

  Im folgenden Beispiel wird die Instance mit dem Tag (Markierung) *Owner*=*TeamA* sowie allen anderen Tags (Markierungen), die in der Startvorlage angegeben werden, gestartet. Wenn in der Startvorlage ein Tag (Markierung) mit dem Schlüssel *Owner* vorhanden ist, wird der Wert durch *TeamA* ersetzt.

  ```
  aws ec2 run-instances \
      --launch-template LaunchTemplateId=lt-0abcd290751193123 \
      --tag-specifications "ResourceType=instance,Tags=[{Key=Owner,Value=TeamA}]"
  ```

  Im folgenden Beispiel wird die Instance mit einem Volume mit dem Gerätenamen */dev/xvdb* sowie beliebigen anderen Blockgerät-Zuweisungen gestartet, die in der Startvorlage angegeben werden. Wenn in der Startvorlage ein für */dev/xvdb* definiertes Volume vorhanden ist, werden dessen Werte durch die angegebenen Werte ersetzt.

  ```
  aws ec2 run-instances \
      --launch-template LaunchTemplateId=lt-0abcd290751193123 \
      --block-device-mappings "DeviceName=/dev/
  xvdb,Ebs={VolumeSize=20,VolumeType=gp2}"
  ```

Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Fehlerbehebung bei Amazon-EC2-Instances.

PowerShell

So starten Sie eine Instance über eine Startvorlage mithilfe der AWS -Tools für PowerShell

- Verwenden Sie den New-EC2Instance-Befehl und geben Sie den `-LaunchTemplate`-Parameter an. Optional können Sie die zu verwendende Startvorlagenversion angeben. Wenn Sie keine Version angeben, wird die Standardversion verwendet.

  ```
  Import-Module AWS.Tools.EC2
  New-EC2Instance `
      -LaunchTemplate (
          New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
  Property @{
              LaunchTemplateId = 'lt-0abcd290751193123';
  ```

```
            Version          = '4'
    }
)
```

- Um einen Startvorlagenparameter zu überschreiben, geben Sie den Parameter im New-EC2InstanceBefehl an. Das folgende Beispiel übersteuert den Instance-Typ, der in der Startvorlage angegeben wird (sofern zutreffend).

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
)
```

- Wenn Sie einen verschachtelten Parameter angeben, der Teil einer komplexen Struktur ist, wird die Instance wie in der Startvorlage angegeben mittels der komplexen Struktur sowie aller zusätzlichen von Ihnen angegebenen verschachtelten Parameter gestartet.

  Im folgenden Beispiel wird die Instance mit dem Tag (Markierung) *Owner*=*TeamA* sowie allen anderen Tags (Markierungen), die in der Startvorlage angegeben werden, gestartet. Wenn in der Startvorlage ein Tag (Markierung) mit dem Schlüssel *Owner* vorhanden ist, wird der Wert durch *TeamA* ersetzt.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
        }
) `
    -TagSpecification (
        New-Object -TypeName Amazon.EC2.Model.TagSpecification -Property @{
            ResourceType = 'instance';
            Tags         = @(
```

```
                @{key = "Owner"; value = "TeamA" },
                @{key = "Department"; value = "Operations" }
            )
        }
)
```

Im folgenden Beispiel wird die Instance mit einem Volume mit dem Gerätenamen */dev/xvdb* sowie beliebigen anderen Blockgerät-Zuweisungen gestartet, die in der Startvorlage angegeben werden. Wenn in der Startvorlage ein für */dev/xvdb* definiertes Volume vorhanden ist, werden dessen Werte durch die angegebenen Werte ersetzt.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
) `
    -BlockDeviceMapping  (
        New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping -Property @{
            DeviceName = '/dev/xvdb';
            EBS        = (
                New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property @{
                    VolumeSize = 25;
                    VolumeType = 'gp3'
                }
            )
        }
)
```

Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Fehlerbehebung bei Amazon-EC2-Instances.

Starten Sie Instances in einer Amazon EC2 Auto Scaling Scaling-Gruppe mithilfe einer Startvorlage

Sie können eine Amazon EC2 Auto Scaling Scaling-Gruppe erstellen und eine Startvorlage angeben, die für die Gruppe verwendet werden soll. Wenn Amazon EC2 Auto Scaling Instances in der Amazon EC2 Auto Scaling Scaling-Gruppe startet, verwendet es die in der zugehörigen Startvorlage definierten Startparameter.

Bevor Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe mithilfe einer Startvorlage erstellen können, müssen Sie zunächst eine Startvorlage erstellen, die die Parameter enthält, die zum Starten einer Instance in einer Amazon EC2 Auto Scaling Scaling-Gruppe erforderlich sind. Einige Parameter sind erforderlich, z. B. die ID des AMI, und einige Parameter sind nicht für die Verwendung mit einer Amazon EC2 Auto Scaling Scaling-Gruppe verfügbar. Die Konsole bietet Anleitungen zur Erstellung einer Vorlage, die Sie mit Amazon EC2 Auto Scaling verwenden können.

So erstellen Sie mithilfe der Konsole eine Amazon EC2 Auto Scaling Scaling-Gruppe mit einer Startvorlage

- Anweisungen finden Sie unter Erstellen einer Auto Scaling Scaling-Gruppe mithilfe einer Startvorlage im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Um eine Amazon EC2 Auto Scaling Scaling-Gruppe mit einer Startvorlage zu erstellen oder zu aktualisieren, verwenden Sie den AWS CLI

- Verwenden Sie den update-auto-scaling-groupBefehl create-auto-scaling-groupoder und geben Sie den `--launch-template` Parameter an.

Weitere Informationen finden Sie in den folgenden Themen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch:

- Erstellen Sie eine Startvorlage für eine Amazon EC2 Auto Scaling Scaling-Gruppe
- Erstellen einer Startvorlage mithilfe erweiterter Einstellungen
- Beispiele für das Erstellen und Verwalten von Startvorlagen mit der AWS Command Line Interface (AWS CLI) – Enthält Beispiele, die zeigen, wie Startvorlagen mit verschiedenen Parameterkombinationen erstellt werden.
- Amazon EC2 Auto Scaling Scaling-Gruppen mithilfe von Startvorlagen erstellen
- Eine Amazon EC2 Auto Scaling Scaling-Gruppe aktualisieren

Starten Sie eine EC2 Flotte mithilfe einer Startvorlage

Eine Startvorlage ist eine Voraussetzung für die Erstellung einer EC2 Flottenanfrage. Wenn Amazon die EC2 Flottenanfrage EC2 erfüllt, verwendet es die Startparameter, die in der zugehörigen Startvorlage definiert sind. Sie können einige der Parameter überschreiben, die in der Startvorlage angegeben werden. Weitere Informationen finden Sie unter Erstellen Sie eine EC2 Flotte.

Um eine EC2 Flotte mit einer Startvorlage zu erstellen, verwenden Sie AWS CLI

- Verwenden Sie den Befehl create-fleet. Geben Sie mit dem Parameter `--launch-template-configs` die Startvorlage und alle Überschreibungen für die Startvorlage an.

Eine Spot-Flotte über eine Startvorlage starten

Eine Startvorlage ist optional, wenn Sie eine Spot-Flotten-Anforderung erstellen. Wenn Sie keine Startvorlage verwenden, können Sie die Startparameter manuell angeben. Wenn Sie eine Startvorlage verwenden und Amazon die Spot-Flotte-Anfrage EC2 erfüllt, verwendet Amazon die in der zugehörigen Startvorlage definierten Startparameter. Sie können einige der Parameter überschreiben, die in der Startvorlage angegeben werden. Weitere Informationen finden Sie unter Erstellen einer Spot-Flotte.

So erstellen Sie eine Spot-Flotten-Anfrage mithilfe einer Startvorlage

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Spot Instances anfordern aus.
4. Wählen Sie unter Launch parameters (Startparameter) die Option Use a launch template (Eine Startvorlage verwenden) aus.
5. Wählen Sie unter Launch template (Startvorlage) eine Startvorlage und dann im Feld auf der rechten Seite die Version der Startvorlage aus.
6. Konfigurieren Sie Ihre Spot-Flotte, indem Sie verschiedene Optionen auf diesem Bildschirm auswählen. Weitere Informationen zu diesen Optionen finden Sie unter Eine Spot-Flottenanforderung mit definierten Parametern erstellen.
7. Wenn Sie bereit sind, Ihre Spot-Flotte zu erstellen, klicken Sie auf Launch (Starten).

So erstellen Sie eine Spot-Flotten-Anfrage mithilfe einer Startvorlage

- Verwenden Sie den Befehl request-spot-fleet. Geben Sie mit dem Parameter `LaunchTemplateConfigs` die Startvorlage und alle Überschreibungen für die Startvorlage an.

Starten Sie eine EC2 Instance mit Details aus einer vorhandenen Instance

Die EC2 Amazon-Konsole bietet eine Launch Amore like this Option, mit der Sie eine aktuelle Instance als Basis für den Start anderer Instances verwenden können. Diese Option füllt den Amazon EC2 Launch Instance Wizard automatisch mit bestimmten Konfigurationsdetails der ausgewählten Instance.

Überlegungen

- Wir klonen Ihre Instances nicht, sondern replizieren nur einige der Konfigurationsdetails. Um eine Kopie Ihrer Instance zu erstellen, erstellen Sie zuerst ein AMI davon und starten Sie dann weitere Instance über das AMI. Erstellen Sie eine Startvorlage, um sicherzustellen, dass Sie Ihre Instances mit denselben Startdetails starten.
- Die aktuelle Instance muss sich im Status `running` befinden.

Details kopiert

Die folgenden Konfigurationsdetails werden von der ausgewählten Instance in den Launch Instance Wizard kopiert:

- AMI-ID
- Instance-Typ
- Availability Zone oder die VPC und das Subnetz, in der bzw. dem sich die ausgewählte Instance befindet
- Öffentliche IPv4 Adresse. Wenn die ausgewählte Instance derzeit über eine öffentliche IPv4 Adresse verfügt, erhält die neue Instance unabhängig von der Standardeinstellung für die öffentliche IPv4 Adresse der ausgewählten Instance eine öffentliche IPv4 Adresse. Weitere Informationen zu öffentlichen IPv4 Adressen finden Sie unterÖffentliche IPv4-Adressen.
- Platzierungsgruppe, falls zutreffend
- Die der Instance zugeordnete IAM-Rolle, falls zutreffend
- Einstellung des Beendigungsverhaltens (Anhalten oder Beenden)

- Einstellung des Beendigungsschutzes ("true" oder "false")
- CloudWatch Überwachung (aktiviert oder deaktiviert)
- Amazon EBS-Optimierungseinstellung ("true" oder "false")
- Tenancy-Einstellung beim Start in einer VPC (geteilt oder dediziert)
- Kernel-ID und RAM-Datenträger-ID, falls zutreffend
- Benutzerdaten, falls angegeben
- Der Instance zugeordnete Tags (Markierungen), falls zutreffend
- Der Instance zugeordnete Sicherheitsgruppen
- [Windows-Instances] Zuordnungsinformationen. Wenn die ausgewählte Instance einer Konfigurationsdatei zugeordnet ist, wird dieselbe Datei automatisch der neuen Instance zugeordnet. Wenn die Konfigurationsdatei eine verbundene Domain-Konfiguration enthält, wird die neue Instance automatisch mit derselben Domain verknüpft. Weitere Informationen zum Beitritt zu einer Domäne finden Sie unter Nahtloses Hinzufügen einer EC2 Windows-Instanz zu Ihrem AWS verwalteten Microsoft AD Active Directory im AWS Directory Service Administratorhandbuch.

Details wurden nicht kopiert

Die folgenden Konfigurationsdetails werden nicht von der ausgewählten Instance kopiert. Stattdessen wendet der Assistent deren Standardeinstellungen oder Verhalten an:

- Anzahl der Netzwerkschnittstellen – Der Standard ist eine Netzwerkschnittstelle, und zwar die primäre Netzwerkschnittstelle (eth0).
- Speicher – Die Standardspeicherkonfiguration wird vom AMI und dem Instance-Typ bestimmt.

So starten Sie weitere Instances wie eine bestehende Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie eine Instance aus und dann Aktionen, Images und Vorlagen, Mehr von dieser Art starten.
4. Der Launch Instance Wizard wird geöffnet. Sie können alle notwendigen Änderungen an der Instance-Konfiguration vornehmen, indem Sie verschiedene Optionen auf diesem Bildschirm auswählen.

Wenn Sie bereit sind, Ihre Instance zu starten, wählen Sie Launch instance (Instance starten) aus.

5. Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Fehlerbehebung bei Amazon-EC2-Instances.

Starten einer Amazon-EC2-Instance von einem AWS Marketplace-AMI

Sie können ein AWS Marketplace-AMI abonnieren und mit der Amazon-EC2-Konsole oder einem Befehlszeilentool eine Instance davon starten. Weitere Informationen zu AWS Marketplace-AMIs finden Sie unter Gebührenpflichtige AMIs im AWS Marketplace für Amazon-EC2-Instances.

Um Ihr Abonnement für das AMI nach dem Start zu kündigen, müssen Sie zunächst alle Instances beenden, die über das AMI gestartet wurden. Weitere Informationen finden Sie unter Verwalten Ihrer AWS Marketplace-Abonnements.

Eine Instance von einem AWS Marketplace-AMI mit der Amazon-EC2-Konsole starten

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Dashboard der Amazon EC2-Konsole die Option Instance starten aus.
3. (Optional) Geben Sie unter Name und Tags für Name einen beschreibenden Namen für Ihre Instance ein.
4. Wählen Sie unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image) die Option Weitere AMIs durchsuchen und wählen Sie dann die Registerkarte AWS Marketplace-AMIs aus. Finden Sie eine passende AMI, indem Sie die Kategorien durchsuchen oder die Suchfunktion verwenden. Um ein Produkt auszuwählen, wählen Sie Select (Auswählen).
5. Es öffnet sich ein Fenster mit einer Übersicht des ausgewählten Produkts. Sie können die Preisinformationen und andere vom Anbieter bereitgestellte Informationen anzeigen. Sobald Sie bereit sind, klicken Sie auf eine der folgenden Schaltflächen:

   - Beim Start der Instance abonnieren – Ihr Abonnement beginnt, wenn Sie Instance starten wählen (in Schritt 10).
   - Jetzt abonnieren – Ihr Abonnement beginnt sofort. Während das Abonnement läuft, können Sie die Instance konfigurieren, indem Sie mit den Schritten in diesem Verfahren fortfahren. Sollten Probleme mit den Kreditkarteninformationen bestehen, werden Sie zum Aktualisieren dieser aufgefordert.

> **Note**
>
> Die Nutzung des Produkts wird Ihnen erst in Rechnung gestellt, wenn Sie eine Instance mit dem AMI gestartet haben. Beachten Sie die Preise für jeden unterstützten Instance-Typ, wenn Sie einen Instance-Typ auswählen. Für das Produkt können auch zusätzliche Steuern anfallen.

6. Wählen Sie unter Instance type (Instance-Typ) einen Instance Typ für Ihre Instance aus. Der Instance-Typ definiert die Hardware-Konfiguration und die Größe der zu startenden Instance.
7. Wählen Sie unter Schlüsselpaar (Anmeldung) für Schlüsselpaarname ein vorhandenes Schlüsselpaar aus oder erstellen Sie ein neues.
8. Notieren Sie sich unter Netzwerkeinstellungen, Firewall (Sicherheitsgruppen) die neue Sicherheitsgruppe, die gemäß den Spezifikationen des Herstellers für das Produkt erstellt wurde. Die Sicherheitsgruppe kann Regeln enthalten, die allen IPv4-Adressen (`0.0.0.0/0`) den Zugriff auf SSH (Port 22) unter Linux oder RDP (Port 3389) unter Windows erlauben. Wir empfehlen, die Regeln anzupassen, sodass nur eine bestimmte Adresse bzw. ein bestimmter Adressbereich über diese Ports auf Ihre Instance zugreifen kann.
9. Sie können die anderen Felder auf dem Bildschirm verwenden, um Ihre Instance zu konfigurieren, Speicher und Tags hinzuzufügen. Weitere Informationen zu den verschiedenen Optionen, die Sie konfigurieren können, finden Sie unter Referenz für EC2 Amazon-Instance-Konfigurationsparameter.
10. Überprüfen Sie im Bereich Summary (Zusammenfassung) unter Software Image (AMI) (Software-Image (AMI)) die Details des AMI, von dem Sie die Instance starten wollen. Überprüfen Sie auch die anderen Konfigurationsdetails, die Sie angegeben haben. Wenn Sie bereit sind, Ihre Instance zu starten, wählen Sie Instance starten aus.
11. Je nach abonniertem Produkt kann der Start der Instance ein paar Minuten oder länger dauern. Wählen Sie in Schritt 5 die Option Beim Instance-Start abonnieren aus. Sie werden zuerst für das Produkt abonniert, bevor Ihre Instance starten kann. Sollten Probleme mit den Kreditkarteninformationen bestehen, werden Sie zum Aktualisieren dieser aufgefordert. Wenn die Bestätigungsseite für den Start angezeigt wird, wählen Sie View all instances (Alle Instances anzeigen), um zur Seite Instances zu gelangen.

> **Note**
>
> Der Abonnementpreis wird Ihnen in Rechnung gestellt, solange sich Ihre Instance im `running`-Status befindet, auch wenn diese inaktiv ist. Wenn Ihre Instance angehalten wird, wird Ihnen möglicherweise weiterhin Speicherplatz in Rechnung gestellt.

12. Wenn sich die Instance im Zustand `running` befindet, können Sie eine Verbindung zu ihr herstellen. Wählen Sie dazu Ihre Instance in der Liste aus, wählen Sie Connect (Verbinden) und wählen Sie eine Verbindungsoption aus. Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Connect zu Ihrer EC2 Instance her.

> **Important**
>
> Überprüfen Sie die Nutzungsanweisungen des Anbieters sorgfältig, da Sie möglicherweise einen bestimmten Benutzernamen verwenden müssen, um eine Verbindung zu Ihrer Instance herzustellen. Weitere Informationen zum Zugriff auf Ihre Abonnementdetails finden Sie unter Verwalten Ihrer AWS Marketplace-Abonnements.

13. Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Fehlerbehebung bei Amazon-EC2-Instances.

So starten Sie eine Instance auf einem AWS Marketplace-AMI unter Verwendung des Befehlszeilen-Tools

Um Instances von AWS Marketplace-Produkten aus mittels API oder Befehlszeilen-Tools zu starten, abonnieren Sie das Produkt. Anschließend starten Sie eine Instance mit der AMI-ID des Produkts. Gehen Sie hierzu folgendermaßen vor:

Art	Dokumentation
AWS CLI	Verwenden Sie den Befehl run-instances oder schlagen Sie das folgende Thema nach, um weitere Informationen zu erhalten: Ihre Instance starten im Benutzerhandbuch für AWS Command Line Interface.
AWS Tools for Windows PowerShell	Verwenden Sie den New-EC2Instance-Befehl oder schlagen Sie unter folgendem Thema nach, um weitere Informationen zu

Art	Dokumentation
	erhalten: Starten einer Amazon EC2-Instance mittels Windows PowerShell.
Abfrage-API	Verwenden Sie die RunInstances-Anforderung.

Connect zu Ihrer EC2 Instance her

Ihre EC2 Amazon-Instance ist ein virtueller Server in der AWS Cloud. Zum Anmelden an Ihrer Instance müssen Sie eine Verbindung zu der Instance herstellen. Wie Sie eine Verbindung zu Ihrer Instance herstellen, hängt vom Betriebssystem der Instance und dem Betriebssystem auf dem Computer ab, mit dem Sie sich mit der Instance verbinden. Die folgende Tabelle enthält die Anforderungen für die einzelnen Verbindungsmethoden.

Verbindungsoption	Instance-Betriebssystem	Regel für eingehenden Verkehr	IAM-Berechtigungen	Instance-Profilrolle	Software in Instance	Software im Verbindungssystem	Schlüsselpaar
SSH-Client	Linux	Ja	Nein	Nein	Nein	Ja	Ja
EC2 Instanzverbindung	Linux	Ja	Ja	Nein	Ja[1]	Nein	Nein
PuTTY	Linux	Ja	Nein	Nein	Nein	Ja	Ja
RDP-Client	Windows	Ja	Nein	Nein	Nein	Ja	Ja[2]
Fleet Manager	Windows	Nein	Ja	Ja	Ja[1]	Nein	Ja
Session Manager	Linux, Windows	Nein	Ja	Ja	Ja[1]	Nein	Nein

Verbindungsoption	Instance-Betriebssystem	Regel für eingehenden Verkehr	IAM-Berechtigungen	Instance-Profilrolle	Software in Instance	Software im Verbindungssystem	Schlüsselpaar
EC2 Instance Connect-Endpunkt	Linux, Windows	Ja	Ja	Nein	Nein	Nein	Nein [3]

[1] Die erforderliche Software ist nur auf bestimmten AMIs Geräten vorinstalliert. Sie können die erforderliche Software bei Bedarf auf unterstützten Betriebssystemen manuell installieren.

[2] Das Schlüsselpaar ist nur erforderlich, wenn Sie das zufällig generierte Passwort für das lokale Administrator-Benutzerkonto verwenden.

[3] Ein Schlüsselpaar ist erforderlich, wenn Sie die SSH-Verbindungsmethode verwenden.

Weitere Informationen finden Sie in der Dokumentation zu der Verbindungsoption, die Sie verwenden möchten.

Verbindungsoptionen

- Verbinden mit der Linux-Instance über einen SSH-Client
- Verbindung mit Ihrer Linux-Instance mithilfe von PuTTY
- Verbindung zu Ihrer Windows-Instance mithilfe eines RDP-Clients herstellen
- Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von Fleet Manager
- Herstellen einer Verbindung über Session Manager
- Stellen Sie eine Verbindung über eine öffentliche IP und EC2 Instance Connect her
- Stellen Sie eine Connect über eine private IP und einen EC2 Instance Connect-Endpunkt her

Allgemeine Voraussetzungen für eine Verbindung

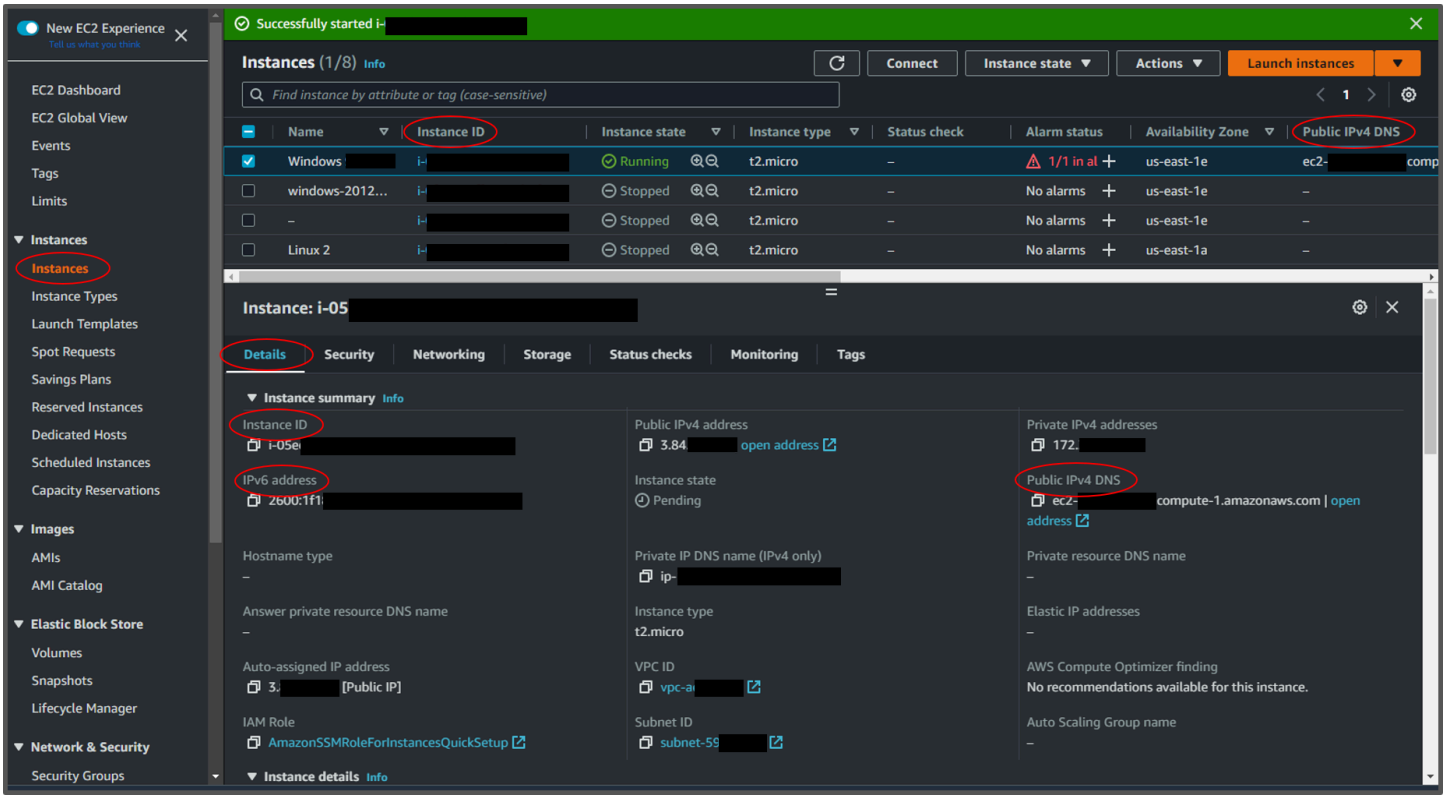
Im Folgenden sind die allgemeinen Voraussetzungen aufgeführt, um eine Verbindung zu einer Instance herzustellen. Beachten Sie, dass möglicherweise zusätzliche Voraussetzungen gelten, die für die von Ihnen gewählte Verbindungsoption spezifisch sind.

Allgemeine Voraussetzungen

- Stellen Sie sicher, dass Ihre Instance ihre Statusprüfungen bestanden hat. Es kann ein paar Minuten dauern, bis die Instance für die Verbindung bereitsteht. Weitere Informationen finden Sie unter Anzeigen der Statusprüfungen.
- Rufen Sie die erforderlichen Instance-Details ab.
- Lokalisieren des privaten Schlüssels und Festlegen von Berechtigungen.
- (Optional) Anfordern des Instance-Fingerabdrucks.

Rufen Sie die erforderlichen Instance-Details ab

Um die Verbindung mit Ihrer Instance vorzubereiten, rufen Sie die folgenden Informationen von der EC2 Amazon-Konsole oder über die Befehlszeile ab.



- Rufen Sie den öffentlichen DNS-Namen der Instance ab.

  Sie können das öffentliche DNS für Ihre Instance von der EC2 Amazon-Konsole abrufen. Sehen Sie in der Spalte Öffentliche IPv4 DNS im Bereich Instances nach. Wenn diese Spalte ausgeblendet ist, wählen Sie das Einstellungssymbol (⚙)

in der oberen rechten Ecke des Bildschirms und wählen Sie Public IPv4 DNS aus. Sie finden das öffentliche DNS auch im Bereich „Instance-Informationen“ des Instances-Bereichs. Wenn Sie die Instance im Bereich Instances der EC2 Amazon-Konsole auswählen, werden Informationen zu dieser Instance in der unteren Hälfte der Seite angezeigt. Suchen Sie auf der Registerkarte Details nach Public IPv4 DNS.

Wenn Sie möchten, können Sie die Befehle describe-instances (AWS CLI) oder Get-EC2Instance(AWS Tools for Windows PowerShell) verwenden.

Wenn kein Public IPv4 DNS angezeigt wird, vergewissern Sie sich, dass der Instanzstatus Running lautet und dass Sie die Instance nicht in einem privaten Subnetz gestartet haben. Wenn Sie Ihre Instance mit dem Launch Instance Wizard gestartet haben, haben Sie möglicherweise das Feld Öffentliche IP automatisch zuweisen unter Netzwerkeinstellungen bearbeitet und den Wert in Deaktivieren geändert. Wenn Sie die Option Öffentliche IP automatisch zuweisen deaktivieren, wird der Instance beim Start keine öffentliche IP-Adresse zugewiesen.

- (IPv6 nur Instanzen) Ruft die IPv6 Adresse der Instanz ab.

  Wenn Sie Ihrer Instance eine IPv6 Adresse zugewiesen haben, können Sie optional eine Verbindung zur Instance herstellen, indem Sie deren IPv6 Adresse anstelle einer öffentlichen IPv4 Adresse oder eines öffentlichen IPv4 DNS-Hostnamens verwenden. Ihr lokaler Computer muss über eine IPv6 Adresse verfügen und für die Verwendung IPv6 konfiguriert sein. Sie können die IPv6 Adresse Ihrer Instance von der EC2 Amazon-Konsole abrufen. Überprüfen Sie die IPv6 IPsSpalte im Bereich „Instances“. Sie können die IPv6 Adresse auch im Abschnitt mit den Instanzinformationen finden. Wenn Sie die Instance im Bereich Instances der EC2 Amazon-Konsole auswählen, werden Informationen zu dieser Instance in der unteren Hälfte der Seite angezeigt. Suchen Sie auf der Registerkarte Details nach der IPv6Adresse.

  Wenn Sie möchten, können Sie die Befehle describe-instances (AWS CLI) oder Get-EC2Instance(AWS Tools for Windows PowerShell) verwenden. Weitere Informationen zu finden Sie IPv6 unter. IPv6-Adressen

- (Linux-Instances) Rufen Sie den Benutzernamen für Ihre Instance ab.

  Sie können mit dem Benutzernamen für Ihr Benutzerkonto oder dem Standardbenutzernamen für das AMI, das Sie zum Starten Ihrer Instance verwendet haben, eine Verbindung zu Ihrer Instance herstellen.

  - Abrufen des Benutzernamens für Ihr Benutzerkonto ab.

Weitere Informationen zum Erstellen eines Benutzerkontos finden Sie unter Verwalten von Benutzern auf einer Amazon-EC2-Linux-Instance.

- Abrufen des Standardbenutzernamens für das AMI, das Sie zum Starten der Instance verwendet haben.
  - Amazon Linux – `ec2-user`
  - CentOS – `centos` oder `ec2-user`
  - Debian – `admin`
  - Fedora – `fedora` oder `ec2-user`
  - FreeBSD — `ec2-user`
  - RHEL – `ec2-user` oder `root`
  - SUSE – `ec2-user` oder `root`
  - Ubuntu – `ubuntu`
  - Oracle – `ec2-user`
  - Bitnami – `bitnami`
  - Rocky Linux – `rocky`
  - Andere – Wenden Sie sich an den AMI-Anbieter

Lokalisieren des privaten Schlüssels und Festlegen von Berechtigungen

Sie müssen den Speicherort Ihrer privaten Schlüsseldatei kennen, um die erste Verbindung zu einer Linux-Instance über SSH oder zu einer Windows-Instance über RDP herzustellen. Für SSH-Verbindungen müssen Sie die Berechtigungen so festlegen, dass nur Sie die Datei lesen können.

Informationen zur Funktionsweise von Schlüsselpaaren bei der Nutzung von Amazon EC2 finden Sie unter EC2 Amazon-Schlüsselpaare und EC2 Amazon-Instances.

- Lokalisieren Sie den privaten Schlüssel.

  Rufen Sie den vollständig qualifizierten Pfad des Speicherorts auf Ihrem Computer für die Datei `.pem` für das beim Start der Instance angegebene Schlüsselpaar ab. Weitere Informationen finden Sie unter the section called “Identifizieren des öffentlichen Schlüssels, der beim Start angegeben wurde”.

  Wenn Sie Ihre private Schlüsseldatei nicht finden können, lesen Sie unter Ich habe meinen privaten Schlüssel verloren. Wie kann ich eine Verbindung zu meiner Instance herstellen?

(Linux-Instances) Wenn Sie mit Putty eine Verbindung zu Ihrer Instance herstellen und die `.pem`-Datei in `.ppk` konvertieren müssen, lesen Sie unter Konvertieren Ihres privaten Schlüssels mit PuTTYgen.

- (Linux-Instances) Festlegen der Berechtigungen für Ihren privaten Schlüssel, so dass nur Sie diesen lesen können.
  - Herstellen einer Verbindung über macOS oder Linux

    Wenn Sie einen SSH-Kunden auf einem macOS- oder Linux-Computer verwenden möchten, um eine Verbindung zu Ihrer Linux Instance herzustellen, legen Sie mit dem folgenden Befehl die Berechtigungen für Ihre private Schlüsseldatei so fest, dass nur Sie sie lesen können.

    ```
    chmod 400 key-pair-name.pem
    ```

    Wenn Sie diese Berechtigungen nicht festlegen, können Sie unter Verwendung dieses Schlüsselpaars keine Verbindung zu Ihrer Instance herstellen. Weitere Informationen finden Sie unter Fehler: Ungeschützte private Schlüsseldatei.
  - Herstellen einer Verbindung über Windows

    Öffnen Sie den Datei-Explorer und klicken Sie mit der rechten Maustaste auf die `.pem`-Datei. Wählen Sie Eigenschaften > Registerkarte Sicherheit und dann Erweitert aus. Wählen Sie Vererbung deaktivieren. Entfernen Sie den Zugriff für alle Benutzer mit Ausnahme des aktuellen Benutzers.

(Optional) Anfordern des Instance-Fingerabdrucks

Um sich vor man-in-the-middle Angriffen zu schützen, können Sie die Echtheit der Instance, zu der Sie eine Verbindung herstellen möchten, überprüfen, indem Sie den angezeigten Fingerabdruck verifizieren. Die Überprüfung des Fingerabdrucks ist nützlich, wenn Sie Ihre Instance über ein öffentliches AMI starten, das von einem Drittanbieter bereitgestellt wird.

Übersicht über die Aufgaben

Holen Sie sich zunächst den Instance-Fingerabdruck von der Instance. Wenn Sie anschließend eine Verbindung mit der Instance herstellen und zum Überprüfung des Fingerabdrucks aufgefordert werden, vergleichen Sie den Fingerabdruck, den Sie in diesem Verfahren abgerufen haben, mit dem Fingerabdruck, der angezeigt wird. Wenn die Fingerabdrücke nicht übereinstimmen, versucht

möglicherweise jemand einen man-in-the-middle Angriff. Wenn sie übereinstimmen, können Sie bedenkenlos eine Verbindung mit der Instance herstellen.

Voraussetzungen für das Abrufen des Instance-Fingerabdrucks

- Die Instance darf sich nicht im Status `pending` befinden. Der Fingerabdruck ist erst verfügbar, nachdem der erste Start der Instance abgeschlossen ist.
- Sie müssen der Instance-Eigentümer sein, um die Konsolenausgabe zu erhalten.
- Es gibt verschiedene Methoden, um den Instance-Fingerabdruck zu bekommen. Wenn Sie den AWS CLI verwenden möchten, muss er auf Ihrem lokalen Computer installiert sein. Informationen zur Installation von finden Sie unter Erste Schritte mit dem AWS CLI im AWS Command Line Interface Benutzerhandbuch. AWS CLI

So fordern Sie den Instance-Fingerabdruck an

In Schritt 1 erhalten Sie die Konsolenausgabe, die den Instance-Fingerabdruck enthält. In Schritt 2 finden Sie den Fingerabdruck der Instance in der Konsolenausgabe.

1. Verwenden Sie eine der folgenden Methoden, um die Konsolenausgabe zu erhalten.

   Console

   1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
   2. Wählen Sie im linken Navigationsbereich Instances aus.
   3. Wählen Sie die Instance aus und wählen Sie dann Aktionen, Überwachung und Fehlerbehebung, Systemprotokoll abrufen.

   AWS CLI

   Verwenden Sie auf Ihrem lokalen Computer (nicht auf der Instance, zu der Sie eine Verbindung herstellen) den get-console-outputBefehl. Wenn die Ausgabe umfangreich ist, können Sie sie an eine Textdatei weiterleiten, wo sie möglicherweise einfacher zu lesen ist.

   ```
   aws ec2 get-console-output \
       --instance-id i-1234567890abcdef0 \
       --query Output \
       --output text > temp.txt
   ```

PowerShell

Verwenden Sie auf Ihrem lokalen Computer das folgende Get-EC2ConsoleOutputCmdlet.

```
$encodedOutput = (Get-EC2ConsoleOutput -InstanceId i-1234567890abcdef0).Output
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($encodedOutput
```

2. Suchen Sie in der Konsolenausgabe den Instance-Fingerabdruck (Host-Fingerabdruck), der sich unter `BEGIN SSH HOST KEY FINGERPRINTS` befindet. Möglicherweise gibt es mehrere Instance-Fingerabdrücke. Wenn Sie eine Verbindung mit Ihrer Instance herstellen, wird nur einer der Fingerabdrücke angezeigt.

   Die genaue Ausgabe kann je nach Betriebssystem, AMI-Version und davon, ob AWS die Schlüsselpaare erstellt hat, variieren. Es folgt eine Beispielausgabe.

```
ec2:#############################################################
ec2: -----BEGIN SSH HOST KEY FINGERPRINTS-----
ec2: 256 SHA256:l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY no comment (ECDSA)
ec2: 256 SHA256:kpEa+rw/Uq3zxaYZN8KT501iBtJOIdHG52dFi66EEfQ no comment (ED25519)
ec2: 2048 SHA256:L8l6pepcA7iqW/jBecQjVZClUrKY+o2cHLI0iHerbVc no comment (RSA)
ec2: -----END SSH HOST KEY FINGERPRINTS-----
ec2: #############################################################
```

   > **Note**
   >
   > Sie verweisen auf diesen Fingerabdruck, wenn Sie eine Verbindung mit der Instance herstellen.

Herstellen einer Verbindung zu Ihrer Linux-Instance mit SSH

Es gibt verschiedene Möglichkeiten, eine Verbindung zu Ihrer Linux-Instance mit SSH herzustellen. Einige Wege hängen vom Betriebssystem des lokalen Rechners ab, von dem aus Sie die Verbindung herstellen. Andere Methoden sind browserbasiert, wie EC2 Instance Connect oder AWS Systems Manager Session Manager, und können von jedem Computer aus verwendet werden. Sie können SSH verwenden, um sich mit Ihrer Linux-Instance zu verbinden und Befehle auszuführen, oder SSH verwenden, um Dateien zwischen Ihrem lokalen Computer und Ihrer Instance zu übertragen.

Erfüllen Sie die folgenden Voraussetzungen, bevor Sie eine Verbindung mit Ihrer Linux-Instance mit SSH herstellen:

- Stellen Sie sicher, dass Ihre Instance ihre Statusprüfungen bestanden hat. Es kann ein paar Minuten dauern, bis die Instance für die Verbindung bereitsteht. Weitere Informationen finden Sie unter Anzeigen der Statusprüfungen.
- Stellen Sie sicher, dass die mit Ihrer Instance verknüpfte Sicherheitsgruppe eingehenden SSH-Datenverkehr von Ihrer IP-Adresse zulässt. Weitere Informationen finden Sie unter Regeln für die Verbindung mit Instances von Ihrem Computer aus.
- Rufen Sie die erforderlichen Instance-Details ab.
- Lokalisieren des privaten Schlüssels und Festlegen von Berechtigungen.
- (Optional) Anfordern des Instance-Fingerabdrucks.

Wählen Sie dann eine der folgenden Optionen, um eine Verbindung zu Ihrer Linux-Instance mit SSH herzustellen.

- Verbindung mit einem SSH-Client herstellen
- Verbindung über PuTTY
- Übertragen von Dateien mit SCP

Wenn Sie keine Verbindung mit Ihrer Instance herstellen können und Sie Hilfe zur Fehlerbehebung benötigen, siehe Fehlersuche bei Verbindungsproblemen mit Ihrer Amazon-EC2-Linux-Instance.

Verbinden mit der Linux-Instance über einen SSH-Client

Sie können Secure Shell (SSH) verwenden, um von Ihrem lokalen Computer aus eine Verbindung zu Ihrer Linux-Instance herzustellen. Weitere Informationen über andere Optionen finden Sie unter Connect zu Ihrer EC2 Instance her.

> **Note**
>
> Wenn Sie beim Versuch, eine Verbindung zu Ihrer Instance herzustellen, eine Fehlermeldung erhalten, stellen Sie sicher, dass Ihre Instance alle Voraussetzungen für eine SSH-Verbindung erfüllt. Wenn alle Voraussetzungen erfüllt sind und Sie immer noch keine Verbindung zu Ihrer Linux-Instance herstellen können, lesen Sie Fehlersuche bei Verbindungsproblemen mit Ihrer Amazon-EC2-Linux-Instance.

Inhalt

- Voraussetzungen für eine SSH-Verbindung
- Verbinden mit der Linux-Instance über einen SSH-Client

Voraussetzungen für eine SSH-Verbindung

Bevor Sie sich über SSH mit Ihrer Linux-Instance verbinden können, müssen Sie die folgenden Aufgaben erledigen.

Vervollständigen Sie die allgemeinen Voraussetzungen.

- Stellen Sie sicher, dass Ihre Instance ihre Statusprüfungen bestanden hat. Es kann ein paar Minuten dauern, bis die Instance für die Verbindung bereitsteht. Weitere Informationen finden Sie unter Anzeigen der Statusprüfungen.
- Rufen Sie die erforderlichen Instance-Details ab.
- Lokalisieren des privaten Schlüssels und Festlegen von Berechtigungen.
- (Optional) Anfordern des Instance-Fingerabdrucks.

Lassen Sie eingehenden SSH-Datenverkehr von Ihrer IP-Adresse zu.

Stellen Sie sicher, dass die mit Ihrer Instance verknüpfte Sicherheitsgruppe eingehenden SSH-Datenverkehr von Ihrer IP-Adresse zulässt. Weitere Informationen finden Sie unter Regeln für die Verbindung mit Instances von Ihrem Computer aus.

Installieren Sie einen SSH-Client auf dem lokalen Computer (falls notwendig).

Auf Ihrem lokalen Computer ist möglicherweise standardmäßig ein SSH-Client installiert. Sie können dies überprüfen, indem Sie den folgenden Befehl in ein Terminal-Fenster eingeben. Wenn Ihr Computer den Befehl nicht erkennt, müssen Sie einen SSH-Client installieren.

```
ssh
```

Im Folgenden sind einige der möglichen Optionen für Windows aufgeführt. Wenn auf Ihrem Computer ein anderes Betriebssystem ausgeführt wird, finden Sie in der Dokumentation zu diesem Betriebssystem Informationen zu den SSH-Clientoptionen.

OpenSSH unter Windows installieren

Nachdem Sie OpenSSH unter Windows installiert haben, können Sie von Ihrem Windows-Computer aus eine Verbindung zu Ihrer Linux-Instance über SSH herstellen. Stellen Sie vor Beginn sicher, dass die folgenden Anforderungen erfüllt sind.

Windows-Version

Die Version von Windows auf Ihrem Computer muss Windows Server 2019 oder höher sein.

Für frühere Versionen von Windows laden Sie Win32-OpenSSH herunter und installieren Sie es.

Voraussetzungen für PowerShell

Um OpenSSH mit PowerShell auf Ihrem Windows-Betriebssystem zu installieren, müssen Sie PowerShell Version 5.1 oder höher ausführen und Ihr Konto muss Mitglied der integrierten Administratorgruppe sein. Führen Sie `$PSVersionTable.PSVersion` von PowerShell aus, um Ihre PowerShell-Version zu überprüfen.

Führen Sie den folgenden PowerShell-Befehl aus, um zu überprüfen, ob Sie Mitglied der integrierten Administratorgruppe sind:

```
(New-Object
 Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())).Is
```

Wenn Sie Mitglied der integrierten Administratorgruppe sind, lautet die Ausgabe `True`.

Um OpenSSH für Windows mit PowerShell zu installieren, führen Sie den folgenden PowerShell-Befehl aus.

```
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Es folgt eine Beispielausgabe.

```
Path          :
Online        : True
RestartNeeded : False
```

Um OpenSSH von Windows mit PowerShell zu deinstallieren, führen Sie den folgenden PowerShell-Befehl aus.

```
Remove-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Es folgt eine Beispielausgabe.

```
Path          :
Online        : True
RestartNeeded : True
```

Windows-Subsystem für Linux (WSL) installieren

Nach der Installation der WSL unter Windows können Sie von Ihrem Windows-Computer aus eine Verbindung zu Ihrer Linux-Instance herstellen, indem Sie Linux-Befehlszeilen-Tools, wie z. B. einen SSH-Client, verwenden.

Folgen Sie den Anweisungen in Das Windows-Subsystem für Linux auf Ihrer EC2-Windows-Instance installieren. Wenn Sie den Anweisungen in der Installationsanleitung von Microsoft folgen, wird dort die Ubuntu-Distribution von Linux installiert. Sie können eine andere Linux-Distribution installieren, wenn Sie dies wünschen.

Kopieren Sie in einem WSL-Terminal-Fenster die Datei `.pem` (für das Schlüsselpaar, das Sie beim Start der Instance angegeben haben) von Windows zu WSL. Beachten Sie den vollqualifizierten Pfad zur Datei `.pem` in WSL, der zum Herstellen der Verbindung mit Ihrer Instance verwendet wird. Informationen dazu, wie Sie den Pfad zu Ihrem Windows-Laufwerk angeben, finden Sie unter How do I access my C drive?.

```
cp /mnt/<Windows drive letter>/path/my-key-pair.pem ~/WSL-path/my-key-pair.pem
```

Informationen zum Deinstallieren des Windows-Subsystems für Linux finden Sie unter How do I uninstall a WSL Distribution?.

Verbinden mit der Linux-Instance über einen SSH-Client

Verwenden Sie die folgende Vorgehensweise, um per SSH-Client eine Verbindung mit Ihrer Linux-Instance herzustellen.

So stellen Sie mithilfe eines SSH-Clients eine Verbindung zu Ihrer Instance her

1. Öffnen Sie ein Terminal-Fenster auf Ihrem Computer.
2. Stellen Sie mit dem Befehl ssh eine Verbindung zur Instance her. Sie benötigen die Details zu Ihrer Instance, die Sie im Rahmen der Voraussetzungen gesammelt haben. Sie benötigen

beispielsweise den Speicherort des privaten Schlüssels (`.pem`-Datei), den Benutzernamen und den öffentlichen DNS-Namen oder die IPv6-Adresse. Die Folgenden sind Beispielbefehle.

- (Öffentliches DNS) Geben Sie den folgenden Befehl ein, um den öffentlichen DNS-Namen zu verwenden.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-dns-name
```

- (IPv6) Wenn Ihre Instance eine IPv6-Adresse hat, geben Sie alternativ den folgenden Befehl ein, um die IPv6-Adresse zu verwenden.

```
ssh -i /path/key-pair-name.pem instance-user-name@2001:db8::1234:5678:1.2.3.4
```

Nachfolgend finden Sie eine Beispielantwort.

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'
 can't be established.
ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
Are you sure you want to continue connecting (yes/no)?
```

3. (Optional) Vergewissern Sie sich, dass der Fingerabdruck in der Sicherheitswarnung mit dem Fingerabdruck übereinstimmt. Wenn diese Fingerabdrücke nicht übereinstimmen, wird möglicherweise versucht, einen Man-In-the-Middle-Angriff durchzuführen. Falls die Fingerabdrücke übereinstimmen, können Sie mit dem nächsten Schritt fortfahren. Weitere Informationen finden Sie unter Den Instance-Fingerabdruck erhalten.
4. Geben Sie ei **`yes`**.

   Sie erhalten in etwa folgende Antwort:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to
 the list of known hosts.
```

Verbindung mit Ihrer Linux-Instance mithilfe von PuTTY

Sie können eine Verbindung zu Ihrer Linux-Instance mit PuTTY, einem kostenlosen SSH-Client für Windows, herstellen.

Wenn Sie Windows Server 2019 oder höher ausführen, empfehlen wir die Verwendung von OpenSSH, einem Open-Source-Verbindungstool für die Fernanmeldung mit dem SSH-Protokoll.

> **Note**
>
> Wenn Sie beim Versuch, eine Verbindung zu Ihrer Instance herzustellen, eine Fehlermeldung erhalten, stellen Sie sicher, dass Ihre Instance alle Voraussetzungen für eine SSH-Verbindung erfüllt. Wenn alle Voraussetzungen erfüllt sind und Sie immer noch keine Verbindung zu Ihrer Linux-Instance herstellen können, lesen Sie Fehlersuche bei Verbindungsproblemen mit Ihrer Amazon-EC2-Linux-Instance.

Inhalt

- Voraussetzungen
- (Optional) Konvertieren Ihres privaten Schlüssels mit PuTTYgen
- Herstellen einer Verbindung zur Linux-Instance

Voraussetzungen

Erledigen Sie die folgenden Aufgaben, bevor Sie mit PuTTY eine Verbindung mit Ihrer Linux-Instance herstellen.

Vervollständigen Sie die allgemeinen Voraussetzungen.

- Stellen Sie sicher, dass Ihre Instance ihre Statusprüfungen bestanden hat. Es kann ein paar Minuten dauern, bis die Instance für die Verbindung bereitsteht. Weitere Informationen finden Sie unter Anzeigen der Statusprüfungen.
- Rufen Sie die erforderlichen Instance-Details ab.
- Lokalisieren des privaten Schlüssels und Festlegen von Berechtigungen.
- (Optional) Anfordern des Instance-Fingerabdrucks.

Lassen Sie eingehenden SSH-Datenverkehr von Ihrer IP-Adresse zu.

Stellen Sie sicher, dass die mit Ihrer Instance verknüpfte Sicherheitsgruppe eingehenden SSH-Datenverkehr von Ihrer IP-Adresse zulässt. Weitere Informationen finden Sie unter Regeln für die Verbindung mit Instances von Ihrem Computer aus.

Installieren Sie PuTTY auf Ihrem lokalen Computer (falls erforderlich).

Laden Sie PuTTY über die Downloadseite für PuTTY herunter und führen Sie die Installation durch. Wenn Sie bereits eine frühere Version von PuTTY installiert haben, wird empfohlen, die neueste Version herunterzuladen. Vergewissern Sie sich, dass Sie die gesamte Suite installieren.

Konvertieren Sie den privaten Schlüssel mit PuTTYgen in das PPK-Format.

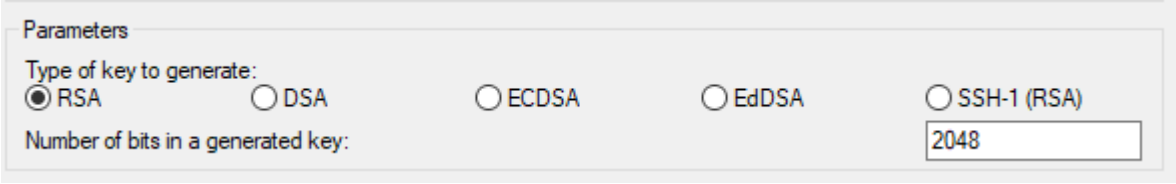
Sie müssen den privaten Schlüssel für das Schlüsselpaar angeben, das Sie beim Start der Instance angegeben haben. Wenn Sie den privaten Schlüssel im PEM-Format erstellt haben, müssen Sie ihn ins PPK-Format umwandeln, damit er mit PuTTY genutzt werden kann. Suchen Sie den privaten Schlüssel (PEM-Datei) und folgen Sie dann den Schritten in Konvertieren Ihres privaten Schlüssels mit PuTTYgen.

(Optional) Konvertieren Ihres privaten Schlüssels mit PuTTYgen

PuTTY unterstützt das PEM-Format für SSH-Schlüssel nicht nativ. PuTTY stellt ein Tool namens PuTTYgen bereit, das PEM-Schlüssel in das gewünschte Format „PPK“ für PuTTY konvertiert. Wenn Sie den Schlüssel im PEM-Format statt PPK-Format erstellt haben, müssen Sie Ihren privaten Schlüssel (PEM-Datei) ins Format (PPK-Datei) umwandeln, damit er mit PuTTY genutzt werden kann.

Einen privaten PEM-Schlüssel in das PPK-Format konvertieren

1. Wählen Sie im Menü Start All Programs (Alle Programme), PuTTY, PuTTYgen aus.
2. Wählen Sie unter Type of key to generate die Option RSA. Wenn Ihre Version von PuTTYgen diese Option nicht enthält, wählen Sie SSH-2 RSA.



3. Wählen Sie Load (Laden) aus. PuTTYgen zeigt standardmäßig nur Dateien mit der Erweiterung a `.ppk`. Damit Sie die `.pem`-Datei finden, wählen Sie die Option zur Anzeige aller Dateitypen aus.

4. Wählen Sie Ihre `.pem`-Datei für das Schlüsselpaar aus, das Sie beim Starten Ihrer Instance angegeben haben, und wählen Sie anschließend Open (Öffnen). PuTTYgen zeigt einen Hinweis an, dass die `.pem`-Datei erfolgreich importiert wurde. Klicken Sie auf OK.

5. Klicken Sie auf Save private key, um den Schlüssel in einem mit PuTTY kompatiblen Format zu speichern. PuTTYgen zeigt einen Warnhinweis zur Speicherung des Schlüssels ohne Passphrase an. Wählen Sie Yes (Ja).

   > **Note**
   >
   > Eine Passphrase stellt bei einem privaten Schlüssel eine zusätzliche Schutzebene dar. Auch wenn Ihr privater Schlüssel erkannt wird, kann er ohne die Passphrase nicht verwendet werden. Der Nachteil einer Passphrase ist, dass sie die Automatisierung erschwert, da für Anmeldungen bei einer Instance oder dem Kopieren von Dateien zu einer Instance menschliche Eingriffe erforderlich sind.

6. Geben Sie den gleichen Namen für den Schlüssel an, den Sie für das Schlüsselpaar verwendet haben (z. B. `key-pair-name`), und wählen Sie Save (Speichern) aus. PuTTY fügt automatisch die Dateierweiterung `.ppk` hinzu.

Ihr persönlicher Schlüssel ist nun im korrekten Format zur Verwendung mit PuTTY. Sie können sich nun über den SSH-Client von PuTTY mit Ihrer Instance verbinden.

Herstellen einer Verbindung zur Linux-Instance

Verwenden Sie die folgende Vorgehensweise, um per PuTTY eine Verbindung mit Ihrer Linux-Instance herzustellen. Sie benötigen die `.ppk`-Datei, die Sie für Ihren privaten Schlüssel erstellt haben. Für weitere Informationen vgl. (Optional) Konvertieren Ihres privaten Schlüssels mit PuTTYgen im vorherigen Abschnitt. Weitere Informationen zu Problemen, die beim Aufbau einer Verbindung zu Instances auftreten können, finden Sie unter Fehlersuche bei Verbindungsproblemen mit Ihrer Amazon-EC2-Linux-Instance.

Letzte getestete Version – PuTTY .78

So stellen Sie mithilfe von PuTTY eine Verbindung mit Ihrer Instance her

1. Starten Sie PuTTY (suchen Sie im Startmenü nach PuTTY und wählen Sie anschließend Öffnen aus).
2. Wählen Sie im Bereich Category die Option Session und füllen Sie die folgenden Felder aus:

   a. Führen Sie im Feld Host Name (Hostname) einen der folgenden Schritte aus:

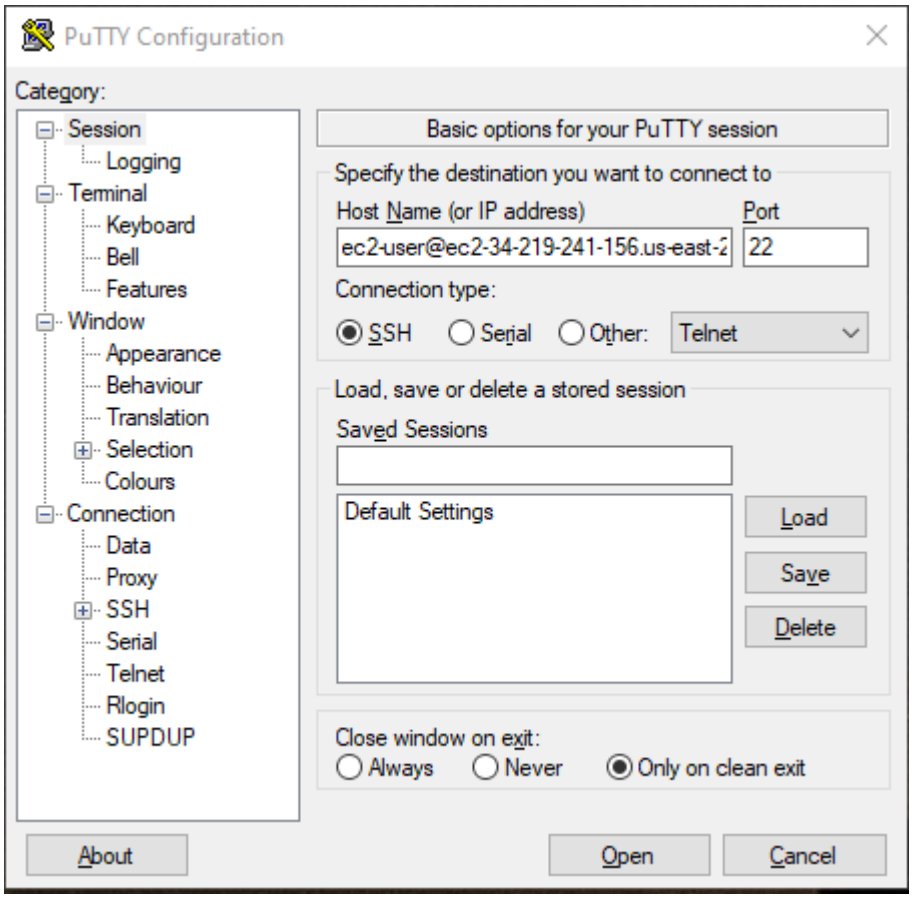
      - (Public DNS) Um eine Verbindung über den öffentlichen DNS-Namen Ihrer Instance herzustellen, geben Sie *instance-user-name*@*instance-public-dns-name* ein.

- (IPv6) Wenn Ihre Instance über eine IPv6-Adresse verfügt, können Sie alternativ mit der IPv6-Adresse Ihrer Instance eine Verbindung herstellen, indem Sie *instance-user-name*@*2001:db8::1234:5678:1.2.3.4* eingeben.

Informationen zum Abrufen des Benutzernamens für Ihre Instance sowie des öffentlichen DNS-Namens oder der IPv6-Adresse Ihrer Instance finden Sie unter Rufen Sie die erforderlichen Instance-Details ab.

b. Vergewissern Sie sich, dass der Port-Wert 22 ist.

c. Wählen Sie unter Connection type die Option SSH.



3. (Optional) Sie können konfigurieren, dass PuTTY in regelmäßigen Zeitabständen automatisch 'keepalive'-Daten sendet, um die Sitzung aktiv zu halten. Auf diese Weise können Sie vermeiden, dass die Verbindung mit Ihrer Instance aufgrund von Sitzungsinaktivität getrennt wird. Wählen Sie im Bereich Kategorie die Option Verbindung aus und geben Sie dann das erforderliche Intervall in Sekunden zwischen Keepalives ein. Wenn Ihre Sitzung z. B. nach 10 Minuten Inaktivität getrennt wird, geben Sie „180“ ein, damit PuTTY so konfiguriert wird, dass alle 3 Minuten keepalive-Daten gesendet werden.

4. Erweitern Sie im Bereich Kategorie die Optionen Verbindung, SSH und Authentifizierung. Wählen Sie Anmeldeinformationen aus.
5. Wählen Sie neben Private Schlüsseldatei für Authentifizierung: die Option Durchsuchen aus. Wählen Sie im Dialogfeld Private Schlüsseldatei auswählen die `.ppk`-Datei aus, die Sie für Ihr Schlüsselpaar generiert haben. Sie können entweder auf die Datei doppelklicken oder Öffnen im Dialogfeld Private Schlüsseldatei auswählen wählen.
6. (Optional) Wenn Sie planen, nach dieser Sitzung erneut eine Verbindung zu dieser Instance herzustellen, können Sie die Sitzungsinformationen für die zukünftige Verwendung speichern. Wählen Sie im Bereich Kategorie die Option Sitzung aus. Geben Sie unter Gespeicherte Sitzungen einen Namen für die Sitzung ein und wählen Sie dann Speichern.
7. Um eine Verbindung mit der Instance herzustellen, wählen Sie Öffnen.
8. Wenn Sie zum ersten Mal eine Verbindung mit dieser Instance hergestellt haben, zeigt PuTTY ein Dialogfeld mit einer Sicherheitswarnung an. Darin werden Sie gefragt, ob Sie dem Host vertrauen, mit dem die Verbindung hergestellt werden soll.

    a. (Optional) Vergewissern Sie sich, dass der Fingerabdruck im Dialogfeld der Sicherheitswarnung mit dem Fingerabdruck übereinstimmt, den Sie zuvor unter abgerufen habe (Optional) Anfordern des Instance-Fingerabdrucks. Wenn diese Fingerabdrücke nicht übereinstimmen, wird ggf. versucht, einen Man-In-the-Middle-Angriff durchzuführen. Falls die Fingerabdrücke übereinstimmen, können Sie mit dem nächsten Schritt fortfahren.

    b. Wählen Sie Accept (Akzeptieren) aus. Ein neues Fenster wird geöffnet, und Sie sind mit Ihrer Instance verbunden.

    > **Note**
    >
    > Falls Sie eine Passphrase angegeben haben, als Sie den persönlichen Schlüssel in das PuTTY-Format konvertiert hatten, müssen Sie diese Passphrase eingeben, wenn Sie sich bei der Instance anmelden.

Weitere Informationen zu Problemen, die beim Aufbau einer Verbindung zu Instances auftreten können, finden Sie unter Fehlersuche bei Verbindungsproblemen mit Ihrer Amazon-EC2-Linux-Instance.

Dateien zu einer Linux-Instance mit SCP übertragen

Eine Möglichkeit, Dateien zwischen Ihrem lokalen Computer und einer Linux-Instance zu übertragen, ist die Verwendung von Secure Copy Protocol (SCP). SCP ist eine gute Option für einfache Vorgänge, wie z. B. einmalige Dateikopien. SCP sichert Dateiübertragungen mit derselben PEM-Datei, mit der Sie über SSH eine Verbindung zu einer Instance herstellen. Wenn Sie Dateien synchronisieren müssen oder wenn die Dateien groß sind, ist rsync schneller und effizienter als SCP. Verwenden Sie aus Sicherheitsgründen rsync über SSH, da rsync Daten standardmäßig im Klartext überträgt.

Erfüllen Sie die folgenden Voraussetzungen, bevor Sie eine Verbindung mit Ihrer Linux-Instance mit SCP herstellen:

- Die allgemeinen Voraussetzungen erfüllen.
  - Stellen Sie sicher, dass Ihre Instance ihre Statusprüfungen bestanden hat. Es kann ein paar Minuten dauern, bis die Instance für die Verbindung bereitsteht. Weitere Informationen finden Sie unter Anzeigen der Statusprüfungen.
  - Rufen Sie die erforderlichen Instance-Details ab.
  - Lokalisieren des privaten Schlüssels und Festlegen von Berechtigungen.
  - (Optional) Anfordern des Instance-Fingerabdrucks.
- Lassen Sie eingehenden SSH-Datenverkehr von Ihrer IP-Adresse zu.

  Stellen Sie sicher, dass die mit Ihrer Instance verknüpfte Sicherheitsgruppe eingehenden SSH-Datenverkehr von Ihrer IP-Adresse zulässt. Weitere Informationen finden Sie unter Regeln für die Verbindung mit Instances von Ihrem Computer aus.
- Installieren eines SCP-Clients

  Die meisten Linux-, Unix- und Apple-Computer enthalten standardmäßig einen SCP-Client. Falls dies bei Ihnen nicht der Fall ist, können Sie über das OpenSSH-Projekt die kostenlose Implementierung der gesamten SSH-Tools nutzen, einschließlich des SCP-Clients. Weitere Informationen finden Sie unter https://www.openssh.com.

Das folgende Verfahren führt Sie durch die Verwendung von SCP zum Übertragen einer Datei unter Verwendung des öffentlichen DNS-Namens der Instance oder der IPv6-Adresse, falls Ihre Instance eine hat.

So verwenden Sie SCP zum Übertragen von Dateien zwischen Ihrem Computer und Ihrer Instance

1. Bestimmen Sie den Speicherort der Quelldatei auf Ihrem Computer und den Zielpfad auf der Instance. In den folgenden Beispielen ist der Name der privaten Schlüsseldatei `key-pair-name.pem`, die zu übertragende Datei ist `my-file.txt`, der Benutzername für die Instance ist ec2-user, der öffentliche DNS-Name der Instance ist `instance-public-dns-name` und die IPv6-Adresse der Instance ist `2001:db8::1234:5678:1.2.3.4`.
   - (Öffentlicher DNS) Um eine Datei an das Ziel der Instance zu übertragen, geben Sie den folgenden Befehl von Ihrem Computer aus ein.

     ```
     scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@instance-public-dns-name:path/
     ```

   - (IPv6) Um eine Datei an das Ziel der Instance zu übertragen, wenn die Instance eine IPv6-Adresse hat, geben Sie den folgenden Befehl von Ihrem Computer aus ein. Die IPv6-Adresse muss in eckige Klammern (`[ ]`) gesetzt werden, die mit einem Escape-Zeichen (\) versehen sein müssen.

     ```
     scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@
     \[2001:db8::1234:5678:1.2.3.4\]:path/
     ```

2. Wenn Sie noch keine Verbindung mit der Instance über SSH hergestellt haben, wird eine Antwort wie etwa die folgende angezeigt:

   ```
   The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
   can't be established.
   RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
   Are you sure you want to continue connecting (yes/no)?
   ```

   (Optional) Sie können optional überprüfen, ob der Fingerabdruck in der Sicherheitswarnung mit dem Fingerabdruck der Instance übereinstimmt. Weitere Informationen finden Sie unter (Optional) Anfordern des Instance-Fingerabdrucks.

   Geben Sie ei **`yes`**.

3. Wenn die Übertragung erfolgreich ist, ähnelt die Antwort der folgenden:

   ```
   Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
   to the list of known hosts.
   my-file.txt                                   100%   480     24.4KB/s   00:00
   ```

4. Kehren Sie die Reihenfolge der Host-Parameter um, um eine Datei in der anderen Richtung zu übertragen (von der Amazon EC2 Instance auf Ihren Computer). Sie können beispielsweise, wie in den folgenden Beispielen gezeigt, `my-file.txt` von Ihrer EC2-Instance zu einem Ziel als `my-file2.txt` auf Ihrem lokalen Computer übertragen.

   - (Öffentlicher DNS) Um eine Datei an ein Ziel auf Ihrem Computer zu übertragen, geben Sie den folgenden Befehl von Ihrem Computer aus ein.

     ```
     scp -i /path/key-pair-name.pem ec2-user@instance-public-dns-name:path/my-file.txt path/my-file2.txt
     ```

   - (IPv6) Um eine Datei an ein Ziel auf Ihrem Computer zu übertragen, wenn die Instance eine IPv6-Adresse hat, geben Sie den folgenden Befehl von Ihrem Computer aus ein. Die IPv6-Adresse muss in eckige Klammern (`[ ]`) gesetzt werden, die mit einem Escape-Zeichen (\) versehen sein müssen.

     ```
     scp -i /path/key-pair-name.pem ec2-user@\[2001:db8::1234:5678:1.2.3.4\]:path/my-file.txt path/my-file2.txt
     ```

Verwalten von Benutzern auf einer Amazon-EC2-Linux-Instance

Jede Linux-Instance wird mit einem Standardbenutzer des Linux-Systems gestartet. Sie können Benutzer zu Ihrer Instance hinzufügen und Benutzer löschen.

Für den Standardbenutzer wird der Standardbenutzername durch das AMI bestimmt, das beim Starten der Instance angegeben wurde.

> **Note**
>
> Standardmäßig sind die Passwortauthentifizierung und die Root-Anmeldung deaktiviert und sudo ist aktiviert. Um sich bei Ihrer Instance anzumelden, müssen Sie ein Schlüsselpaar verwenden. Weitere Informationen zum Anmelden finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance mit SSH.
> Sie können die Passwortauthentifizierung und die Root-Anmeldung für Ihre Instance zulassen. Weitere Informationen finden Sie in der Dokumentation für das Betriebssystem Ihrer Instance.

> **Note**
>
> Linux-Systembenutzer sollten nicht mit IAM-Benutzern verwechselt werden. Weitere Informationen finden Sie unter IAM-Benutzer im IAM-Benutzerhandbuch.

Inhalt

- Standardbenutzernamen
- Überlegungen
- Erstellen eines Benutzers
- Entfernen eines Benutzers

Standardbenutzernamen

Der Standardbenutzername für Ihre EC2-Instance wird durch das AMI bestimmt, das beim Starten der Instance angegeben wurde.

Die Standardbenutzernamen lauten:

- Bei einem Amazon-Linux-AMI lautet der Benutzername `ec2-user`.
- Bei einem CentOS-AMI lautet der Benutzername `centos` oder `ec2-user`.
- Für ein Debian-AMI lautet der Benutzername `admin`.
- Bei einem Fedora-AMI lautet der Benutzername `fedora` oder `ec2-user`.
- Für ein FreeBSD-AMI lautet der Benutzername `ec2-user`.
- Bei einem RHEL-AMI lautet der Benutzername `ec2-user` oder `root`.
- Bei einem SUSE-AMI lautet der Benutzername `ec2-user` oder `root`.
- Für ein Ubuntu-AMI lautet der Benutzername `ubuntu`.
- Bei einem Oracle-AMI lautet der Benutzername `ec2-user`.
- Für ein Bitnami-AMI lautet der Benutzername `bitnami`.

> **Note**
>
> Um den Standardbenutzernamen für andere Linux-Distributionen zu finden, wenden Sie sich an den AMI-Anbieter.

Überlegungen

Die Verwendung des Standardbenutzers ist für viele Anwendungen ausreichend. Sie können jedoch auch Benutzer hinzufügen, damit jeder seine eigenen Dateien und Workspaces haben kann. Darüber hinaus ist das Erstellen von Benutzern für neue Benutzer viel sicherer, als mehreren (möglicherweise unerfahrenen) Benutzern Zugriff auf den Standardbenutzer zu gewähren, da der Standardbenutzer bei unsachgemäßer Verwendung großen Schaden an einem System anrichten kann. Weitere Informationen finden Sie unter Tips for Securing Your EC2 Instance.

Um Benutzern den SSH-Zugriff auf Ihre EC2-Instance mithilfe eines Linux-Systembenutzers zu gewähren, müssen Sie den SSH-Schlüssel für den Benutzer freigeben. Alternativ können Sie mit EC2 Instance Connect Benutzern Zugriff erteilen, ohne SSH-Schlüssel freigeben und verwalten zu müssen. Weitere Informationen finden Sie unter Stellen Sie über eine öffentliche IP-Adresse und Instance Connect eine Verbindung zu Ihrer EC2 Linux-Instance Connect.

Erstellen eines Benutzers

Erstellen Sie zuerst den Benutzer und fügen Sie dann den öffentlichen SSH-Schlüssel hinzu, der es dem Benutzer ermöglicht, eine Verbindung mit der Instance herzustellen und sich bei ihr anzumelden.

> **Important**
>
> In Schritt 1 dieses Verfahrens erstellen Sie ein neues Schlüsselpaar. Da ein Schlüsselpaar wie ein Passwort funktioniert, ist es wichtig, es sicher zu handhaben. Wenn Sie ein Schlüsselpaar für einen Benutzer erstellen, müssen Sie sicherstellen, dass der private Schlüssel sicher an ihn gesendet wird. Alternativ kann der Benutzer die Schritte 1 und 2 abschließen, indem er sein eigenes Schlüsselpaar erstellt, den privaten Schlüssel sicher auf seinem Computer aufbewahrt und Ihnen dann den öffentlichen Schlüssel sendet, um das Verfahren aus Schritt 3 abzuschließen.

So erstellen Sie einen Benutzer

1. Erstellen Sie ein neues Schlüsselpaar. Sie müssen die `.pem`-Datei dem Benutzer bereitstellen, für den Sie den Benutzer erstellen. Er muss diese Datei verwenden, um eine Verbindung mit der Instance herzustellen.
2. Rufen Sie den öffentlichen Schlüssel aus dem Schlüsselpaar ab, das Sie im vorherigen Schritt erstellt haben.

```
$ ssh-keygen -y -f /path_to_key_pair/key-pair-name.pem
```

Der Befehl gibt den öffentlichen Schlüssel zurück, wie im folgenden Beispiel gezeigt.

```
ssh-rsa
 AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6Vhz2ItxCih
+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/
d6RJhJOI0iBXrlsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/
i8SeJtjnV3iAoG/cQk+0FzZqaeJAAHco
+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi
+z7wB3RbBQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

3. Stellen Sie eine Verbindung mit der Instance her.
4. Verwenden Sie den adduser-Befehl, um den Benutzer zu erstellen und ihn dem System hinzuzufügen (mit einem Eintrag in der `/etc/passwd`-Datei). Der Befehl erstellt außerdem eine Gruppe und ein Basisverzeichnis für den Benutzer. In diesem Beispiel lautet der Benutzer *`newuser`*.

   - AL2023 und Amazon Linux 2

     Bei AL2023 und Amazon Linux 2 wird der Benutzer standardmäßig mit deaktivierter Kennwortauthentifizierung erstellt.

     ```
     [ec2-user ~]$ sudo adduser newuser
     ```

   - Ubuntu

     Schließen Sie den `--disabled-password`-Parameter ein, um den Benutzer mit deaktivierter Kennwortauthentifizierung zu erstellen.

     ```
     [ubuntu ~]$ sudo adduser newuser --disabled-password
     ```

5. Wechseln Sie zum neuen Benutzer, damit das Verzeichnis und die Datei, die Sie erstellen, die richtigen Eigentumsrechte erhalten.

   ```
   [ec2-user ~]$ sudo su - newuser
   ```

   Die Eingabeaufforderung wechselt von `ec2-user` zu *`newuser`*, um anzuzeigen, dass Sie die Shell-Sitzung auf den neuen Benutzer umgestellt haben.

6. Fügen Sie dem Benutzer den öffentlichen SSH-Schlüssel hinzu. Erstellen Sie zuerst im Stammverzeichnis des Benutzers ein Verzeichnis für die SSH-Schlüsseldatei. Erstellen Sie dann die Schlüsseldatei und fügen Sie abschließend den öffentlichen Schlüssel in die Schlüsseldatei ein, wie in den folgenden Unterschritten beschrieben.

   a. Erstellen Sie ein Verzeichnis `.ssh` im Stammverzeichnis von *`newuser`* und ändern Sie seine Dateiberechtigungen in `700` (nur der Eigentümer kann das Verzeichnis öffnen, lesen oder darin schreiben).

   ```
   [newuser ~]$ mkdir .ssh
   ```

   ```
   [newuser ~]$ chmod 700 .ssh
   ```

   > **Important**
   >
   > Ohne diese Dateiberechtigungen kann sich der Benutzer nicht anmelden.

   b. Erstellen Sie eine Datei namens `authorized_keys` im Verzeichnis `.ssh` und ändern Sie seine Dateiberechtigungen in `600` (nur der Eigentümer kann diese Datei lesen oder darin schreiben).

   ```
   [newuser ~]$ touch .ssh/authorized_keys
   ```

   ```
   [newuser ~]$ chmod 600 .ssh/authorized_keys
   ```

   > **Important**
   >
   > Ohne diese Dateiberechtigungen kann sich der Benutzer nicht anmelden.

   c. Öffnen Sie die Datei `authorized_keys` mit einem Texteditor Ihrer Wahl, z. B. vim oder nano.

   ```
   [newuser ~]$ nano .ssh/authorized_keys
   ```

   Fügen Sie den öffentlichen Schlüssel, den Sie in Schritt 2 abgerufen haben, in die Datei ein, und speichern Sie die Änderungen.

> **Important**
>
> Stellen Sie sicher, dass Sie den öffentlichen Schlüssel in eine durchgehende Zeile einfügen. Der öffentliche Schlüssel darf nicht auf mehrere Zeilen aufgeteilt werden.

Der Benutzer sollte sich nun bei dem *newuser*-Benutzer auf Ihrer Instance mit dem privaten Schlüssel anmelden können, der dem öffentlichen Schlüssel entspricht, den Sie der `authorized_keys`-Datei hinzugefügt haben. Weitere Informationen zu den verschiedenen Methoden zum herstellen einer Verbindung mit einer Linux-Instance finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance mit SSH.

Entfernen eines Benutzers

Wenn ein Benutzer nicht mehr benötigt wird, können Sie ihn entfernen, damit er nicht mehr verwendet werden kann.

Verwenden Sie den userdel-Befehl, um den Benutzer aus dem System zu entfernen. Wenn Sie den Parameter `-r` angeben, werden das Stammverzeichnis und die Mail Spool gelöscht. Lassen Sie den Parameter `-r` weg, um das Stammverzeichnis und die Mail Spool nicht zu löschen.

```
[ec2-user ~]$ sudo userdel -r olduser
```

Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von RDP

Sie können sich mit Amazon-EC2-Instances, die von den meisten Windows Amazon Machine Images (AMIs) erstellt werden, mithilfe des Remote Desktop verbinden. Das Remote Desktop verwendet das Remote Desktop Protocol (RDP) und bietet Ihnen die Möglichkeit, sich mit Ihrer Instance zu verbinden und sie wie einen normalen (lokalen) Computer zu verwenden. Sie steht für die meisten Windows-Versionen und auch für Mac OS zur Verfügung.

Die Lizenz für das Windows Server-Betriebssystem ermöglicht zwei gleichzeitige Remote-Verbindungen zu Verwaltungszwecken. Die Lizenzkosten für Windows Server sind in den Kosten für Ihre Windows-Instance enthalten. Falls Sie mehr als zwei gleichzeitige Remote-Verbindungen benötigen, ist der Erwerb einer Remote Desktop Services-Lizenz (RDS) erforderlich. Wenn Sie versuchen, eine dritte Verbindung aufzubauen, erhalten Sie eine Fehlermeldung.

> **Tip**
>
> Wenn Sie eine Verbindung zu Ihrer Instance herstellen müssen, um Boot-, Netzwerkkonfigurations- und andere Probleme für Instances, die auf dem AWS Nitro System aufgebaut sind, zu beheben, können Sie die EC2 Serielle Konsole für Instanzen verwenden.

Inhalt

- Verbindung zu Ihrer Windows-Instance mithilfe eines RDP-Clients herstellen
- Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von Fleet Manager
- Dateien mit RDP auf eine Windows-Instance übertragen

Verbindung zu Ihrer Windows-Instance mithilfe eines RDP-Clients herstellen

Sie können eine Verbindung zu Ihrer Windows-Instance mit einem RDP-Client wie folgt herstellen.

> **Tip**
>
> Alternativ können Sie mit Systems Manager Flotten-Manager oder EC2-Instance-Verbindungs-Endpunkt eine Verbindung zu Ihrer Windows-Instance herstellen.

Voraussetzungen

Sie müssen die folgenden Voraussetzungen erfüllen, um eine Verbindung mit Ihrer Windows-Instance mithilfe eines RDP-Clients herzustellen.

- Vervollständigen Sie die allgemeinen Voraussetzungen.
  - Stellen Sie sicher, dass Ihre Instance ihre Statusprüfungen bestanden hat. Es kann ein paar Minuten dauern, bis die Instance für die Verbindung bereitsteht. Weitere Informationen finden Sie unter Anzeigen der Statusprüfungen.
  - Rufen Sie die erforderlichen Instance-Details ab.
  - Lokalisieren des privaten Schlüssels und Festlegen von Berechtigungen.
  - (Optional) Anfordern des Instance-Fingerabdrucks.
- Installieren eines RDP-Clients.

  - (Windows) Windows enthält standardmäßig einen RDP-Client. Zum Überprüfen geben Sie mstsc in ein Eingabeaufforderungfenster ein. Wenn Ihr Computer diesen Befehl nicht erkennt, laden Sie die Microsoft Remote Desktop App aus dem Microsoft Store herunter.
  - (macOS X) Laden Sie die Windows-App für Mac (ehemalig Microsoft Remote Desktop) vom Mac App Store herunter.
  - (Linux) Verwenden Sie Remmina.
- Lassen Sie eingehenden RDP-Datenverkehr von Ihrer IP-Adresse zu.

  Stellen Sie sicher, dass die mit Ihrer Instance verknüpfte Sicherheitsgruppe eingehenden RDP-Datenverkehr von Ihrer IP-Adresse zulässt. Weitere Informationen finden Sie unter Regeln für die Verbindung mit Instances von Ihrem Computer aus.

Das Administrator-Passwort abrufen

Wenn Sie Ihre Instance einer Domain zugewiesen haben, können Sie eine Verbindung mit Ihrer Instance mithilfe der Domain-Anmeldeinformationen von Directory Service herstellen. Verwenden Sie auf dem Anmeldebildschirm für Remotedesktop anstelle des lokalen Computernamens und des generierten Kennworts den vollqualifizierten Benutzernamen für den Administrator (z. B. **`corp.example.com\Admin`**) und das Passwort für dieses Konto.

Zur Verbindung mit einer Windows-Instance mit RDP müssen Sie das anfängliche Administratorpasswort abrufen und es angeben, wenn Sie per Remote Desktop eine Verbindung mit Ihrer Instance herstellen. (Nach dem Start der Instance dauert es einige Minuten, bis das Passwort verfügbar ist.) Ihr Konto muss über die Berechtigung zum Aufrufen der Aktion GetPasswordData verfügen. Weitere Informationen finden Sie unter Beispielrichtlinien zur Steuerung des Zugriffs auf die EC2 Amazon-API.

Der Standardbenutzername für das Administratorkonto hängt von der Sprache des Betriebssystems (OS) ab, das im AMI enthalten ist. Um den richtigen Benutzernamen zu ermitteln, identifizieren Sie die Sprache des Betriebssystems und wählen Sie dann den entsprechenden Benutzernamen. Für ein englisches Betriebssystem lautet der Benutzername beispielsweise `Administrator`, für ein französisches Betriebssystem ist es `Administrateur` und für ein portugiesisches Betriebssystem ist es `Administrador`. Wenn eine Sprachversion des Betriebssystems keinen Benutzernamen in derselben Sprache hat, wählen Sie den Benutzernamen `Administrator (Other)`. Weitere Informationen finden Sie unter Lokalisierte Namen für Administratorkonto in Windows auf der Microsoft-Website.

So rufen Sie das Administrator-Passwort ab

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und klicken Sie auf Connect (Verbinden).
4. Auf der Seite Verbindung mit Instance herstellen wählen Sie die Registerkarte RDP-Client aus.
5. Wählen Sie unter Benutzername den Standardbenutzernamen für das Administratorkonto aus. Der von Ihnen gewählte Benutzername muss der Sprache des Betriebssystems (OS) entsprechen, das im AMI enthalten ist, das Sie zum Starten Ihrer Instance verwendet haben. Wenn es keinen Benutzernamen in derselben Sprache wie Ihr Betriebssystem gibt, wählen Sie Administrator (Andere).
6. Wählen Sie Passwort erhalten.
7. Gehen Sie auf der Seite Windows-Passwort erhalten wie folgt vor:

    a. Klicken Sie auf Private Schlüsseldatei hochladen und navigieren Sie zu der privaten Schlüsseldatei (`.pem`), die Sie beim Starten der Instance angegeben haben. Wählen Sie die Datei aus und klicken Sie auf Open (Öffnen), um den gesamten Inhalt der Datei auf dieses Fenster zu kopieren.

    b. Klicken Sie auf Password entschlüsseln. Die Seite Passwort erhalten wird geschlossen und das Standard-Administrator-Passwort für die Instance wird unter Passwort angezeigt. Es ersetzt den zuvor angezeigten Link Passwort erhalten.

    c. Bewahren Sie das Passwort an einem sicheren Ort auf. Dieses Passwort wird benötigt, um eine Verbindung mit der Instance herzustellen.

Herstellen einer Verbindung mit Ihrer Windows-Instance

Das folgende Verfahren verwendet den Remote Desktop Connection Client für Windows (MSTSC). Wenn Sie einen anderen RDP-Client verwenden, laden Sie die RDP-Datei herunter und lesen Sie dann in der Dokumentation für den RDP-Client nach, wie Sie die RDP-Verbindung herstellen.

So stellen Sie mithilfe eines RDP-Clients eine Verbindung zu einer Windows-Instance her

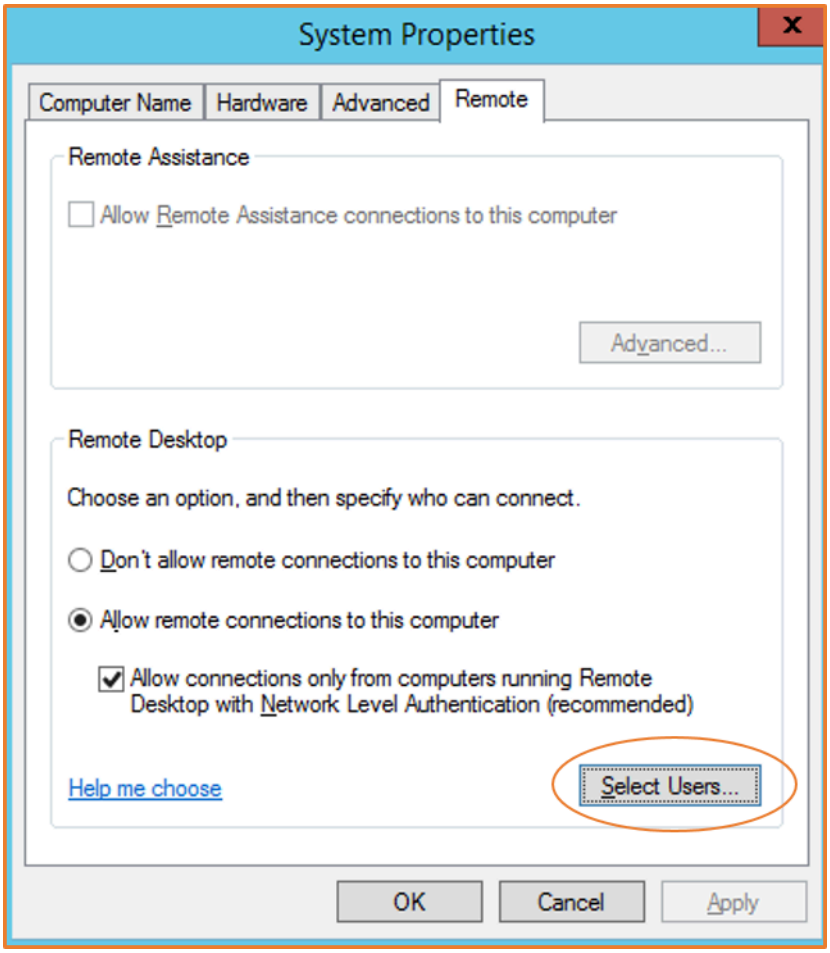
1. Wählen Sie auf der Seite Mit Instance verbinden die Option Remote-Desktop-Datei herunterladen aus. Klicken Sie nach dem Herunterladen der Datei auf Abbrechen, um zur Seite Instances zurückzukehren. Die RDP-Datei wurde in Ihren `Downloads`-Ordner heruntergeladen.
2. Führen Sie `mstsc.exe` aus, um den RDP-Client zu öffnen.

3. Erweitern Sie Optionen anzeigen, wählen Sie Öffnen und wählen Sie die RDP-Datei aus Ihrem `Downloads`-Ordner aus.
4. Standardmäßig ist Computer der öffentliche IPv4-DNS-Name der Instance und Benutzername ist das Administratorkonto. Um stattdessen über IPv6 eine Verbindung mit der Instance herzustellen, ersetzen Sie den öffentlichen IPv4-DNS-Namen der Instance durch ihre IPv6-Adresse. Überprüfen und ändern Sie nach Bedarf die folgenden Einstellungen.
5. Wählen Sie Connect aus. Wenn Sie eine Warnmeldung erhalten, dass der Publisher der Remote-Verbindung unbekannt ist, klicken Sie auf Verbinden, um fortzufahren.
6. Geben Sie das Passwort ein, das Sie zuvor gespeichert haben, und klicken Sie dann auf OK.
7. Aufgrund der Art selbst signierter Zertifikate erhalten Sie möglicherweise eine Warnmeldung, dass das Sicherheitszertifikat nicht authentifiziert werden konnte. Führen Sie eine der folgenden Aktionen aus:
   - Wenn Sie dem Zertifikat vertrauen, wählen Sie Ja, um eine Verbindung mit Ihrer Instance herzustellen.
   - [Windows] Bevor Sie fortfahren, vergleichen Sie den Fingerabdruck des Zertifikats mit dem Wert im Systemprotokoll, um die Identität des Remotecomputers zu bestätigen. Wählen Sie Zertifikat anzeigen und dann auf der Registerkarte Details die Option Fingerabdruck. Vergleichen Sie diesen Wert mit dem Wert `RDPCERTIFICATE-THUMBPRINT` in Aktionen, Überwachen und Problembehandlung, Systemprotokoll abrufen.
   - [Mac OS X] Bevor Sie fortfahren, vergleichen Sie den Fingerabdruck des Zertifikats mit dem Wert im Systemprotokoll, um die Identität des Remotecomputers zu bestätigen. Wählen Sie Zertifikat anzeigen, erweitern Sie Details und wählen Sie SHA1-Fingerabdrücke. Vergleichen Sie diesen Wert mit dem Wert `RDPCERTIFICATE-THUMBPRINT` in Aktionen, Überwachen und Problembehandlung, Systemprotokoll abrufen.
8. Wenn die RDP-Verbindung erfolgreich ist, zeigt der RDP-Client den Windows-Anmeldebildschirm und dann den Windows-Desktop an. Wenn Sie stattdessen eine Fehlermeldung erhalten, finden Sie weitere Informationen unter the section called “Der Remotedesktopdienst kann keine Verbindung zu dem Remotecomputer herstellen”. Wenn Sie mit der RDP-Verbindung fertig sind, können Sie den RDP-Client schließen.

Benutzerkonten konfigurieren

Nachdem Sie eine Verbindung mit Ihrer Instance über RDP hergestellt haben, empfehlen wir, die folgenden Aufgaben auszuführen:

- Ändern Sie das Standard-Passwort für den Administrator. Sie können das Passwort ändern, während Sie in der Instance angemeldet sind, genau wie bei jedem Computer, auf dem Windows-Server ausgeführt wird.
- Erstellen Sie einen anderen Benutzer mit Administratorrechten für die Instance. Dies dient als Sicherheitsmaßnahme, falls Sie das Administratorpasswort vergessen haben oder ein Problem mit dem Administratorkonto besteht. Der neue Benutzer muss über die Berechtigung zum Zugriff auf die Instance aus der Ferne verfügen. Öffnen Sie Systemeigenschaften durch einen Rechtsklick auf das Symbol Dieser Computer auf dem Windows-Desktop oder wählen Sie im Explorer Eigenschaften. Wählen Sie Remoteeinstellungen und danach Benutzer auswählen, um den Benutzer der Gruppe Remotedesktopbenutzer hinzuzufügen.



Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von Fleet Manager

Mit Fleet Manager, einer Funktion von AWS Systems Manager, können Sie über das Remote Desktop Protocol (RDP) eine Verbindung zu Windows-Instances herstellen und bis zu vier Windows-Instances auf derselben Seite in der AWS-Managementkonsole anzeigen. Sie können

eine Verbindung mit der ersten Instance im Fleet Manager Remote Desktop direkt über die Seite Instances in der Amazon-EC2-Konsole herstellen. Weitere Informationen zu Fleet Manager finden Sie unter Mit Remote Desktop eine Verbindung zu einem verwalteten Knoten herstellen im Benutzerhandbuch für AWS Systems Manager.

Sie müssen eingehenden RDP-Datenverkehr von Ihrer IP-Adresse nicht ausdrücklich zulassen, wenn Sie Fleet Manager für die Verbindung verwenden. Fleet Manager erledigt das für Sie.

Voraussetzungen

Bevor Sie versuchen, eine Verbindung mit einer Instance mithilfe von Flotten-Manager herzustellen, müssen Sie Ihre Umgebung einrichten. Weitere Informationen finden Sie unter Umgebung einrichten im AWS Systems Manager-Benutzerhandbuch.

So stellen Sie mithilfe von Flotten-Manager eine Verbindung zu einer Windows-Instance her

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und klicken Sie auf Connect (Verbinden).
4. Wählen Sie auf der Registerkarte RDP-Client für Verbindungstyp die Option Mit Flotten-Manager verbinden aus.
5. Wählen Sie Fleet Manager Remote Destop aus. Daraufhin wird die Seite Fleet Manager Remote Desktop in der AWS Systems Manager-Konsole geöffnet.
6. Geben Sie Ihre Anmeldeinformationen ein und wählen Sie Verbinden aus.
7. Wenn die RDP-Verbindung erfolgreich ist, zeigt Flotten-Manager den Windows-Desktop an. Wenn Sie mit der Sitzung fertig sind, wählen Sie Aktionen, Sitzung beenden.

Weitere Informationen finden Sie im AWS Systems Manager-Benutzerhandbuch unter Herstellen einer Verbindung zu einer Windows-Server-verwalteten Instance mithilfe von Remote Desktop.

Dateien mit RDP auf eine Windows-Instance übertragen

Sie können mit Ihrer Windows-Instance so wie mit jedem anderen Windows-Server arbeiten. Sie können beispielsweise zwischen einer Windows-Instance und Ihrem lokalen Computer Dateien übertragen, indem Sie das Datenaustausch-Feature der Microsoft Remote Desktop Connection (RDP)-Software verwenden. Sie können auf lokale Dateien auf Festplattenlaufwerken, DVD-Laufwerken, tragbaren Medienlaufwerken und zugeordneten Netzlaufwerken zugreifen.

Um von Ihren Windows-Instances aus auf Ihre lokalen Dateien zugreifen zu können, müssen Sie das Feature zur lokalen Dateifreigabe aktivieren, indem Sie das Laufwerk der Remotesitzung Ihrem lokalen Laufwerk zuordnen. Die Schritte unterscheiden sich geringfügig, je nachdem, ob Ihr lokales Computerbetriebssystem Windows oder macOS X ist.

Weitere Informationen zu den Voraussetzungen für eine Verbindung mit RDP finden Sie unter Voraussetzungen.

Windows

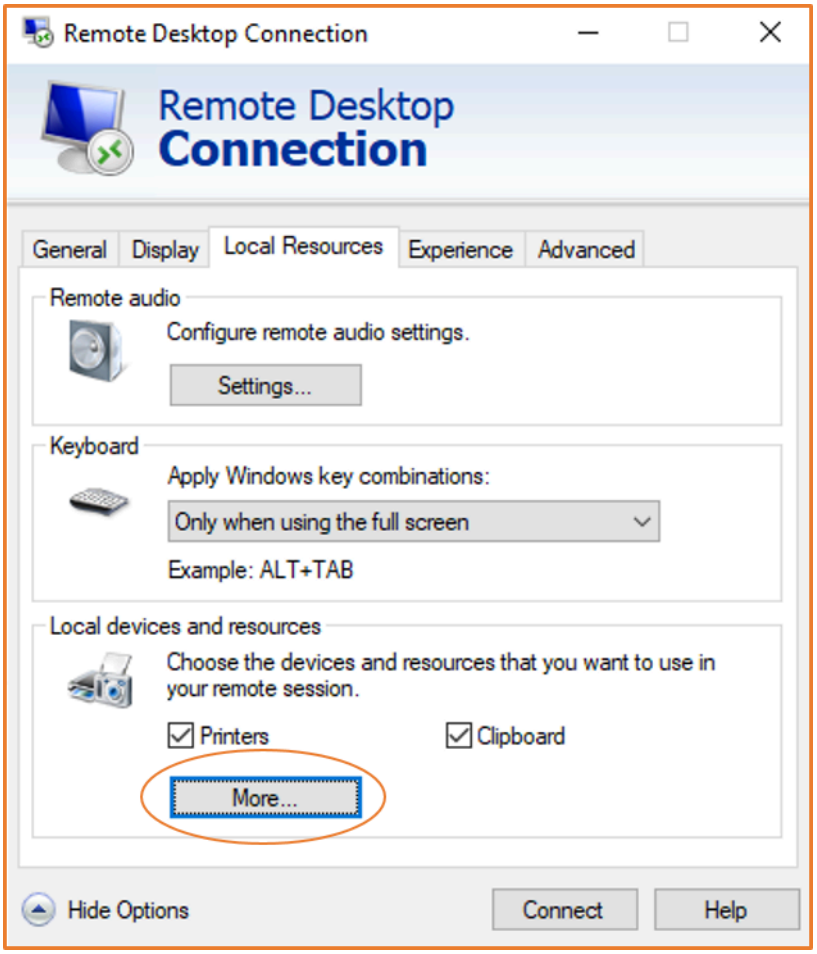
Laufwerk der Remotesitzung dem lokalen Laufwerk auf Ihrem lokalen Windows-Computer zuordnen

1. Öffnen Sie den Remote Desktop Connection-Client.
2. Wählen Sie Show Options aus.
3. Fügen Sie den Instance-Host-Namen dem Feld Computer und den Benutzernamen dem Feld Benutzername hinzu, wie nachfolgend gezeigt:

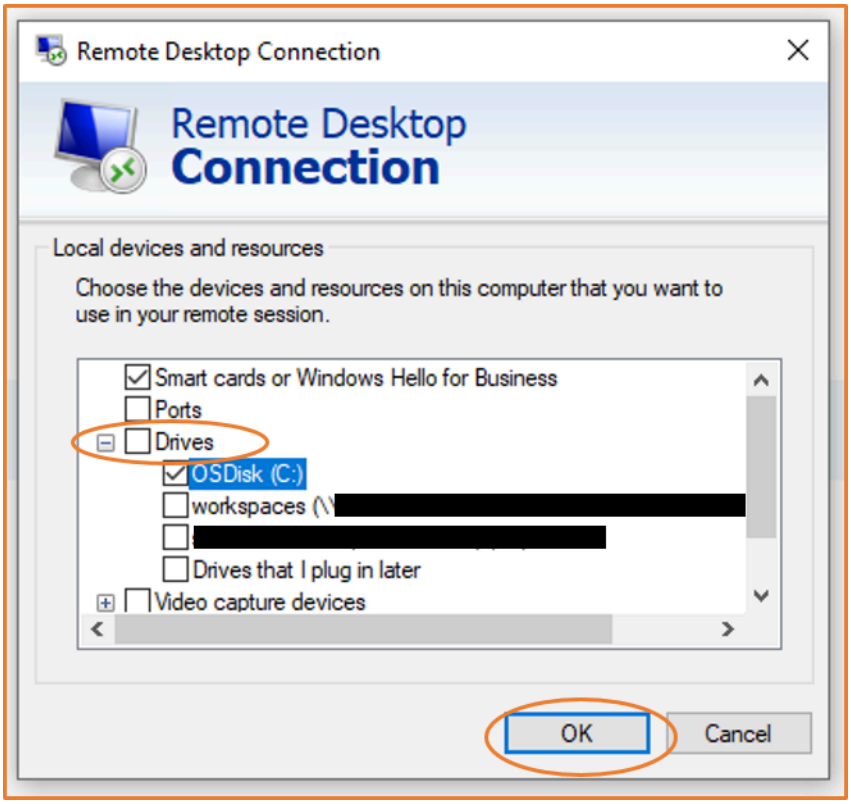
   a. Wählen Sie unter Connection settings (Verbindungseinstellungen) Open... (Öffnen…) aus und navigieren Sie zur RDP-Verknüpfungsdatei, die Sie in der Amazon-EC2-Konsole heruntergeladen haben. Die Datei enthält den öffentlichen IPv4-DNS-Hostnamen, der die Instance identifiziert, und den Benutzernamen des Administrators.

   b. Wählen Sie die Datei und dann Open (Öffnen) aus. Die Felder Computer und User name (Benutzername) werden mit den Werten aus der RDP-Verknüpfungsdatei gefüllt.

   c. Wählen Sie Speichern.
4. Wählen Sie die Registerkarte Local Resources (Lokale Ressourcen).
5. Wählen Sie unter Local devices and resources (Lokale Geräte und Ressourcen) die Option More... (Mehr...) aus.



6. Öffnen Sie Drives (Laufwerke) und wählen Sie das lokale Laufwerk aus, das Sie der Windows-Instance zuordnen möchten.
7. Klicken Sie auf OK.

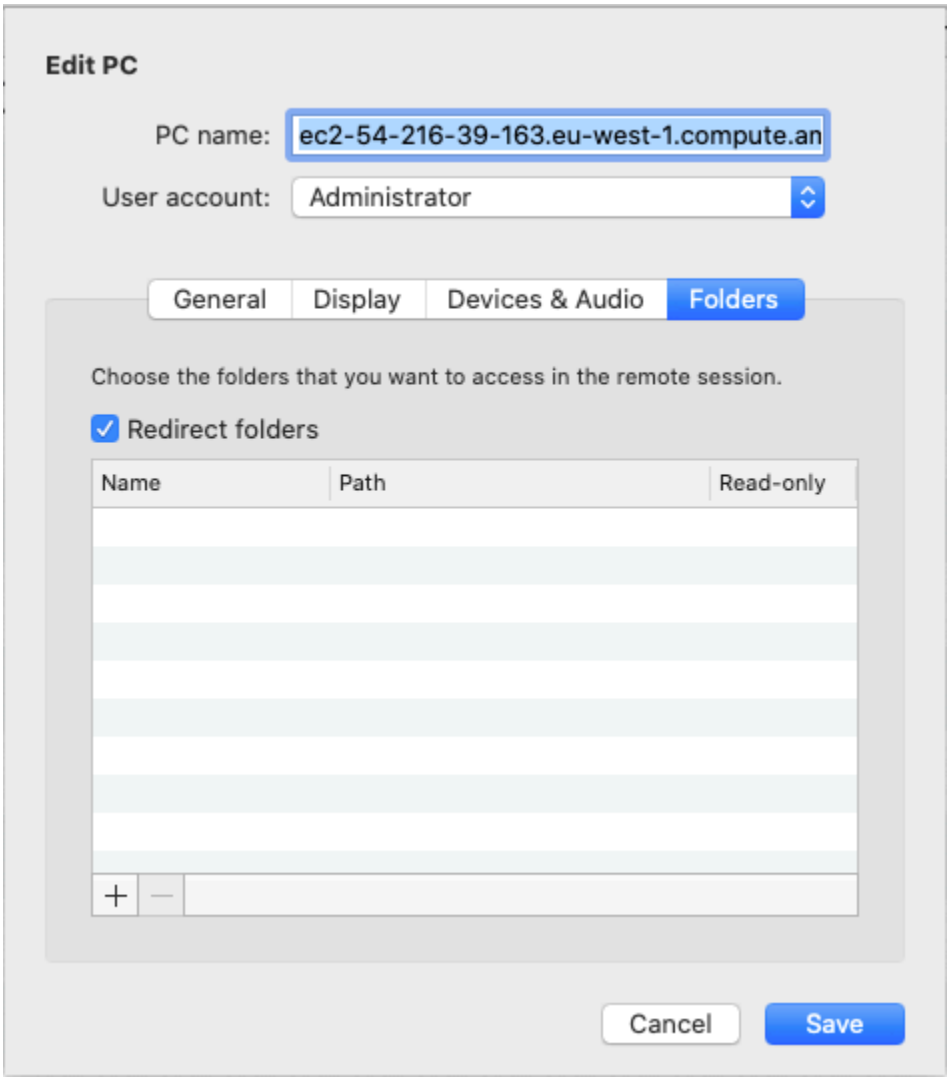


8. Wählen Sie Connect (Verbinden) aus, um eine Verbindung mit der Windows-Instance herzustellen.

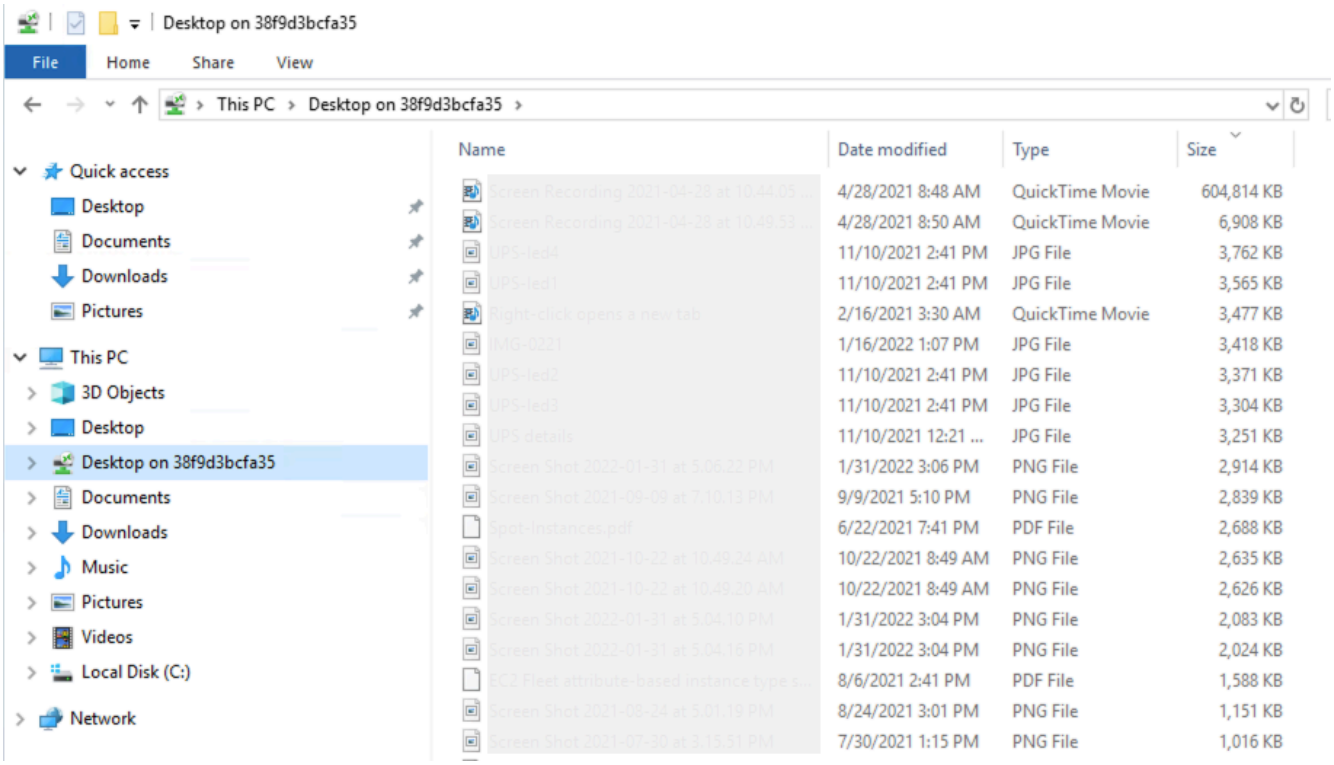
macOS X

Laufwerk der Remotesitzung dem lokalen Verzeichnis auf Ihrem lokalen macOS X-Computer zuordnen

1. Öffnen Sie den Remote Desktop Connection-Client.
2. Navigieren Sie zu der RDP-Datei, die Sie in der Amazon-EC2-Konsole heruntergeladen haben (als Sie erstmals die Verbindung zur Instance hergestellt haben), und ziehen Sie sie auf den Remotedesktopverbindungs-Client.
3. Klicken Sie mit der rechten Maustaste auf die RDP-Datei und wählen Sie Edit (Bearbeiten) aus.
4. Wählen Sie die Registerkarte Ordner und dann das Kontrollkästchen Ordner umleiten aus.



5. Wählen Sie das +-Symbol unten links aus, navigieren Sie zu dem Ordner, den Sie zuordnen möchten, und wählen Sie Open (Öffnen) aus. Wiederholen Sie diesen Schritt für jeden Ordner, der zugeordnet werden soll.
6. Wählen Sie Speichern.
7. Wählen Sie Connect (Verbinden) aus, um eine Verbindung mit der Windows-Instance herzustellen. Sie werden zur Passworteingabe aufgefordert.
8. Erweitern Sie auf der Instance im Datei-Explorer Dieser PC und navigieren Sie zu dem freigegebenen Ordner, über den Sie auf Ihre lokalen Dateien zugreifen können. Im folgenden Screenshot wurde der Ordner Desktop auf dem lokalen Computer dem Laufwerk der Remotesitzung auf der Instance zugeordnet.



Weitere Informationen dazu, wie Sie lokale Geräte für eine Remotesitzung auf einem Mac-Computer verfügbar machen, finden Sie unter Erste Schritte mit dem macOS-Client.

Verbinden mit Ihrer Amazon-EC2-Instance über Session Manager

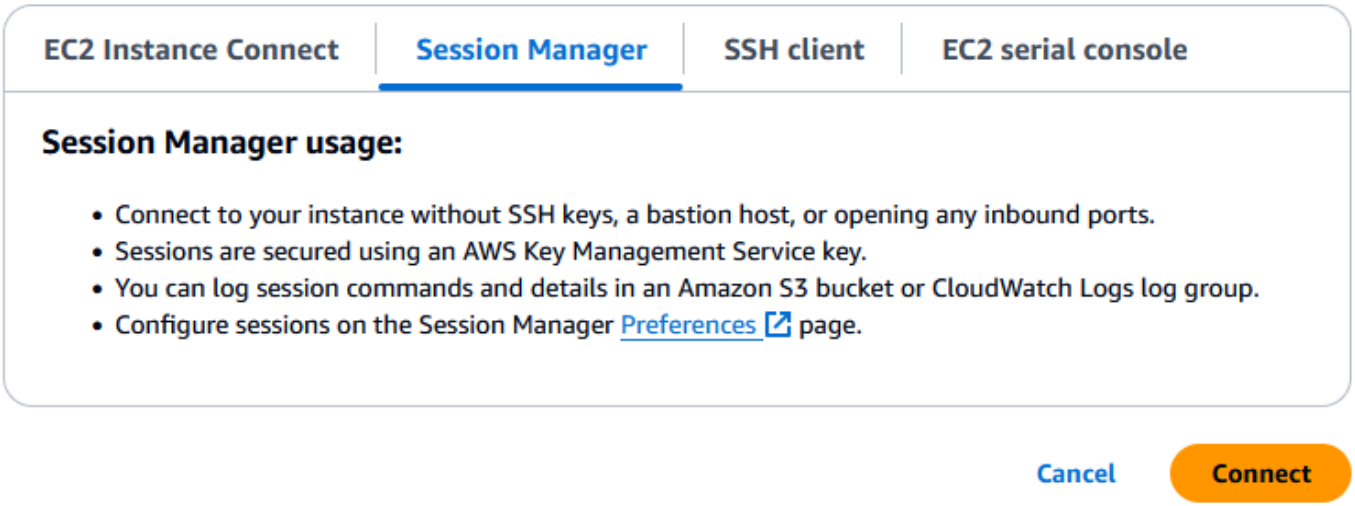
Der Session Manager ist eine vollständig verwaltete AWS Systems Manager-Funktion, mit der Sie Ihre Amazon EC2-Instances über eine interaktive browserbasierte One-Click-Shell oder über AWS CLI verwalten können. Sie können Session Manager verwenden, um eine Sitzung mit einer Instance in Ihrem Konto zu starten. Nachdem die Sitzung gestartet wurde, können Sie interaktive Befehle auf der Instance wie bei jedem anderen Verbindungstyp ausführen. Weitere Informationen zum Session Manager finden Sie unter AWS Systems Manager Session Manager im AWS Systems Manager-Benutzerhandbuch.

Voraussetzungen

Bevor Sie versuchen, eine Verbindung mit einer Instance mithilfe des Session Managers herzustellen, müssen Sie die erforderlichen Einrichtungsschritte abschließen. Die Instance muss beispielsweise von SSM verwaltet werden und eine angefügte IAM-Rolle mit der Richtlinie AmazonSSMManagedInstanceCore haben. Weitere Informationen finden Sie unter Einrichten von Session Manager.

So stellen Sie mithilfe von Session Manager in der Amazon EC2-Konsole eine Verbindung zu einer Amazon-EC2-Instance her

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance und Connect (Verbinden) aus.
4. Wählen Sie für Verbindungsmethode Session Manager.
5. Wählen Sie Verbinden, um die Sitzung zu starten.



Fehlerbehebung

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht berechtigt sind, eine oder mehrere Systems-Manager-Aktionen auszuführen (`ssm:command-name`), müssen Sie Ihre Richtlinien aktualisieren, damit Sie Sitzungen über die Amazon-EC2-Konsole starten können. Weitere Informationen und Anleitungen finden Sie unter Quick-Start Standard-IAM-Richtlinien für Session Manager im AWS Systems Manager-Benutzerhandbuch.

Stellen Sie über eine öffentliche IP-Adresse und Instance Connect eine Verbindung zu Ihrer EC2 Linux-Instance Connect

Amazon EC2 Instance Connect bietet eine sichere Möglichkeit, über Secure Shell (SSH) eine Verbindung zu Ihren Linux-Instances herzustellen. Mit EC2 Instance Connect verwenden Sie AWS Identity and Access Management (IAM) -Richtlinien und -Prinzipale, um den SSH-Zugriff auf Ihre Instances zu kontrollieren, sodass Sie SSH-Schlüssel nicht mehr teilen und verwalten müssen. Alle

Verbindungsanfragen, die EC2 Instance Connect verwenden, werden protokolliert, AWS CloudTrail sodass Sie Verbindungsanfragen überprüfen können.

Sie können EC2 Instance Connect verwenden, um über die EC2 Amazon-Konsole oder den SSH-Client Ihrer Wahl eine Verbindung zu Ihren Instances herzustellen.

Wenn Sie über Instance Connect eine Verbindung zu einer EC2 Instance Connect, überträgt die EC2 Instance Connect-API einen öffentlichen SSH-Schlüssel an die Instance-Metadaten, wo er 60 Sekunden lang verbleibt. Eine an Ihren Benutzer angefügte IAM-Richtlinie autorisiert Ihren Benutzer, den öffentlichen Schlüssel an die Instance-Metadaten zu übertragen. Der SSH-Daemon verwendet `AuthorizedKeysCommand` und`AuthorizedKeysCommandUser`, die bei der Installation von EC2 Instance Connect konfiguriert werden, um den öffentlichen Schlüssel aus den Instanz-Metadaten für die Authentifizierung zu suchen, und verbindet Sie mit der Instance.

> **Tip**
>
> EC2 Instance Connect ist eine der Optionen, um eine Verbindung zu Ihrer Linux-Instance herzustellen. Weitere Optionen finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance mit SSH. Um eine Verbindung mit einer Windows-Instance herzustellen, lesen Sie Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von RDP.

Preisgestaltung

EC2 Instance Connect ist ohne zusätzliche Kosten verfügbar.

Verfügbarkeit in Regionen

EC2 Instance Connect ist in allen AWS-Regionen Ländern außer im asiatisch-pazifischen Raum (Taipeh) verfügbar. Es wird in Local Zones nicht unterstützt.

Inhalt

- Tutorial: Vervollständigen Sie die Konfiguration, die für die Verbindung mit Ihrer Instance mithilfe von EC2 Instance Connect erforderlich ist
- Voraussetzungen für EC2 Instance Connect
- Erteilen Sie IAM-Berechtigungen für EC2 Instance Connect
- EC2 Installiere Instance Connect auf deinen EC2 Instances
- Stellen Sie mithilfe von Instance Connect eine Verbindung zu einer EC2 Linux-Instance Connect

- EC2 Instance Connect deinstallieren

Einen Blogbeitrag, in dem erläutert wird, wie Sie die Sicherheit Ihrer Bastion-Hosts mithilfe von EC2 Instance Connect verbessern können, finden Sie unter Sichern Ihrer Bastion-Hosts mit Amazon EC2 Instance Connect.

Tutorial: Vervollständigen Sie die Konfiguration, die für die Verbindung mit Ihrer Instance mithilfe von EC2 Instance Connect erforderlich ist

Um über EC2 Instance Connect in der EC2 Amazon-Konsole eine Verbindung zu Ihrer Instance herzustellen, müssen Sie zunächst die erforderliche Konfiguration abschließen, damit Sie erfolgreich eine Verbindung zu Ihrer Instance herstellen können. Der Zweck dieses Tutorials besteht darin, Sie durch die Aufgaben zum Abschließen der erforderlichen Konfiguration zu führen.

Tutorial-Übersicht

In diesem Tutorial erledigen Sie die vier folgenden Aufgaben:

- Aufgabe 1: Gewähren Sie die für die Verwendung von EC2 Instance Connect erforderlichen Berechtigungen

  Zunächst erstellen Sie eine IAM-Richtlinie, welche die IAM-Berechtigungen enthält, mit denen Sie einen öffentlichen Schlüssel für die Instance-Metadaten bereitstellen können. Hängen Sie diese Richtlinie an Ihre IAM-Identität (Benutzer, Gruppe oder Rolle) an, sodass Ihre IAM-Identität diese Berechtigungen erhält.
- Aufgabe 2: Zulassen von eingehendem Traffic vom EC2 Instance Connect-Dienst zu Ihrer Instance

  Anschließend erstellen Sie eine Sicherheitsgruppe, die den Datenverkehr vom EC2 Instance Connect-Dienst zu Ihrer Instance zulässt. Dies ist erforderlich, wenn Sie EC2 Instance Connect in der EC2 Amazon-Konsole verwenden, um eine Verbindung zu Ihrer Instance herzustellen.
- Aufgabe 3: Ihre Instance starten

  Anschließend starten Sie eine EC2 Instance mit einem AMI, auf dem EC2 Instance Connect vorinstalliert ist, und fügen die Sicherheitsgruppe hinzu, die Sie im vorherigen Schritt erstellt haben.
- Aufgabe 4: Verbindung mit Ihrer Instance herstellen

  Schließlich verwenden Sie EC2 Instance Connect in der EC2 Amazon-Konsole, um eine Verbindung zu Ihrer Instance herzustellen. Wenn Sie eine Verbindung herstellen können,

können Sie sicher sein, dass die erforderliche Konfiguration, die Sie in den Aufgaben 1, 2 und 3 abgeschlossen haben, erfolgreich war.

Aufgabe 1: Gewähren Sie die für die Verwendung von EC2 Instance Connect erforderlichen Berechtigungen

Wenn Sie über Instance Connect eine Verbindung zu einer EC2 Instance Connect, überträgt die EC2 Instance Connect-API einen öffentlichen SSH-Schlüssel an die Instance-Metadaten, wo er 60 Sekunden lang verbleibt. Sie benötigen eine IAM-Richtlinie, die an Ihre IAM-Identität (Benutzer, Gruppe oder Rolle) angefügt ist, damit Sie die erforderliche Berechtigung haben, den öffentlichen Schlüssel an die Instance-Metadaten zu übertragen.

Aufgabenziel

Sie werden dann die IAM-Richtlinie erstellen, die die Berechtigung gewähren, den öffentlichen Schlüssel an die Instance zu übertragen. Die spezifische Aktion, die zugelassen werden soll, ist `ec2-instance-connect:SendSSHPublicKey`. Sie müssen die `ec2:DescribeInstances` Aktion auch zulassen, damit Sie Ihre Instance in der EC2 Amazon-Konsole anzeigen und auswählen können.

Nachdem Sie die Richtlinie erstellt haben, verknüpfen Sie sie mit Ihrer IAM-Identität (Benutzer, Benutzergruppe oder Rolle), damit Ihre IAM-Identität die Berechtigungen erhält.

Sie werden eine Richtlinie erstellen, die wie folgt konfiguriert ist:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeInstances",
            "Resource": "*"
        }
    ]
```

```
}
```

> **Important**
>
> Die in diesem Tutorial erstellte IAM-Richtlinie ist sehr freizügig. Sie ermöglicht es Ihnen, mit einem beliebigen AMI-Benutzernamen eine Verbindung zu jeder Instance herzustellen. Wir verwenden diese sehr freizügige Richtlinie, um das Tutorial einfach zu halten und uns auf die spezifischen Konfigurationen zu konzentrieren, die in diesem Tutorial vermittelt werden. In einer Produktionsumgebung empfehlen wir jedoch, dass Ihre IAM-Richtlinie so konfiguriert wird, dass sie geringste Berechtigungen bereitstellt. Beispiele für IAM-Richtlinien finden Sie unter Erteilen Sie IAM-Berechtigungen für EC2 Instance Connect.

Um eine IAM-Richtlinie zu erstellen und anzuhängen, die es Ihnen ermöglicht, EC2 Instance Connect zu verwenden, um eine Verbindung zu Ihren Instances herzustellen

1. Zuerst erstellen Sie die IAM-Richtlinie
   a. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
   b. Wählen Sie im Navigationsbereich Richtlinien.
   c. Wählen Sie Richtlinie erstellen aus.
   d. Führen Sie auf der Seite Berechtigungen festlegen Folgendes aus:
      i. Wählen Sie für Service EC2 Instance Connect aus.
      ii. Beginnen Sie unter Zulässige Aktionen im Suchfeld mit der Eingabe, **`send`** um die entsprechenden Aktionen anzuzeigen, und wählen Sie dann SSHPublicSchlüssel senden aus.
      iii. Wählen Sie unter Ressourcen die Option Alle aus. Für eine Produktionsumgebung empfehlen wir, die Instance anhand ihres ARN anzugeben, aber für dieses Tutorial lassen Sie alle Instances zu.
      iv. Wählen Sie Add more permissions aus.
      v. Wählen Sie unter Service die Option EC2aus.
      vi. Beginnen Sie unter Zulässige Aktionen im Suchfeld mit der Eingabe**`describein`**, um die entsprechenden Aktionen anzuzeigen, und wählen Sie dann aus DescribeInstances.
      vii. Wählen Sie Weiter aus.

e. Gehen Sie auf der Seite Überprüfen und erstellen wie folgt vor:

   i. Geben Sie unter Policy Name (Richtlinienname) einen Namen für diese Richtlinie ein.

   ii. Wählen Sie Richtlinie erstellen aus.

2. Fügen Sie dann die Richtlinie Ihrer Identität an

   a. Wählen Sie im Navigationsbereich der IAM-Konsole die Option Policies.

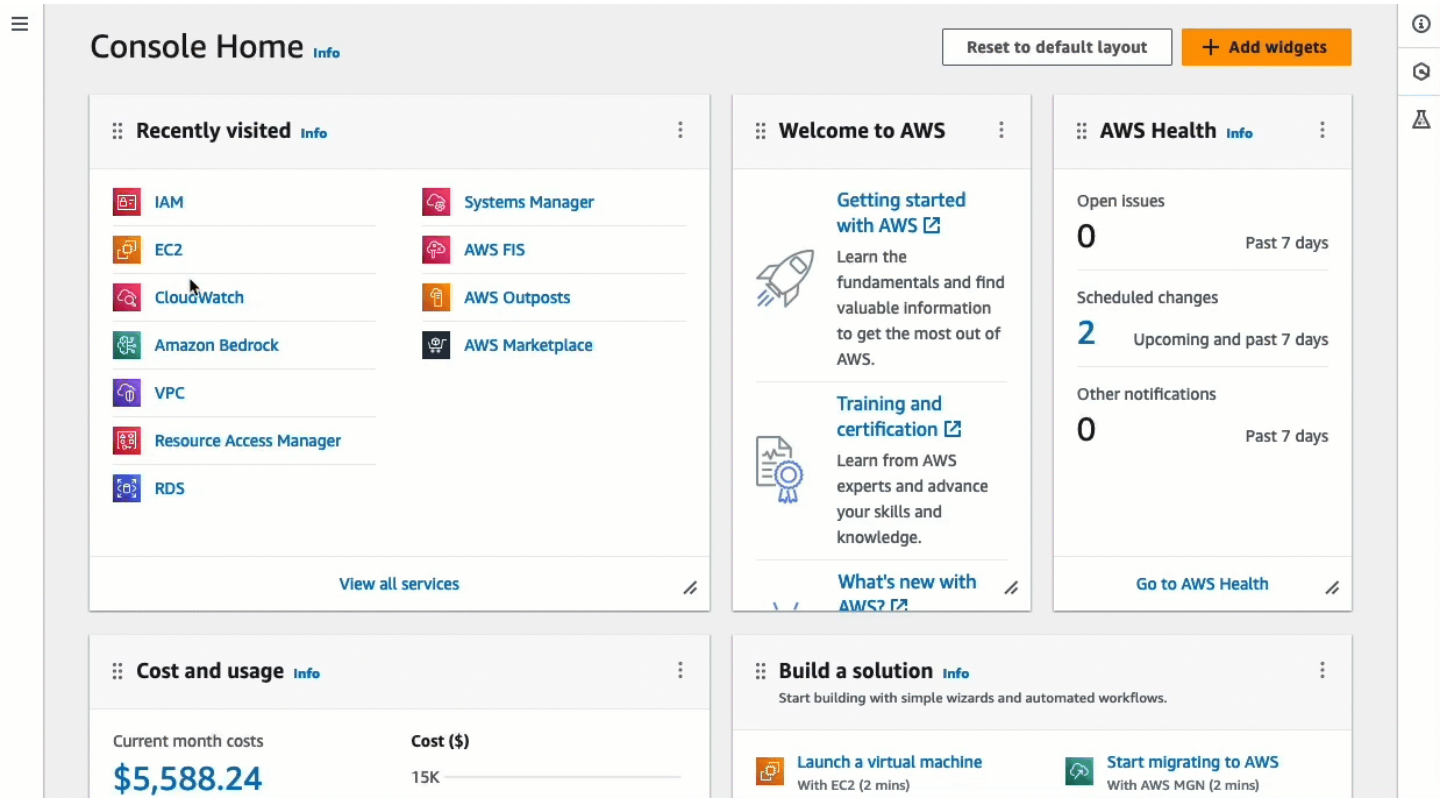
   b. Aktivieren Sie in der Liste der Richtlinien die Optionsschaltfläche neben dem Namen der anzufügenden Richtlinie aus. Sie können über das Suchfeld die Liste der Gruppen filtern.

   c. Wählen Sie Actions (Aktionen) und Attach (Anfügen).

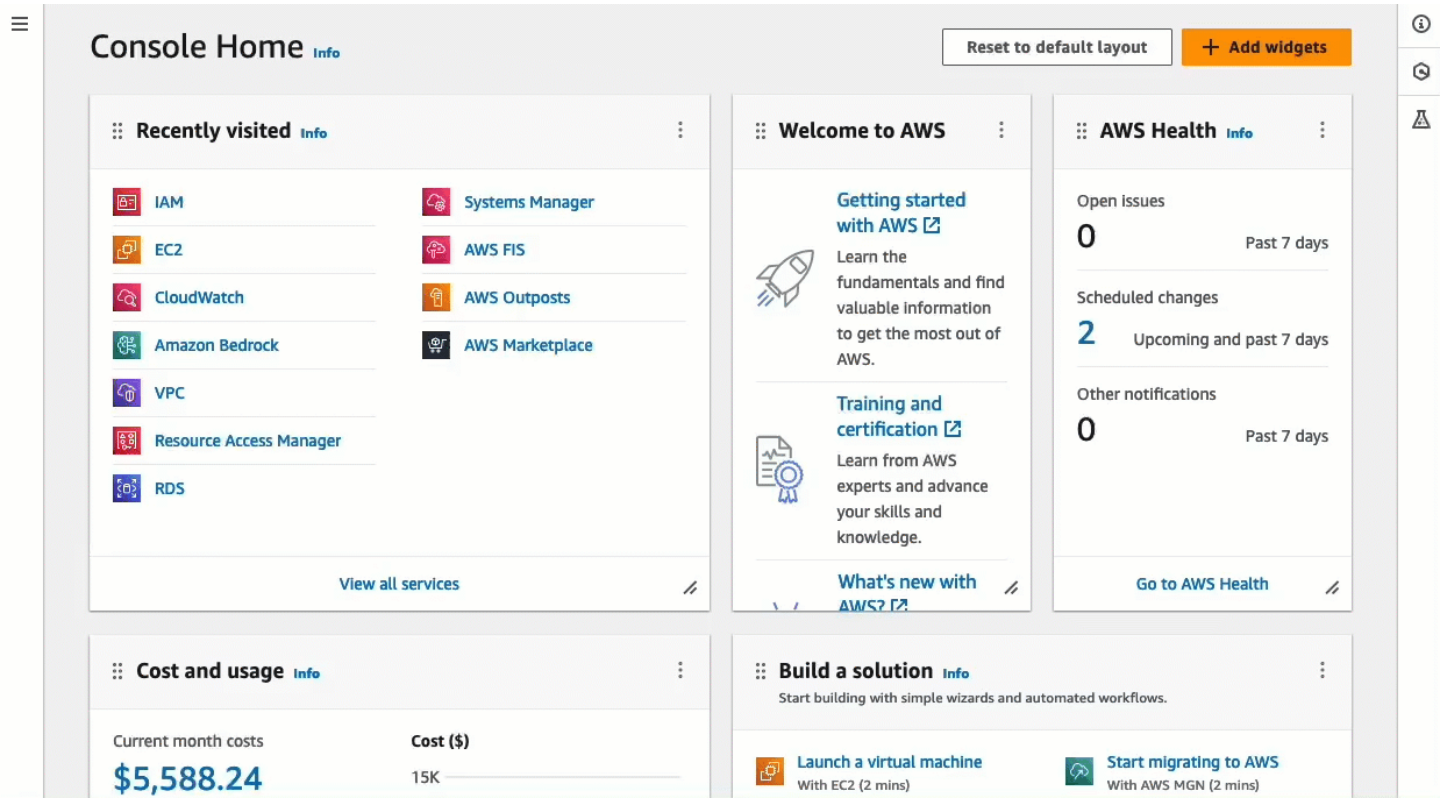
   d. Aktivieren Sie unter IAM-Entitäten das Kontrollkästchen neben Ihrer Identität (Benutzer, Benutzergruppe oder Rolle). Sie können über das Suchfeld die Liste der Entitäten filtern.

   e. Wählen Sie Richtlinie anfügen aus.

Animation anzeigen: Erstellen einer IAM-Richtlinie



Animation anzeigen: Anhängen einer IAM-Richtlinie



Aufgabe 2: Zulassen von eingehendem Traffic vom EC2 Instance Connect-Dienst zu Ihrer Instance

Wenn Sie EC2 Instance Connect in der EC2 Amazon-Konsole verwenden, um eine Connect zu einer Instance herzustellen, ist der Datenverkehr, der die Instance erreichen darf, Datenverkehr vom EC2 Instance Connect-Service. Dies unterscheidet sich von der Verbindung von Ihrem lokalen Computer zu einer Instance. In diesem Fall müssen Sie den Datenverkehr von Ihrem lokalen Computer zu Ihrer Instance zulassen. Um Datenverkehr vom EC2 Instance Connect-Dienst zuzulassen, müssen Sie eine Sicherheitsgruppe erstellen, die eingehenden SSH-Verkehr aus dem IP-Adressbereich für den EC2 Instance Connect-Dienst zulässt.

AWS verwendet Präfixlisten zur Verwaltung von IP-Adressbereichen. Die Namen der EC2 Instance Connect-Präfixlisten lauten wie folgt und *`region`* werden durch den Regionalcode ersetzt:

- IPv4 Name der Präfixliste: `com.amazonaws.`*`region`*`.ec2-instance-connect`
- IPv6 Name der Präfixliste: `com.amazonaws.`*`region`*`.ipv6.ec2-instance-connect`

Aufgabenziel

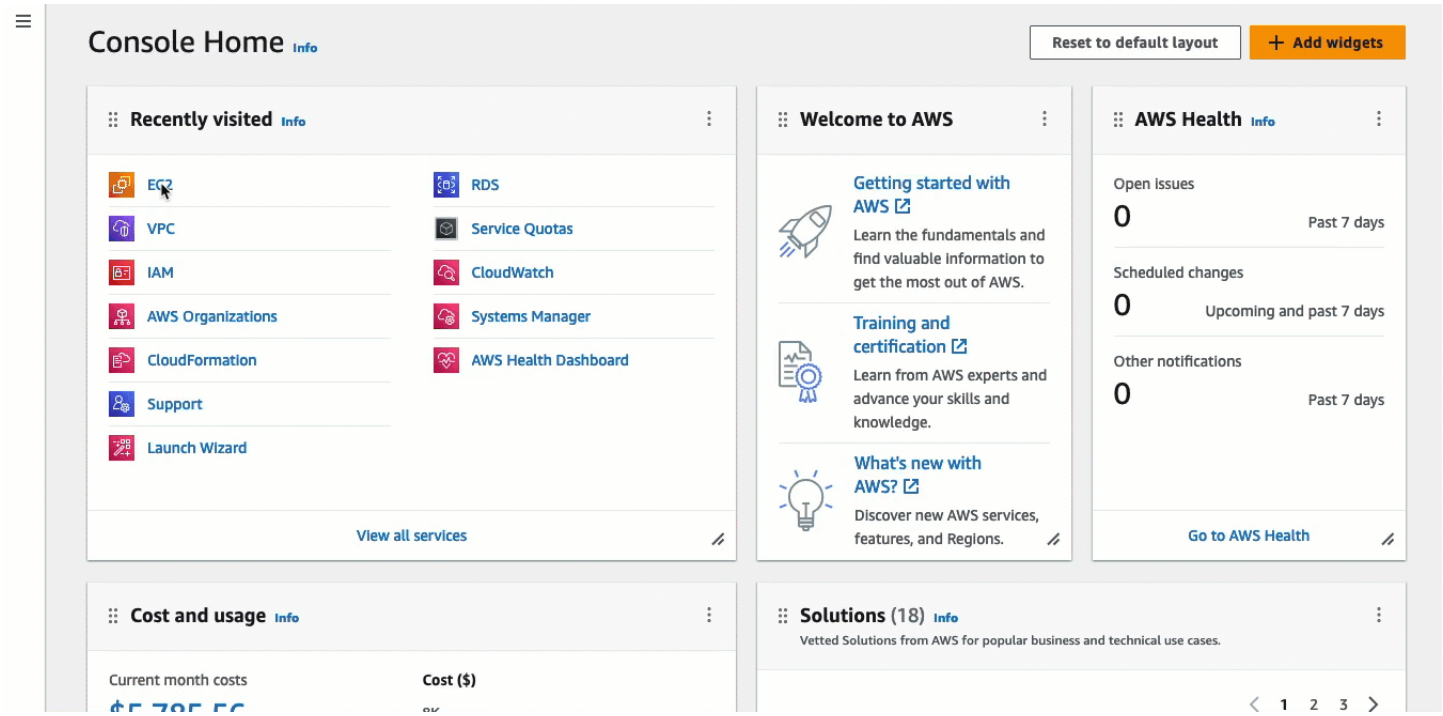
Sie erstellen eine Sicherheitsgruppe, die eingehenden SSH-Verkehr auf Port 22 aus der IPv4 Präfixliste in der Region zulässt, in der sich Ihre Instance befindet.

Um eine Sicherheitsgruppe zu erstellen, die eingehenden Datenverkehr vom EC2 Instance Connect-Dienst zu Ihrer Instance zulässt

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus.
4. Gehen Sie unter Basic details (Grundlegende Angaben) wie folgt vor:
   a. Geben Sie für Sicherheitsgruppenname einen Namen für Ihre Sicherheitsgruppe ein.
   b. Geben Sie in das Feld Beschreibung eine sinnvolle Beschreibung für Ihre Sicherheitsgruppe ein.
5. Führen Sie unter Regeln für eingehenden Datenverkehr die folgenden Schritte aus:
   a. Wählen Sie Regel hinzufügen aus.
   b. Wählen Sie unter Typ die Option SSH aus.
   c. Belassen Sie für Quelle die Option Benutzerdefiniert.
   d. Wählen Sie im Feld neben Quelle die Präfixliste für EC2 Instance Connect aus.

      Wenn sich Ihre Instance beispielsweise in der Region USA Ost (Nord-Virginia) (`us-east-1`) befindet und Ihre Benutzer eine Verbindung zu ihrer öffentlichen IPv4 Adresse herstellen, wählen Sie die folgende Präfixliste aus: com.amazonaws.us-east-1.ec2-instance-connect
6. Wählen Sie Sicherheitsgruppe erstellen aus.

Animation anzeigen: Erstellen der Sicherheitsgruppe



Aufgabe 3: Ihre Instance starten

Beim Starten einer Instance müssen Sie ein AMI angeben, das die zum Starten der Instance erforderlichen Informationen enthält. Sie können wählen, ob Sie eine Instance mit oder ohne vorinstalliertes EC2 Instance Connect starten möchten. In dieser Aufgabe geben wir ein AMI an, das mit EC2 Instance Connect vorinstalliert ist.

Wenn Sie Ihre Instance ohne vorinstallierte EC2 Instance Connect starten und EC2 Instance Connect verwenden möchten, um eine Verbindung zu Ihrer Instance herzustellen, müssen Sie zusätzliche Konfigurationsschritte durchführen. Diese Schritte werden in dieser Anleitung allerdings nicht behandelt.

Aufgabenziel

Sie starten eine Instance mit dem Amazon Linux 2023 AMI, auf dem EC2 Instance Connect vorinstalliert ist. Sie geben auch die Sicherheitsgruppe an, die Sie zuvor erstellt haben, sodass Sie EC2 Instance Connect in der EC2 Amazon-Konsole verwenden können, um eine Verbindung zu Ihrer Instance herzustellen. Da Sie EC2 Instance Connect verwenden, um eine Verbindung zu Ihrer Instance herzustellen, wodurch ein öffentlicher Schlüssel auf die Metadaten Ihrer Instance übertragen wird, müssen Sie beim Starten Ihrer Instance keinen SSH-Schlüssel angeben.

Um eine Instance zu starten, die EC2 Instance Connect in der EC2 Amazon-Konsole für die Verbindung verwenden kann

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. In der Navigationsleiste oben auf dem Bildschirm wird die aktuelle AWS Region angezeigt (z. B. Irland). Wählen Sie eine Region aus, in der die Instance gestartet werden soll. Diese Auswahl ist wichtig, da Sie eine Sicherheitsgruppe erstellt haben, die Traffic für eine bestimmte Region zulässt. Sie müssen also dieselbe Region auswählen, in der Ihre Instance gestartet werden soll.
3. Wählen Sie im Dashboard der EC2 Amazon-Konsole die Option Launch instance aus.
4. (Optional) Geben Sie unter Name und Tags für Name einen beschreibenden Namen für Ihre Instance ein.
5. Wählen Sie unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image) die Option Schnellstart aus. Amazon Linux ist standardmäßig ausgewählt. Unter Amazon Machine Image (AMI) ist standardmässig Amazon-Linux-2023-AMI ausgewählt. Behalten Sie die Standardauswahl für diese Aufgabe bei.
6. Wählen Sie unter Instance-Typ einen Instance-Typ aus oder behalten Sie die Standardeinstellung bei oder wählen Sie einen anderen Instance-Typ aus.
7. Wählen Sie unter Schlüsselpaar (Anmeldung) für Name des Schlüsselpaars die Option Ohne Schlüsselpaar fortfahren (nicht empfohlen) aus. Wenn Sie EC2 Instance Connect verwenden, um eine Verbindung zu einer EC2 Instance herzustellen, überträgt Instance Connect ein key pair an die Metadaten der Instanz, und dieses key pair wird für die Verbindung verwendet.
8. Führen Sie unter Network settings (Netzwerkeinstellungen) die folgenden Schritte aus:

   a. Lassen Sie für Öffentliche IP-Adresse automatisch zuweisen die Option Aktivieren ausgewählt.

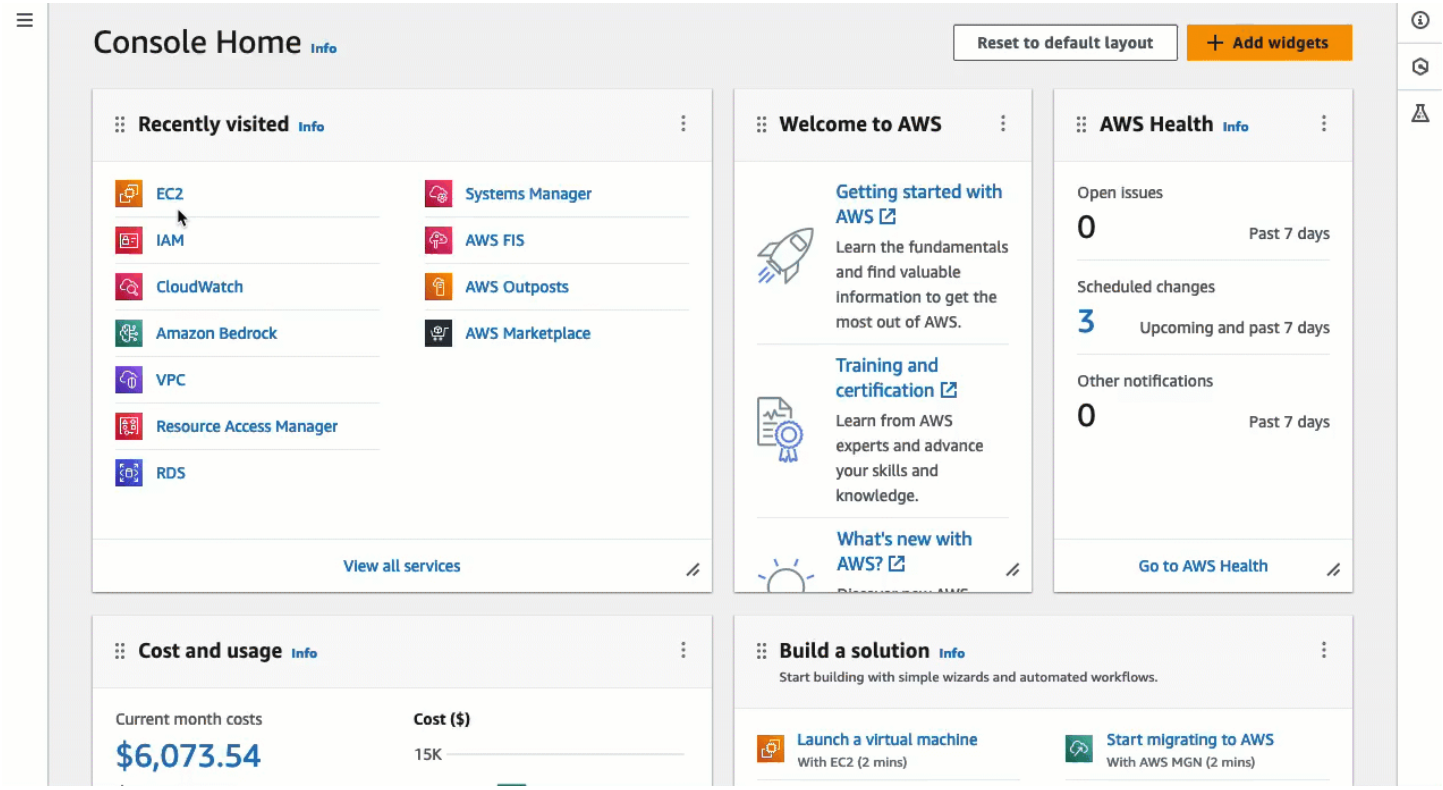
   > **Note**
   >
   > Um EC2 Instance Connect in der EC2 Amazon-Konsole zu verwenden, um eine Verbindung zu einer Instance herzustellen, muss die Instance eine öffentliche IPv6 Adresse IPv4 oder Adresse haben.

   b. Für Firewall (Sicherheitsgruppen) wählen Sie Eine vorhandene Sicherheitsgruppe auswählen aus.

   c. Wählen Sie unter Allgemeine Sicherheitsgruppen die Sicherheitsgruppe aus, die Sie zuvor erstellt haben.

9. Wählen Sie in der Übersicht Launch instance (Instance starten) aus.

Animation anzeigen: Starten Ihrer Instance



Aufgabe 4: Verbindung mit Ihrer Instance herstellen

Wenn Sie über Instance Connect eine Verbindung zu einer EC2 Instance Connect, überträgt die EC2 Instance Connect-API einen öffentlichen SSH-Schlüssel an die Instance-Metadaten, wo er 60 Sekunden lang verbleibt. Der SSH-Daemon verwendet `AuthorizedKeysCommand` und `AuthorizedKeysCommandUser`, um zur Authentifizierung den öffentlichen Schlüssel in der Instance-Metadaten zu suchen, und verbindet Sie mit der Instance.

Aufgabenziel

In dieser Aufgabe stellen Sie mithilfe von Instance Connect in der EC2 Amazon-Konsole eine Verbindung zu Ihrer EC2 Instance her. Wenn Sie die erforderlichen Aufgaben 1, 2 und 3 abgeschlossen haben, sollte die Verbindung erfolgreich sein.

Schritte zum Herstellen einer Verbindung mit Ihrer Instance

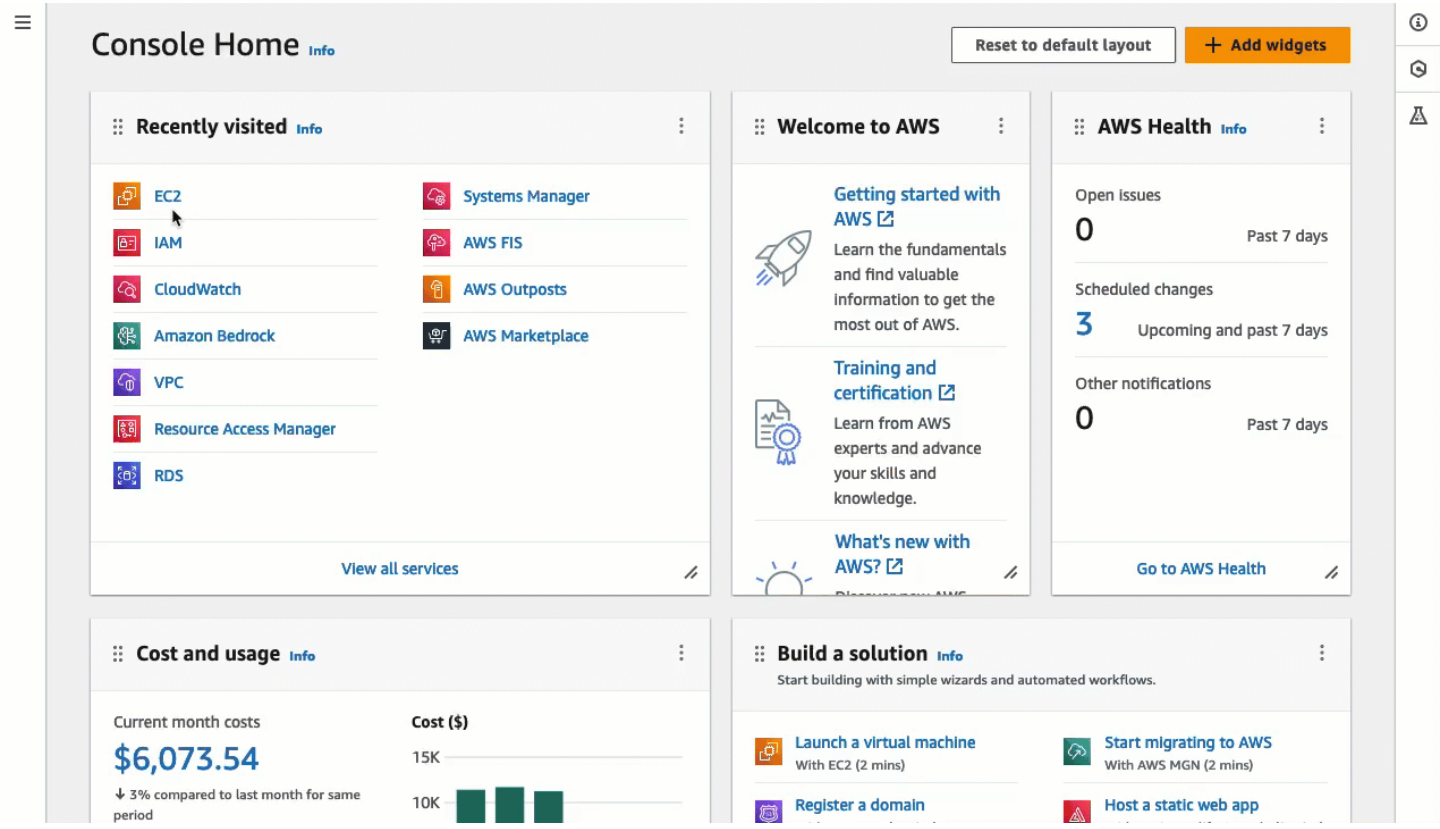
Führen Sie die folgenden Schritte aus, um sich mit Ihrer Instance zu verbinden. Eine Animation dieser Schritte finden Sie unter Animation anzeigen: Verbinden zu Ihrer Instance.

So verbinden Sie eine Instance mithilfe von EC2 Instance Connect in der EC2 Amazon-Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. In der Navigationsleiste oben auf dem Bildschirm wird die aktuelle AWS Region angezeigt (z. B. Irland). Wählen Sie die Region, in der sich Ihre Instance befindet.
3. Wählen Sie im Navigationsbereich Instances aus.
4. Wählen Sie Ihre Instance aus und anschließend Connect.
5. Wählen Sie den Tab EC2 Instance Connect.
6. Wählen Sie Mit einer öffentlichen IP verbinden aus.
7. Wählen Sie Connect aus.

   Ein neues Terminal-Fenster wird geöffnet, und Sie sind mit Ihrer Instance verbunden.

Animation anzeigen: Verbinden zu Ihrer Instance



Voraussetzungen für EC2 Instance Connect

Im Folgenden sind die Voraussetzungen für die Installation und Verwendung von EC2 Instance Connect aufgeführt:

- Installieren Sie EC2 Instance Connect
- Lokale Netzwerkkonnektivität sicherstellen
- Eingehenden SSH-Verkehr zulassen
- Erteilen Sie Berechtigungen
- Einen SSH-Client auf Ihrem lokalen Computer installieren
- Erfüllung der Anforderungen für den Benutzernamen

Installieren Sie EC2 Instance Connect

Um EC2 Instance Connect für die Verbindung mit einer Instance zu verwenden, muss auf der Instance EC2 Instance Connect installiert sein. Sie können die Instance entweder mit einem AMI starten, das mit EC2 Instance Connect vorinstalliert ist, oder Sie können EC2 Instance Connect auf Instances installieren, die mit Support AMIs gestartet wurden. Weitere Informationen finden Sie unter EC2 Installiere Instance Connect auf deinen EC2 Instances.

Lokale Netzwerkkonnektivität sicherstellen

Instances können so konfiguriert werden, dass Benutzer über das Internet oder über die private IP-Adresse der Instance eine Verbindung zu Ihrer Instance herstellen können. Je nachdem, wie Ihre Benutzer mithilfe von Instance Connect eine Verbindung zu Ihrer EC2 Instance herstellen, müssen Sie den folgenden Netzwerkzugriff konfigurieren:

- Wenn Ihre Benutzer über das Internet eine Verbindung zu Ihrer Instance herstellen, muss Ihre Instance eine öffentliche IPv4 IPv6 Adresse haben und sich in einem öffentlichen Subnetz mit einer Route zum Internet befinden. Wenn Sie Ihr öffentliches Standardsubnetz nicht geändert haben, enthält es IPv4 nur eine Route zum Internet für und nicht für. IPv6 Weitere Informationen finden Sie unter Aktivieren des VPC-Internetzugangs über Internet-Gateways im Benutzerhandbuch für Amazon-VPC.
- Wenn Ihre Benutzer über die private IPv4 Adresse der Instance eine Verbindung zu Ihrer Instance herstellen, müssen Sie eine private Netzwerkkonnektivität zu Ihrer VPC einrichten, z. B. mithilfe von AWS Direct Connect AWS Site-to-Site VPN, oder VPC-Peering, damit Ihre Benutzer die private IP-Adresse der Instance erreichen können.

Wenn Ihre Instance keine öffentliche IPv6 Adresse IPv4 oder Adresse hat und Sie es vorziehen, den Netzwerkzugriff nicht wie oben beschrieben zu konfigurieren, können Sie EC2 Instance Connect Endpoint als Alternative zu EC2 Instance Connect in Betracht ziehen. Mit EC2 Instance Connect

Endpoint können Sie über SSH oder RDP eine Verbindung zu einer Instance herstellen, auch wenn die Instance keine öffentliche Adresse IPv4 oder IPv6 Adresse hat. Weitere Informationen finden Sie unter Stellen Sie über die EC2 Amazon-Konsole eine Verbindung zu Ihrer Linux-Instance her.

Eingehenden SSH-Verkehr zulassen

Wenn Sie die EC2 Amazon-Konsole verwenden, um eine Verbindung zu einer Instance herzustellen

Wenn Benutzer über die EC2 Amazon-Konsole eine Connect zu einer Instance herstellen, ist der Datenverkehr, der die Instance erreichen darf, Datenverkehr vom EC2 Instance Connect-Service. Der Service wird anhand bestimmter IP-Adressbereiche identifiziert, die über Präfixlisten AWS verwaltet werden. Sie müssen eine Sicherheitsgruppe erstellen, die eingehenden SSH-Verkehr vom EC2 Instance Connect-Dienst zulässt. Um dies zu konfigurieren, wählen Sie für die eingehende Regel im Feld neben Quelle die EC2 Instance Connect-Präfixliste aus.

AWS bietet unterschiedliche verwaltete Präfixlisten IPv4 und IPv6 Adressen für jede Region. Die Namen der EC2 Instance Connect-Präfixlisten lauten wie folgt und *region* werden durch den Regionalcode ersetzt:

- IPv4 Name der Präfixliste: `com.amazonaws.region.ec2-instance-connect`
- IPv6 Name der Präfixliste: `com.amazonaws.region.ipv6.ec2-instance-connect`

Anweisungen für das Erstellen einer Sicherheitsgruppe finden Sie unter Aufgabe 2: Zulassen von eingehendem Traffic vom EC2 Instance Connect-Dienst zu Ihrer Instance. Weitere Informationen finden Sie unter Verfügbare AWS verwaltete Präfixlisten im Amazon VPC-Benutzerhandbuch.

Wenn Sie über die CLI oder SSH Verbindungen mit einer Instance herstellen

Stellen Sie sicher, dass die Ihrer Instance zugeordnete Sicherheitsgruppe eingehenden SSH-Verkehr auf Port 22 von Ihrer IP-Adresse oder Ihres Netzwerks aus zulässt. Die standardmäßige Sicherheitsgruppe für die VPC lässt keinen eingehenden SSH-Datenverkehr zu. Die über den Launch Instance Wizard erstellte Sicherheitsgruppe lässt eingehenden SSH-Datenverkehr standardmäßig zu. Weitere Informationen finden Sie unter Regeln für die Verbindung mit Instances von Ihrem Computer aus.

Erteilen Sie Berechtigungen

Sie müssen jedem IAM-Benutzer, der EC2 Instance Connect verwendet, um eine Verbindung zu einer Instance herzustellen, die erforderlichen Berechtigungen gewähren. Weitere Informationen finden Sie unter Erteilen Sie IAM-Berechtigungen für EC2 Instance Connect.

Einen SSH-Client auf Ihrem lokalen Computer installieren

Wenn Ihre Benutzer eine Verbindung über SSH herstellen, müssen sie sicherstellen, dass ihr lokaler Computer über einen SSH-Client verfügt.

Auf Ihrem lokalen Computer ist höchstwahrscheinlich standardmäßig ein SSH-Client installiert. Sie können nach einem SSH-Client suchen, indem Sie in der Befehlszeile ssh eingeben. Wenn ihr lokaler Computer den Befehl nicht erkennt, können sie einen SSH-Client installieren. Weitere Informationen zum Installieren eines SSH-Client unter Linux oder macOS X finden Sie unter http://www.openssh.com. Weitere Informationen zur Installation eines SSH-Clients unter Windows 10 finden Sie unter OpenSSH unter Windows.

Es ist nicht erforderlich, einen SSH-Client auf einem lokalen Computer zu installieren, wenn Ihre Benutzer nur die EC2 Amazon-Konsole verwenden, um eine Verbindung zu einer Instance herzustellen.

Erfüllung der Anforderungen für den Benutzernamen

Wenn Sie EC2 Instance Connect verwenden, um eine Verbindung zu einer Instance herzustellen, muss der Benutzername die folgenden Anforderungen erfüllen:

- Erstes Zeichen: Muss ein Buchstabe (`A-Z`, `a-z`), eine Ziffer (`0-9`) oder ein Unterstrich (`_`) sein
- Nachfolgende Zeichen: Dabei kann es sich um Buchstaben (`A-Z`, `a-z`), Ziffern (`0-9`) oder die folgenden Zeichen handeln: `@ . _ -`
- Mindestlänge: 1 Zeichen.
- Maximale Länge: 31 Zeichen.

Erteilen Sie IAM-Berechtigungen für EC2 Instance Connect

Um mithilfe von Instance Connect eine Verbindung zu einer EC2 Instance herzustellen, müssen Sie eine IAM-Richtlinie erstellen, die Ihren Benutzern Berechtigungen für die folgenden Aktionen und Bedingungen gewährt:

- `ec2-instance-connect:SendSSHPublicKey`-Aktion – Erteilt einem -Benutzer die Berechtigung, den öffentlichen Schlüssel per Push zu einer Instance zu übertragen.
- `ec2:osuser`-Bedingung – Gibt den Namen des Betriebssystembenutzers an, der den öffentlichen Schlüssel per Push an die Instance übertragen kann. Verwenden Sie den Standardbenutzernamen der AMI, den Sie beim Starten der Instance verwendet haben. Der Standardbenutzername für AL2 023 und Amazon Linux 2 ist`ec2-user`, und für Ubuntu ist es`ubuntu`.

- `ec2:DescribeInstances`action — Erforderlich, wenn die EC2 Konsole verwendet wird, da der Wrapper diese Aktion aufruft. Benutzer besitzen möglicherweise bereits die Berechtigung zum Aufruf dieser Aktion in einer anderen Richtlinie.
- `ec2:DescribeVpcs`Aktion — Erforderlich, wenn eine Verbindung zu einer IPv6 Adresse hergestellt wird.

Erwägen Sie, den Zugriff auf bestimmte EC2 Instanzen einzuschränken. Andernfalls können alle IAM-Prinzipale mit der Berechtigung für die `ec2-instance-connect:SendSSHPublicKey` Aktion eine Verbindung zu allen Instanzen herstellen. EC2 Sie können den Zugriff einschränken, indem Sie eine Ressource angeben ARNs oder Ressourcen-Tags als Bedingungsschlüssel verwenden.

Weitere Informationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2 Instance Connect.

Informationen zum Erstellen und Bearbeiten von IAM-Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Erlauben Sie Benutzern die Verbindung zu bestimmten Instances

Die folgende IAM-Richtlinie gewährt die Erlaubnis, eine Verbindung zu bestimmten Instances herzustellen, die anhand ihrer Ressource ARNs identifiziert werden.

In der folgenden Beispiel-IAM-Richtlinie werden die folgenden Aktionen und Bedingungen angegeben:

- Die `ec2-instance-connect:SendSSHPublicKey` Aktion gewährt Benutzern die Erlaubnis, eine Verbindung zu zwei Instances herzustellen, die von der Ressource ARNs angegeben werden. Um Benutzern die Berechtigung zu erteilen, eine Verbindung zu allen EC2 Instanzen herzustellen, ersetzen Sie die Ressource ARNs durch den * Platzhalter.
- Die `ec2:osuser` Bedingung gewährt nur dann die Erlaubnis, eine Verbindung zu den Instanzen herzustellen, wenn die *`ami-username`* beim Herstellen der Verbindung angegeben wurde.
- Die Aktion `ec2:DescribeInstances` wird angegeben, um Benutzern, die sich über die Konsole mit Ihren Instances verbinden wollen, eine Berechtigung zu erteilen. Sie können `ec2:DescribeInstances` auslassen, wenn Ihre Benutzer ausschließlich einen SSH-Client zum Herstellen von Verbindungen mit Ihren Instances verwenden. Beachten Sie, dass die `ec2:Describe*`-API-Aktionen keine Berechtigungen auf Ressourcenebene unterstützen. Aus diesem Grund ist in der obigen Anweisung der *-Platzhalter im `Resource`-Element erforderlich.

- Die `ec2:DescribeVpcs` Aktion ist so spezifiziert, dass Benutzern, die die Konsole verwenden, um über eine IPv6 Adresse eine Verbindung zu Ihren Instances herzustellen, die Erlaubnis erteilt wird. Wenn Ihre Benutzer nur eine öffentliche IPv4 Adresse verwenden, können Sie sie weglassen`ec2:DescribeVpcs`. Beachten Sie, dass die `ec2:Describe`*-API-Aktionen keine Berechtigungen auf Ressourcenebene unterstützen. Aus diesem Grund ist in der obigen Anweisung der *-Platzhalter im `Resource`-Element erforderlich.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": [
                "arn:aws:ec2:us-
east-1:111122223333:instance/i-1234567890abcdef0",
                "arn:aws:ec2:us-east-1:111122223333:instance/i-0598c7d356eba48d7"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        }
    ]
}
```

Erlauben Sie Benutzern die Verbindung zu Instances mit bestimmten Tags

Die attributebasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen auf der Grundlage von Tags definiert werden, die Benutzern und Ressourcen zugewiesen werden

können. AWS Sie können Ressourcen-Tags verwenden, um den Zugriff auf eine Instance zu steuern. Weitere Informationen zur Verwendung von Tags zur Steuerung des Zugriffs auf Ihre AWS Ressourcen finden Sie unter Steuern des Zugriffs auf AWS Ressourcen im IAM-Benutzerhandbuch.

In der folgenden Beispiel-IAM-Richtlinie gewährt die `ec2-instance-connect:SendSSHPublicKey`-Aktion Benutzern die Berechtigung, eine Verbindung zu einer beliebigen Instance herzustellen (gekennzeichnet durch den *-Platzhalter im Ressourcen-ARN), sofern die Instance über ein Ressourcen-Tag mit key=`tag-key` und value=`tag-value` verfügt.

Die Aktion `ec2:DescribeInstances` wird angegeben, um Benutzern, die sich über die Konsole mit Ihren Instances verbinden wollen, eine Berechtigung zu erteilen. Sie können `ec2:DescribeInstances` auslassen, wenn Ihre Benutzer ausschließlich einen SSH-Client zum Herstellen von Verbindungen mit Ihren Instances verwenden. Beachten Sie, dass die `ec2:Describe*`-API-Aktionen keine Berechtigungen auf Ressourcenebene unterstützen. Aus diesem Grund ist in der obigen Anweisung der *-Platzhalter im `Resource`-Element erforderlich.

Die `ec2:DescribeVpcs` Aktion ist so spezifiziert, dass Benutzern, die die Konsole verwenden, die Erlaubnis erteilt wird, über eine IPv6 Adresse eine Verbindung zu Ihren Instances herzustellen. Wenn Ihre Benutzer nur eine öffentliche IPv4 Adresse verwenden, können Sie sie weglassen`ec2:DescribeVpcs`. Beachten Sie, dass die `ec2:Describe*`-API-Aktionen keine Berechtigungen auf Ressourcenebene unterstützen. Aus diesem Grund ist in der obigen Anweisung der *-Platzhalter im `Resource`-Element erforderlich.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/tag-key": "tag-value"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        }
    ]
}
```

EC2 Installiere Instance Connect auf deinen EC2 Instances

Um mit Instance Connect eine Verbindung zu einer EC2 Linux-Instance herzustellen, muss auf der Instance EC2 Instance Connect installiert sein. Durch die Installation von EC2 Instance Connect wird der SSH-Daemon auf der Instanz konfiguriert.

Weitere Informationen zum EC2 Instance Connect-Paket finden Sie unter aws/aws-ec2 - auf der Website. instance-connect-config GitHub

> **Note**
>
> Wenn Sie die `AuthorizedKeysCommandUser` Einstellungen `AuthorizedKeysCommand` und für die SSH-Authentifizierung konfiguriert haben, werden sie bei der EC2 Instance Connect-Installation nicht aktualisiert. Daher können Sie EC2 Instance Connect nicht verwenden.

Voraussetzungen für die Installation

Stellen Sie vor der Installation von EC2 Instance Connect sicher, dass Sie die folgenden Voraussetzungen erfüllen.

- Stellen Sie sicher, dass die Instance eine der folgenden Optionen verwendet:
  - Amazon Linux 2 vor Version 2.0.20190618 *
  - AL2023 minimales AMI oder Amazon ECS-optimiertes AMI
  - CentOS Stream 8 und 9
  - macOS Sonoma vor 14.2.1, Ventura vor 13.6.3 und Monterey vor 12.7.2 *
  - Red Hat Enterprise Linux (RHEL) 8 und 9
  - Ubuntu 16.04 und 18.04 *

> **Tip**
>
> * Für Amazon Linux 2, macOS und Ubuntu: Wenn Sie Ihre Instance mit einer neueren Version als den oben aufgeführten gestartet haben, ist EC2 Instance Connect vorinstalliert und es ist keine manuelle Installation erforderlich.

- Überprüfen Sie die allgemeinen Voraussetzungen für EC2 Instance Connect.

  Weitere Informationen finden Sie unter Voraussetzungen für EC2 Instance Connect.

- Überprüfen Sie die Voraussetzungen für die Verbindung zu Ihrer Instance mithilfe eines SSH-Clients auf Ihrem lokalen Rechner.

  Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance mit SSH.

- Rufen Sie die ID der Instance ab.

  Sie können die ID Ihrer Instance mithilfe der EC2 Amazon-Konsole abrufen (aus der Spalte Instance-ID). Wenn Sie möchten, können Sie den Befehl describe-instances (AWS CLI) oder Get-EC2Instance(AWS Tools for Windows PowerShell) verwenden.

Installieren Sie EC2 Instance Connect manuell

> **Note**
>
> Wenn Sie Ihre Instance mit einer der folgenden Methoden gestartet haben AMIs, ist EC2 Instance Connect vorinstalliert und Sie können dieses Verfahren überspringen:
>
> - AL2023 Standard-AMI
> - Amazon Linux 2 2.0.20190618 oder höher
> - macOS Sonoma 14.2.1 oder höher
> - macOS Ventura 13.6.3 oder neuer
> - macOS Monterey 12.7.2 oder höher
> - Ubuntu 20.04 oder höher

Verwenden Sie je nach Betriebssystem Ihrer EC2 Instance eines der folgenden Verfahren zur Installation von Instance Connect.

Amazon Linux 2

Um EC2 Instance Connect auf einer mit Amazon Linux 2 gestarteten Instance zu installieren

1. Stellen Sie per SSH eine Verbindung zu Ihrer -Instance her.

   Ersetzen Sie die Beispielwerte im folgenden Befehl durch Ihre Werte. Nutzen Sie das SSH-Schlüsselpaar, das beim Start Ihrer Instance dieser zugewiesen wurde, und den Standardbenutzernamen des AMI, mit dem Sie Ihre Instance gestartet haben. Bei Amazon Linux 2 ist der Standardbenutzername `ec2-user`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Verbinden mit der Linux-Instance über einen SSH-Client.

2. Installieren Sie das EC2 Instance Connect-Paket auf Ihrer Instance.

   ```
   [ec2-user ~]$ sudo yum install ec2-instance-connect
   ```

   Im Ordner `/opt/aws/bin/` sollten drei neue Skripts angezeigt werden:

   ```
   eic_curl_authorized_keys
   eic_parse_authorized_keys
   eic_run_authorized_keys
   ```

3. (Optional) Stellen Sie sicher, dass EC2 Instance Connect erfolgreich auf Ihrer Instance installiert wurde.

   ```
   [ec2-user ~]$ sudo less /etc/ssh/sshd_config
   ```

   EC2 Instance Connect wurde erfolgreich installiert, wenn die `AuthorizedKeysCommandUser` Zeilen `AuthorizedKeysCommand` und die folgenden Werte enthalten:

   ```
   AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
   ```

```
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` sorgt dafür, dass das Skript `eic_run_authorized_keys` die Schlüssel aus den Instance-Metadaten liest.
- `AuthorizedKeysCommandUser` legt den Systembenutzer als `ec2-instance-connect` fest.

> **Note**
>
> Wenn Sie `AuthorizedKeysCommand` und zuvor konfiguriert habenAuthorizedKeysCommandUser, ändert die EC2 Instance Connect-Installation die Werte nicht und Sie können EC2 Instance Connect nicht verwenden.

CentOS

Um EC2 Instance Connect auf einer mit CentOS gestarteten Instanz zu installieren

1. Stellen Sie per SSH eine Verbindung zu Ihrer -Instance her.

   Ersetzen Sie die Beispielwerte im folgenden Befehl durch Ihre Werte. Nutzen Sie das SSH-Schlüsselpaar, das beim Start Ihrer Instance dieser zugewiesen wurde, und den Standardbenutzernamen des AMI, mit dem Sie Ihre Instance gestartet haben. Bei CentOS lautet der Standardbenutzername `centos` oder `ec2-user`.

   ```
   $ ssh -i my_ec2_private_key.pem centos@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Verbinden mit der Linux-Instance über einen SSH-Client.

2. Wenn Sie einen HTTP- oder HTTPS-Proxy verwenden, müssen Sie die `http_proxy` oder `https_proxy`-Umgebungsvariablen in der aktuellen Shell-Sitzung einstellen.

   Wenn Sie keinen Proxy verwenden, können Sie diesen Schritt überspringen.

   - Führen Sie für einen HTTP-Proxy-Server die folgenden Befehle aus:

     ```
     $ export http_proxy=http://hostname:port
     ```

```
$ export https_proxy=http://hostname:port
```

- Führen Sie für einen HTTPS-Proxy-Server die folgenden Befehle aus:

```
$ export http_proxy=https://hostname:port
$ export https_proxy=https://hostname:port
```

3. Installieren Sie das EC2 Instance Connect-Paket auf Ihrer Instance, indem Sie die folgenden Befehle ausführen.

   Die EC2 Instance Connect-Konfigurationsdateien für CentOS werden in einem Red Hat Package Manager (RPM) -Paket mit unterschiedlichen RPM-Paketen für CentOS 8 und CentOS 9 sowie Instance-Typen bereitgestellt, die auf Intel/AMD (x86_64) oder ARM () laufen. AArch64

   Verwenden Sie den Befehlsblock für Ihr Betriebssystem und Ihre CPU-Architektur.

   - CentOS 8

     Intel/AMD (x86_64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
     west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-
     connect-2.0.0-5.rhel8.x86_64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
     connect.rpm
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
     selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
     selinux.rpm
     [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
     connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
     ```

     ARM () AArch64

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
     west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-
     connect-2.0.0-5.rhel8.aarch64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
     connect.rpm
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect-
     ```

```
selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

- CentOS 9

  Intel/AMD (x86_64)

  ```
  [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
  west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-
  connect-2.0.0-5.rhel9.x86_64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
  connect.rpm
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
  west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
  selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
  selinux.rpm
  [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
  connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
  ```

  ARM (AArch64)

  ```
  [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
  west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-
  connect-2.0.0-5.rhel9.aarch64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
  connect.rpm
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
  west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect-
  selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
  selinux.rpm
  [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
  connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
  ```

  Sie sollten das folgende neue Skript im Ordner `/opt/aws/bin/` sehen:

  ```
  eic_run_authorized_keys
  ```

4. (Optional) Stellen Sie sicher, dass EC2 Instance Connect erfolgreich auf Ihrer Instance installiert wurde.

- Für CentOS 8:

```
[ec2-user ~]$ sudo less /lib/systemd/system/sshd.service.d/ec2-instance-
connect.conf
```

- Für CentOS 9:

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

EC2 Instance Connect wurde erfolgreich installiert, wenn die `AuthorizedKeysCommandUser` Zeilen `AuthorizedKeysCommand` und die folgenden Werte enthalten:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` sorgt dafür, dass das Skript `eic_run_authorized_keys` die Schlüssel aus den Instance-Metadaten liest.
- `AuthorizedKeysCommandUser` legt den Systembenutzer als `ec2-instance-connect` fest.

> **Note**
>
> Wenn Sie `AuthorizedKeysCommand` und zuvor konfiguriert habenAuthorizedKeysCommandUser, ändert die EC2 Instance Connect-Installation die Werte nicht und Sie können EC2 Instance Connect nicht verwenden.

macOS

Um EC2 Instance Connect auf einer mit macOS gestarteten Instance zu installieren

1. Stellen Sie per SSH eine Verbindung zu Ihrer -Instance her.

   Ersetzen Sie die Beispielwerte im folgenden Befehl durch Ihre Werte. Nutzen Sie das SSH-Schlüsselpaar, das beim Start Ihrer Instance dieser zugewiesen wurde, und den

Standardbenutzernamen des AMI, mit dem Sie Ihre Instance gestartet haben. Für macOS-Instances lautet der Standardbenutzername `ec2-user`.

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Verbinden mit der Linux-Instance über einen SSH-Client.

2. Aktualisieren Sie Homebrew mit dem folgenden Befehl. Das Update wird die Software auflisten, die Homebrew kennt. Das EC2 Instance Connect-Paket wird über Homebrew auf macOS-Instanzen bereitgestellt. Weitere Informationen finden Sie unter Aktualisieren Sie das Betriebssystem und die Software auf Amazon EC2 Mac-Instances.

```
[ec2-user ~]$ brew update
```

3. Installieren Sie das EC2 Instance Connect-Paket auf Ihrer Instance. Dadurch wird die Software installiert und sshd für die Verwendung konfiguriert.

```
[ec2-user ~]$ brew install ec2-instance-connect
```

Sie sollten das folgende neue Skript im Ordner `/opt/aws/bin/` sehen:

```
eic_run_authorized_keys
```

4. (Optional) Stellen Sie sicher, dass EC2 Instance Connect erfolgreich auf Ihrer Instance installiert wurde.

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

EC2 Instance Connect wurde erfolgreich installiert, wenn die `AuthorizedKeysCommandUser` Zeilen `AuthorizedKeysCommand` und die folgenden Werte enthalten:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` sorgt dafür, dass das Skript `eic_run_authorized_keys` die Schlüssel aus den Instance-Metadaten liest.

- `AuthorizedKeysCommandUser` legt den Systembenutzer als `ec2-instance-connect` fest.

> **Note**
>
> Wenn Sie `AuthorizedKeysCommand` und zuvor konfiguriert habenAuthorizedKeysCommandUser, ändert die EC2 Instance Connect-Installation die Werte nicht und Sie können EC2 Instance Connect nicht verwenden.

RHEL

Um EC2 Instance Connect auf einer mit Red Hat Enterprise Linux (RHEL) gestarteten Instance zu installieren

1. Stellen Sie per SSH eine Verbindung zu Ihrer -Instance her.

   Ersetzen Sie die Beispielwerte im folgenden Befehl durch Ihre Werte. Nutzen Sie das SSH-Schlüsselpaar, das beim Start Ihrer Instance dieser zugewiesen wurde, und den Standardbenutzernamen des AMI, mit dem Sie Ihre Instance gestartet haben. Bei RHEL ist der Standardbenutzername `ec2-user` oder `root`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Verbinden mit der Linux-Instance über einen SSH-Client.

2. Wenn Sie einen HTTP- oder HTTPS-Proxy verwenden, müssen Sie die `http_proxy` oder `https_proxy`-Umgebungsvariablen in der aktuellen Shell-Sitzung einstellen.

   Wenn Sie keinen Proxy verwenden, können Sie diesen Schritt überspringen.

   - Führen Sie für einen HTTP-Proxy-Server die folgenden Befehle aus:

     ```
     $ export http_proxy=http://hostname:port
     $ export https_proxy=http://hostname:port
     ```

   - Führen Sie für einen HTTPS-Proxy-Server die folgenden Befehle aus:

```
$ export http_proxy=https://hostname:port
$ export https_proxy=https://hostname:port
```

3. Installieren Sie das EC2 Instance Connect-Paket auf Ihrer Instance, indem Sie die folgenden Befehle ausführen.

   Die EC2 Instance Connect-Konfigurationsdateien für RHEL werden in einem Red Hat Package Manager (RPM) -Paket mit unterschiedlichen RPM-Paketen für RHEL 8 und RHEL 9 sowie Instance-Typen bereitgestellt, die auf Intel/AMD (x86_64) oder ARM () laufen. AArch64

   Verwenden Sie den Befehlsblock für Ihr Betriebssystem und Ihre CPU-Architektur.

   - RHEL 8

     Intel/AMD (x86_64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
     west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-
     connect-2.0.0-5.rhel8.x86_64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
     connect.rpm
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
     selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
     selinux.rpm
     [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
     connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
     ```

     ARM () AArch64

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
     west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-
     connect-2.0.0-5.rhel8.aarch64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
     connect.rpm
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect-
     selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
     selinux.rpm
     ```

```
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

- RHEL 9

  Intel/AMD (x86_64)

  ```
  [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
  west-2.s3.us-west-2.amazonaws.com/latest/linux_amd64/ec2-instance-
  connect-2.0.0-5.rhel9.x86_64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
  connect.rpm
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
  west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
  selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
  selinux.rpm
  [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
  connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
  ```

  ARM (AArch64)

  ```
  [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-
  west-2.s3.us-west-2.amazonaws.com/latest/linux_arm64/ec2-instance-
  connect-2.0.0-5.rhel9.aarch64.rpm -o /tmp/ec2-instance-connect/ec2-instance-
  connect.rpm
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
  west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect-
  selinux-2.0.0-5.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
  selinux.rpm
  [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
  connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
  ```

Sie sollten das folgende neue Skript im Ordner `/opt/aws/bin/` sehen:

```
eic_run_authorized_keys
```

4. (Optional) Stellen Sie sicher, dass EC2 Instance Connect erfolgreich auf Ihrer Instance installiert wurde.

   - Für RHEL 8:

```
[ec2-user ~]$ sudo less /lib/systemd/system/sshd.service.d/ec2-instance-
connect.conf
```

- Für RHEL 9:

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

EC2 Instance Connect wurde erfolgreich installiert, wenn die `AuthorizedKeysCommandUser` Zeilen `AuthorizedKeysCommand` und die folgenden Werte enthalten:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` sorgt dafür, dass das Skript `eic_run_authorized_keys` die Schlüssel aus den Instance-Metadaten liest.
- `AuthorizedKeysCommandUser` legt den Systembenutzer als `ec2-instance-connect` fest.

> **Note**
>
> Wenn Sie `AuthorizedKeysCommand` und zuvor konfiguriert habenAuthorizedKeysCommandUser, ändert die EC2 Instance Connect-Installation die Werte nicht und Sie können EC2 Instance Connect nicht verwenden.

Ubuntu

Um EC2 Instance Connect auf einer Instance zu installieren, die mit Ubuntu 16.04 oder höher gestartet wurde

1. Stellen Sie per SSH eine Verbindung zu Ihrer -Instance her.

   Ersetzen Sie die Beispielwerte im folgenden Befehl durch Ihre Werte. Nutzen Sie das SSH-Schlüsselpaar, das beim Start Ihrer Instance dieser zugewiesen wurde, und den

Standardbenutzernamen des AMI, mit dem Sie Ihre Instance gestartet haben. Für ein Ubuntu-AMI lautet der Benutzername `ubuntu`.

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Verbinden mit der Linux-Instance über einen SSH-Client.

2. (Optional) Stellen Sie sicher, dass Ihre Instance über das neueste Ubuntu-AMI verfügt.

   Führen Sie die folgenden Befehle aus, um alle Pakete auf Ihrer Instance zu aktualisieren.

   ```
   ubuntu:~$ sudo apt-get update
   ```

   ```
   ubuntu:~$ sudo apt-get upgrade
   ```

3. Installieren Sie das EC2 Instance Connect-Paket auf Ihrer Instance.

   ```
   ubuntu:~$ sudo apt-get install ec2-instance-connect
   ```

   Im Ordner `/usr/share/ec2-instance-connect/` sollten drei neue Skripts angezeigt werden:

   ```
   eic_curl_authorized_keys
   eic_parse_authorized_keys
   eic_run_authorized_keys
   ```

4. (Optional) Stellen Sie sicher, dass EC2 Instance Connect erfolgreich auf Ihrer Instance installiert wurde.

   ```
   ubuntu:~$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
   ```

   EC2 Instance Connect wurde erfolgreich installiert, wenn die `AuthorizedKeysCommandUser` Zeilen `AuthorizedKeysCommand` und die folgenden Werte enthalten:

   ```
   AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_keys %
   %u %%f
   ```

```
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` sorgt dafür, dass das Skript `eic_run_authorized_keys` die Schlüssel aus den Instance-Metadaten liest.
- `AuthorizedKeysCommandUser` legt den Systembenutzer als `ec2-instance-connect` fest.

> **Note**
>
> Wenn Sie `AuthorizedKeysCommand` und zuvor konfiguriert habenAuthorizedKeysCommandUser, ändert die EC2 Instance Connect-Installation die Werte nicht und Sie können EC2 Instance Connect nicht verwenden.

Stellen Sie mithilfe von Instance Connect eine Verbindung zu einer EC2 Linux-Instance Connect

In den folgenden Anweisungen wird erklärt, wie Sie mithilfe von EC2 Instance Connect über die EC2 Amazon-Konsole, den AWS CLI oder einen SSH-Client eine Verbindung zu Ihrer Linux-Instance herstellen.

Wenn Sie mithilfe von EC2 Instance Connect über die Konsole oder eine Verbindung zu einer Instance herstellen AWS CLI, überträgt die EC2 Instance Connect-API automatisch einen öffentlichen SSH-Schlüssel an die Instance-Metadaten, wo er 60 Sekunden lang verbleibt. Die IAM-Richtlinie, die an Ihren Benutzer angefügt ist, autorisiert diese Aktion. Wenn Sie es vorziehen, Ihren eigenen SSH-Schlüssel zu verwenden, können Sie einen SSH-Client verwenden und Ihren SSH-Schlüssel mithilfe EC2 von Instance Connect explizit an die Instance übertragen.

Überlegungen

Nachdem Sie mithilfe von Instance Connect eine Verbindung zu einer EC2 Instance hergestellt haben, bleibt die Verbindung bestehen, bis die SSH-Sitzung beendet wird. Die Dauer der Verbindung wird nicht durch die Dauer Ihrer IAM-Anmeldeinformationen bestimmt. Wenn Ihre IAM-Anmeldeinformationen ablaufen, besteht die Verbindung weiterhin. Wenn Sie die EC2 Instance Connect-Konsole verwenden und Ihre IAM-Anmeldeinformationen ablaufen, beenden Sie die Verbindung, indem Sie die Browserseite schließen. Wenn Sie Ihren eigenen SSH-Client und EC2

Instance Connect verwenden, um Ihren Schlüssel zu pushen, können Sie einen SSH-Timeout-Wert festlegen, um die SSH-Sitzung automatisch zu beenden.

Voraussetzungen

Bevor Sie starten, sollten Sie alle Voraussetzungen überprüfen.

Verbindungsoptionen

- Stellen Sie über die EC2 Amazon-Konsole eine Verbindung her
- Connect mit dem her AWS CLI
- Herstellen von Verbindungen über Ihren eigenen Schlüssel und einen SSH-Client
- Fehlerbehebung

Stellen Sie über die EC2 Amazon-Konsole eine Verbindung her

Sie können mit Instance Connect über die EC2 Amazon-Konsole eine Verbindung zu einer EC2 Instance herstellen.

Voraussetzungen

Um eine Verbindung über die EC2 Amazon-Konsole herzustellen, muss die Instance entweder eine öffentliche IPv6 Adresse IPv4 oder eine Adresse haben. Wenn die Instance nur eine private IPv4 Adresse hat, können Sie die AWS CLI ec2-instance-connect verwenden, um eine Verbindung herzustellen.

So stellen Sie über die EC2 Amazon-Konsole eine Verbindung zu Ihrer Instance her

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance und Connect (Verbinden) aus.
4. Wählen Sie den Tab EC2 Instance Connect.
5. Wählen Sie Mit einer öffentlichen IP verbinden aus.
6. Wenn es eine Auswahl gibt, wählen Sie die IP-Adresse aus, mit der Sie eine Verbindung herstellen möchten. Andernfalls wird die IP-Adresse automatisch ausgewählt.
7. Verifizieren Sie für Benutzername den Benutzernamen.
8. Wählen Sie Verbinden, um eine Verbindung herzustellen. Ein Terminalfenster im Browser wird geöffnet.

Connect mit dem her AWS CLI

Sie können den ec2-instance-connect verwenden, um mit einem AWS CLI SSH-Client eine Verbindung zu Ihrer Instance herzustellen. EC2 Instance Connect versucht, eine Verbindung mithilfe einer verfügbaren IP-Adresse in einer vordefinierten Reihenfolge, basierend auf dem angegebenen Verbindungstyp, herzustellen. Wenn eine IP-Adresse nicht verfügbar ist, versucht es automatisch, die nächste in der Reihenfolge zu verwenden.

Verbindungstypen

`auto` (Standard)

EC2 Instance Connect versucht, mithilfe der IP-Adressen der Instanz in der folgenden Reihenfolge und mit dem entsprechenden Verbindungstyp eine Verbindung herzustellen:

1. Öffentlich IPv4: `direct`
2. Privat IPv4: `eice`
3. IPv6: `direct`

`direct`

EC2 Instance Connect versucht, mithilfe der IP-Adressen der Instanz in der folgenden Reihenfolge eine Verbindung herzustellen:

1. Öffentlich IPv4
2. IPv6
3. Privat IPv4 (es wird keine Connect über einen EC2 Instance Connect-Endpunkt hergestellt)

`eice`

EC2 Instance Connect versucht, mithilfe der privaten IPv4 Adresse der Instanz und eines EC2 Instance Connect-Endpunkts eine Verbindung herzustellen.

> **Note**
>
> In der Zukunft könnten wir das Verhalten des `auto`-Verbindungstyps ändern. Um sicherzustellen, dass Ihr gewünschter Verbindungstyp verwendet wird, empfehlen wir, dass Sie den `--connection-type` explizit entweder auf `direct` oder `eice` setzen.

Voraussetzungen

Sie müssen AWS CLI Version 2 verwenden. Weitere Informationen finden Sie unter Die neueste Version der AWS CLI installieren oder aktualisieren.

So stellen Sie unter Verwendung der Instance-ID eine Verbindung mit einer Instance her

Wenn Sie nur die Instance-ID kennen und Instance Connect den für die Verbindung zu Ihrer EC2 Instance zu verwendenden Verbindungstyp bestimmen lassen möchten, verwenden Sie den CLI Befehl ec2-instance-connect ssh mit der Instanz-ID.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example
```

So Connect Sie mithilfe der Instanz-ID und eines Instance Connect-Endpunkts eine Verbindung zu einer EC2 Instance her

Wenn Sie über einen Instance Connect-Endpunkt eine Verbindung zu Ihrer EC2 Instance herstellen möchten, verwenden Sie den vorherigen Befehl und geben Sie auch den `--connection-type` Parameter mit dem `eice` Wert an.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --connection-type eice
```

So stellen Sie mithilfe der Instance-ID und Ihrer eigenen privaten Schlüsseldatei eine Verbindung zu einer Instance her

Wenn Sie Connect Ihrem eigenen privaten Schlüssel über einen EC2 Instance Connect-Endpunkt eine Verbindung zu Ihrer Instance herstellen möchten, geben Sie die Instanz-ID und den Pfad zur privaten Schlüsseldatei an. Nicht *file://* in den Pfad aufnehmen; das folgende Beispiel schlägt fehl:*file:///path/to/key*.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --private-key-file /
path/to/key.pem
```

> **Tip**
>
> Wenn Sie bei der Verwendung dieser Befehle eine Fehlermeldung erhalten, stellen Sie sicher, dass Sie AWS CLI Version 2 verwenden, da der `ssh` Befehl nur in dieser Hauptversion verfügbar ist. Wir empfehlen außerdem, regelmäßig auf die neueste Nebenversion von AWS CLI Version 2 zu aktualisieren, um auf die neuesten Feature zugreifen zu können. Weitere Informationen zu finden Sie unter Über AWS CLI Version 2 im AWS Command Line Interface -Benutzerhandbuch.

Herstellen von Verbindungen über Ihren eigenen Schlüssel und einen SSH-Client

Sie können Ihren eigenen SSH-Schlüssel verwenden und über den SSH-Client Ihrer Wahl eine Connect zu Ihrer Instance herstellen, während Sie die EC2 Instance Connect-API verwenden. Auf diese Weise können Sie von der EC2 Instance Connect-Funktion profitieren, um einen öffentlichen Schlüssel auf die Instance zu übertragen. Diese Verbindungsmethode funktioniert für Instances mit öffentlichen und privaten IP-Adressen.

Voraussetzungen

- Anforderungen für Schlüsselpaare
  - Unterstützte Typen: RSA (OpenSSH und) und SSH2 ED25519
  - Die unterstützten Längen sind 2048 und 4096.
  - Weitere Informationen finden Sie unter Erstellen Sie ein key pair mit einem Drittanbieter-Tool und importieren Sie den öffentlichen Schlüssel zu Amazon EC2.
- Wenn Sie eine Verbindung zu einer Instance herstellen, die nur private IP-Adressen hat, muss der lokale Computer, von dem aus Sie die SSH-Sitzung initiieren, über eine Verbindung EC2 zum Instance Connect-Dienstendpunkt (um Ihren öffentlichen SSH-Schlüssel an die Instanz zu übertragen) sowie über Netzwerkkonnektivität mit der privaten IP-Adresse der Instanz verfügen, um die SSH-Sitzung einzurichten. Der EC2 Instance Connect-Dienstendpunkt ist über das Internet oder über eine Direct Connect öffentliche virtuelle Schnittstelle erreichbar. Um eine Verbindung mit der privaten IP-Adresse der Instance herzustellen, können Sie Dienste wie Direct Connect, AWS Site-to-Site VPN oder VPC-Peering nutzen.

So stellen Sie eine Verbindung zu Ihrer Instance mit einem eigenen Schlüssel und einem beliebigen SSH-Client her

1. (Optional) Generieren neuer privater und öffentlicher SSH-Schlüssel.

   Sie können mit dem folgenden Befehl neue private und öffentliche SSH-Schlüssel, `my_key` und `my_key.pub`, erstellen:

   ```
   ssh-keygen -t rsa -f my_key
   ```

2. Übertragen Ihres öffentlichen SSH-Schlüssels per Push an die Instance.

   Verwenden Sie den send-ssh-public-key-Befehl, um Ihren öffentlichen SSH-Schlüssel an die Instance zu übertragen. Wenn Sie Ihre Instance mit AL2 023 oder Amazon Linux 2 gestartet

haben, lautet der Standardbenutzername für das AMI. `ec2-user` Wenn Sie Ihre Instance mit Ubuntu gestartet haben, lautet der Standardbenutzername für das AMI `ubuntu`.

Im folgenden Beispiel wird der öffentliche Schlüssel per Push an die angegebene Instance in der angegebenen Availability Zone übertragen, um `ec2-user` zu authentifizieren.

```
aws ec2-instance-connect send-ssh-public-key \
    --region us-west-2 \
    --availability-zone us-west-2b \
    --instance-id i-001234a4bf70dec41EXAMPLE \
    --instance-os-user ec2-user \
    --ssh-public-key file://my_key.pub
```

3. Stellen Sie mit Ihrem privaten Schlüssel eine Verbindung zu der Instance her.

   Stellen Sie mit dem Befehl ssh eine Verbindung zu Ihrer Instance mit dem privaten Schlüssel her, ehe der öffentliche Schlüssel aus den Instance-Metadaten entfernt wird. Sie haben dafür 60 Sekunden Zeit. Geben Sie den privaten Schlüssel an, der dem öffentlichen entspricht, den Standardbenutzernamen für das AMI, mit dem Sie Ihre Instance gestartet haben, und den öffentlichen DNS-Namen der Instance (wenn Sie eine Verbindung über ein privates Netzwerk herstellen, geben Sie den privaten DNS-Namen oder die IP-Adresse an). Fügen Sie die `IdentitiesOnly=yes`-Option hinzu, um sicherzustellen, dass nur die Dateien in der SSH-Konfiguration und der angegebene Schlüssel für die Verbindung verwendet werden.

   ```
   ssh -o "IdentitiesOnly=yes" -i my_key ec2-
   user@ec2-198-51-100-1.compute-1.amazonaws.com
   ```

   Im folgenden Beispiel wird `timeout 3600` verwendet, um Ihre SSH-Sitzung nach 1 Stunde zu beenden. Während der Sitzung gestartete Prozesse können auch nach Beendigung der Sitzung auf Ihrer Instance weiter ausgeführt werden.

   ```
   timeout 3600 ssh -o “IdentitiesOnly=yes” -i my_key ec2-
   user@ec2-198-51-100-1.compute-1.amazonaws.com
   ```

Fehlerbehebung

Weitere Informationen zu Problemen, die beim Aufbau einer Verbindung zu Instances auftreten können, finden Sie unter:

- Fehlersuche bei Verbindungsproblemen mit Ihrer Amazon-EC2-Linux-Instance
- Wie behebe ich Probleme beim Herstellen einer Verbindung zu meiner EC2 Instance mithilfe von EC2 Instance Connect?

EC2 Instance Connect deinstallieren

Um EC2 Instance Connect zu deaktivieren, stellen Sie eine Verbindung zu Ihrer Linux-Instance her und deinstallieren Sie das `ec2-instance-connect` Paket, das auf dem Betriebssystem installiert ist. Wenn die `sshd` Konfiguration mit der Konfiguration übereinstimmt, auf die sie bei der Installation von EC2 Instance Connect eingestellt war, wird bei der Deinstallation `ec2-instance-connect` auch die `sshd` Konfiguration entfernt. Wenn Sie die `sshd` Konfiguration nach der Installation von EC2 Instance Connect geändert haben, müssen Sie sie manuell aktualisieren.

Amazon Linux

Sie können EC2 Instance Connect auf AL2 023 und Amazon Linux 2 2.0.20190618 oder höher deinstallieren, wenn EC2 Instance Connect vorkonfiguriert ist.

So deinstallieren Sie EC2 Instance Connect auf einer mit Amazon Linux gestarteten Instance

1. Stellen Sie per SSH eine Verbindung zu Ihrer -Instance her. Geben Sie das SSH-Schlüsselpaar an, das Sie für Ihre Instance verwendet haben, als Sie sie gestartet haben, und den Standardbenutzernamen für das AL2 023- oder Amazon Linux 2-AMI, nämlich. `ec2-user`

   Der folgende ssh-Befehl stellt beispielsweise eine Verbindung mit einer Instance mit dem öffentlichen DNS-Namen `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` her. Hierfür wird das Schlüsselpaar `my_ec2_private_key.pem` verwendet.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

2. Deinstallieren Sie das `ec2-instance-connect`-Paket mit dem yum-Befehl.

   ```
   [ec2-user ~]$ sudo yum remove ec2-instance-connect
   ```

Ubuntu

So deinstallieren Sie EC2 Instance Connect auf einer Instance, die mit einem Ubuntu-AMI gestartet wurde

1. Stellen Sie per SSH eine Verbindung zu Ihrer -Instance her. Geben Sie das SSH-Schlüsselpaar an, das Sie beim Starten Ihrer Instance verwendet haben, und den Standardbenutzernamen für den Ubuntu-AMI. Dieser ist `ubuntu`.

   Der folgende ssh-Befehl stellt beispielsweise eine Verbindung mit einer Instance mit dem öffentlichen DNS-Namen `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` her. Hierfür wird das Schlüsselpaar `my_ec2_private_key.pem` verwendet.

   ```
   $ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

2. Deinstallieren Sie das `ec2-instance-connect`-Paket mit dem apt-get-Befehl.

   ```
   ubuntu:~$ sudo apt-get remove ec2-instance-connect
   ```

Connect Sie über eine private IP-Adresse und einen EC2 Instance Connect-Endpunkt eine Verbindung zu Ihren Instances her

EC2 Mit Instance Connect Endpoint können Sie eine sichere Verbindung zu einer Instanz aus dem Internet herstellen, ohne einen Bastion-Host zu verwenden oder eine direkte Internetverbindung für Ihre Virtual Private Cloud (VPC) zu benötigen.

Vorteile

- Sie können eine Verbindung zu Ihren Instances herstellen, ohne dass die Instances eine öffentliche Adresse IPv4 oder IPv6 Adresse haben müssen. AWS Gebühren für alle öffentlichen IPv4 Adressen, einschließlich öffentlicher IPv4 Adressen, die mit laufenden Instances verknüpft sind, und Elastic IP-Adressen. Weitere Informationen finden Sie auf der Amazon VPC-Preisseite auf der Registerkarte Öffentliche IPv4 Adresse.
- Sie können vom Internet aus eine Verbindung zu Ihren Instances herstellen, ohne dass Ihr VPC über ein Internet-Gateway direkt mit dem Internet verbunden sein muss.

- Sie können den Zugriff auf die Erstellung und Verwendung der EC2 Instance Connect-Endpoints steuern, um mithilfe von IAM-Richtlinien und -Berechtigungen eine Verbindung zu Instances herzustellen.
- Alle Versuche, eine Verbindung zu Ihren Instances herzustellen, sowohl erfolgreiche als auch erfolglose, werden protokolliert. CloudTrail

Preisgestaltung

Für die Nutzung von EC2 Instance Connect-Endpunkten fallen keine zusätzlichen Kosten an. Wenn Sie einen EC2 Instance Connect-Endpunkt verwenden, um eine Verbindung zu einer Instance in einer anderen Availability Zone herzustellen, fallen zusätzliche Gebühren für die Datenübertragung zwischen Availability Zones an.

Inhalt

- Funktionsweise
- Überlegungen
- Erteilen Sie Berechtigungen zur Verwendung von EC2 Instance Connect Endpoint
- Sicherheitsgruppen für EC2 Instance Connect Endpoint
- Einen EC2 Instance Connect-Endpunkt erstellen
- Einen EC2 Instance Connect-Endpunkt ändern
- Löschen Sie einen EC2 Instance Connect-Endpunkt
- Stellen Sie mithilfe von EC2 Instance Connect Endpoint eine Verbindung zu einer EC2 Amazon-Instance Connect
- Über den EC2 Instance Connect-Endpunkt hergestellte Verbindungen protokollieren
- Serviceverknüpfte Rolle für EC2 Instance Connect Endpoint
- Kontingente für den EC2 Instance Connect-Endpunkt

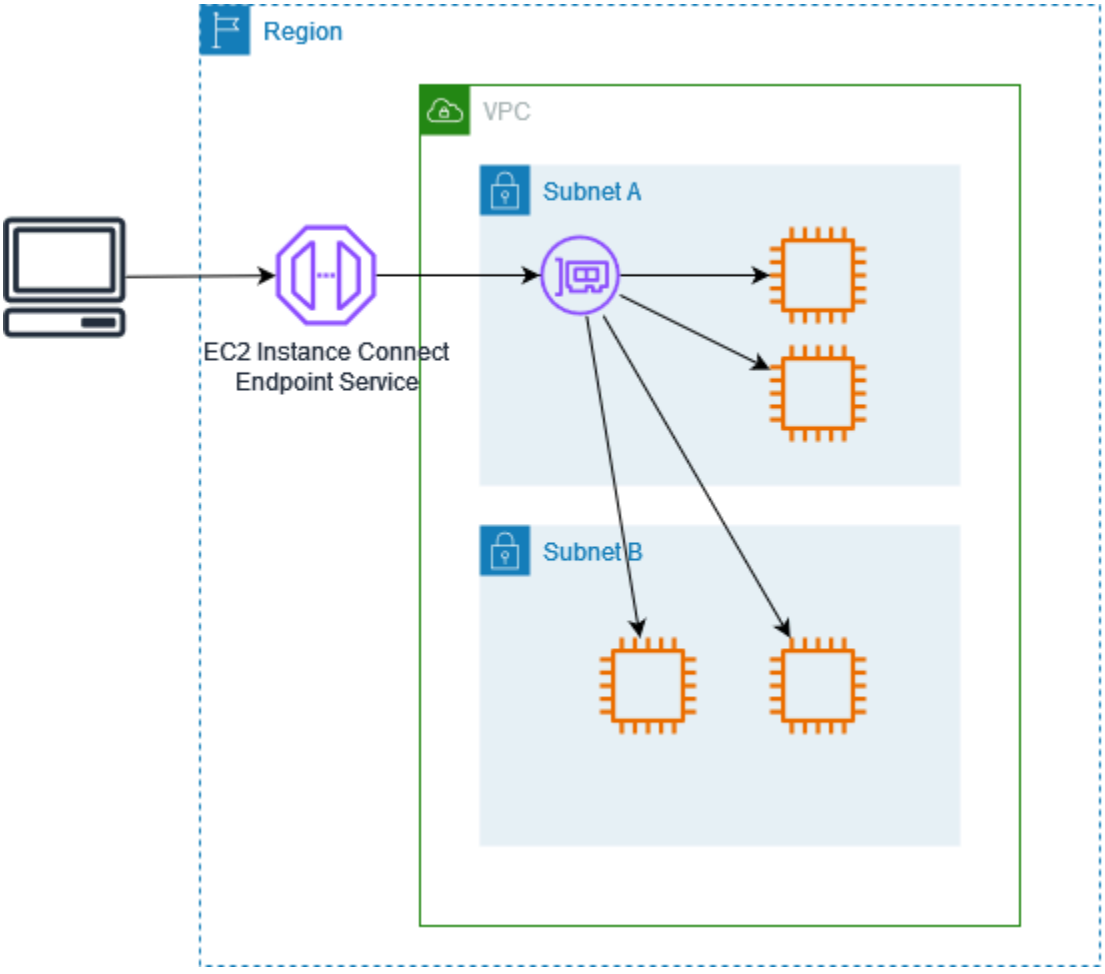
Funktionsweise

EC2 Instance Connect Endpoint ist ein identitätsbewusster TCP-Proxy. Der EC2 Instance Connect Endpoint Service richtet mithilfe der Anmeldeinformationen für Ihre IAM-Entität einen privaten Tunnel von Ihrem Computer zum Endpunkt ein. Der Datenverkehr wird authentifiziert und autorisiert, bevor er Ihre VPC erreicht.

Sie können für Ihre Instances zusätzliche Sicherheitsgruppenregeln konfigurieren, um den eingehenden Datenverkehr einzuschränken. Sie können beispielsweise Regeln für eingehenden Datenverkehr verwenden, um Datenverkehr auf Management-Ports nur vom EC2 Instance Connect-Endpunkt aus zuzulassen.

Sie können Routing-Tabellen-Regeln so konfigurieren, dass der Endpunkt eine Verbindung zu einer beliebigen Instance in einem beliebigen Subnetz der VPC herstellen kann.

Das folgende Diagramm zeigt, wie ein Benutzer über einen Instance Connect-Endpunkt aus dem Internet eine Verbindung zu seinen EC2 Instances herstellen kann. Erstellen Sie zunächst einen EC2 Instance Connect-Endpunkt in Subnetz A. Wir erstellen eine Netzwerkschnittstelle für den Endpunkt im Subnetz, die als Einstiegspunkt für den Datenverkehr dient, der für Ihre Instances in der VPC bestimmt ist. Wenn die Routing-Tabelle für Subnetz B Datenverkehr von Subnetz A zulässt, können Sie den Endpunkt verwenden, um Instances in Subnetz B zu erreichen.



Überlegungen

Bevor Sie beginnen, überlegen Sie folgendes.

- EC2 Instance Connect Endpoint ist speziell für Anwendungsfälle zur Verwaltung des Datenverkehrs vorgesehen, nicht für Datenübertragungen mit hohem Datenvolumen. Datenübertragungen mit hohem Datenvolumen werden gedrosselt.
- Sie können einen EC2 Instance Connect-Endpunkt erstellen, um den Datenverkehr zu einer Instance zu unterstützen, die über eine private IPv4 Adresse oder IPv6 Adresse verfügt. Der IP-Adresstyp des Endpunkts muss mit der IP-Adresse der Instance übereinstimmen. Sie können einen Endpunkt erstellen, der alle IP-Adresstypen unterstützt.
- (Linux-Instances) Wenn Sie Ihr eigenes Schlüsselpaar verwenden, können Sie jedes Linux-AMI verwenden. Andernfalls muss auf Ihrer Instance EC2 Instance Connect installiert sein. Informationen darüber, welche EC2 Instance Connect AMIs enthalten und wie Sie es auf anderen unterstützten Plattformen installieren können AMIs, finden Sie unterInstallieren Sie EC2 Instance Connect.
- Sie können einem EC2 Instance Connect-Endpunkt eine Sicherheitsgruppe zuweisen. Andernfalls werden wir die Standard-Sicherheitsgruppe für die VPC verwenden. Die Sicherheitsgruppe für einen EC2 Instance Connect-Endpunkt muss ausgehenden Datenverkehr zu den Ziel-Instances zulassen. Weitere Informationen finden Sie unter Sicherheitsgruppen für EC2 Instance Connect Endpoint.
- Sie können einen EC2 Instance Connect-Endpunkt so konfigurieren, dass die Quell-IP-Adressen der Clients erhalten bleiben, wenn Anfragen an die Instances weitergeleitet werden. Andernfalls wird die IP-Adresse der Netzwerkschnittstelle zur Client-IP-Adresse für den gesamten eingehenden Datenverkehr.
  - Wenn Sie die Client-IP-Erhaltung aktivieren, müssen die Sicherheitsgruppen für die Instances den Datenverkehr von den Clients zulassen. Außerdem müssen sich die Instances in derselben VPC wie der EC2 Instance Connect-Endpunkt befinden.
  - Wenn Sie die Client-IP-Erhaltung deaktivieren, müssen die Sicherheitsgruppen für die Instances den Datenverkehr von der VPC zulassen. Dies ist die Standardeinstellung.
  - Die Beibehaltung der Client-IP wird nur auf IPv4 EC2 Instance Connect-Endpunkten unterstützt. Um die Client-IP-Erhaltung verwenden zu können, muss der IP-Adresstyp des EC2 Instance Connect-Endpunkts sein IPv4. Die Beibehaltung der Client-IP wird nicht unterstützt, wenn der IP-Adresstyp Dual-Stack oder IPv6 ist.
  - Die folgenden Instance-Typen unterstützen die Aufbewahrung von Client-IP nicht: C1, CG1, CG2, G1, HI1, M1, M2, M3 und T1. Wenn Sie die Client-IP-Erhaltung aktivieren und versuchen, mithilfe von Instance Connect Endpoint eine Verbindung zu einer Instance mit einem dieser EC2 Instance-Typen herzustellen, schlägt die Verbindung fehl.

  - Die Erhaltung der Client-IP wird nicht unterstützt, wenn der Datenverkehr über ein Transit-Gateway geleitet wird.
- Wenn Sie einen EC2 Instance Connect-Endpunkt erstellen, wird automatisch eine serviceverknüpfte Rolle für den EC2 Amazon-Service in AWS Identity and Access Management (IAM) erstellt. Amazon EC2 verwendet die serviceverknüpfte Rolle, um Netzwerkschnittstellen in Ihrem Konto bereitzustellen, die für die Erstellung von EC2 Instance Connect-Endpunkten erforderlich sind. Weitere Informationen finden Sie unter Serviceverknüpfte Rolle für EC2 Instance Connect Endpoint.
- Sie können nur einen EC2 Instance Connect-Endpunkt pro VPC und pro Subnetz erstellen. Weitere Informationen finden Sie unter Kontingente für den EC2 Instance Connect-Endpunkt. Wenn Sie einen weiteren EC2 Instance Connect-Endpoint in einer anderen Availability Zone innerhalb derselben VPC erstellen müssen, müssen Sie zuerst den vorhandenen EC2 Instance Connect-Endpoint löschen. Andernfalls erhalten Sie eine Fehlermeldung.
- Jeder EC2 Instance Connect-Endpunkt kann bis zu 20 gleichzeitige Verbindungen unterstützen.
- Die maximale Dauer für eine hergestellte TCP-Verbindung: 1 Stunde (3 600 Sekunden). Sie können die maximal zulässige Dauer in einer IAM-Richtlinie angeben, die 3 600 Sekunden oder weniger betragen kann. Weitere Informationen finden Sie unter Berechtigungen zur Verwendung von EC2 Instance Connect Endpoint zum Herstellen einer Verbindung zu Instanzen.

  Die Dauer der Verbindung wird nicht durch die Dauer Ihrer IAM-Anmeldeinformationen bestimmt. Wenn Ihre IAM-Anmeldeinformationen ablaufen, bleibt die Verbindung bestehen, bis die angegebene maximale Dauer erreicht ist. Wenn Sie über die Instance Connect Endpoint-Konsole eine Verbindung zu einer EC2 Instance herstellen, legen Sie die maximale Tunneldauer (Sekunden) auf einen Wert fest, der unter der Dauer Ihrer IAM-Anmeldeinformationen liegt. Wenn Ihre IAM-Anmeldeinformationen vorzeitig ablaufen, beenden Sie die Verbindung zu Ihrer Instance, indem Sie die Browserseite schließen.

Erteilen Sie Berechtigungen zur Verwendung von EC2 Instance Connect Endpoint

Standardmäßig sind IAM-Entitäten nicht berechtigt, EC2 Instance Connect-Endpoints zu erstellen, zu beschreiben oder zu ändern. Ein IAM-Administrator kann IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen.

Informationen zum Erstellen und Bearbeiten von IAM-Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Die folgenden Beispielrichtlinien zeigen, wie Sie die Berechtigungen kontrollieren können, die Benutzer für EC2 Instance Connect-Endpoints haben.

Beispiele

- Berechtigungen zum Erstellen, Beschreiben, Ändern und Löschen von EC2 Instance Connect-Endpoints
- Berechtigungen zur Verwendung von EC2 Instance Connect Endpoint zum Herstellen einer Verbindung zu Instanzen
- Herstellen von Verbindungen nur von einem bestimmten IP-Adressbereich berechtigen

Berechtigungen zum Erstellen, Beschreiben, Ändern und Löschen von EC2 Instance Connect-Endpoints

Um einen EC2 Instance Connect-Endpunkt zu erstellen und zu ändern, benötigen Benutzer Berechtigungen für die folgenden Aktionen:

- `ec2:CreateInstanceConnectEndpoint`
- `ec2:CreateNetworkInterface`
- `ec2:CreateTags`
- `ec2:ModifyInstanceConnectEndpoint`
- `iam:CreateServiceLinkedRole`

Um EC2 Instance Connect-Endpoints zu beschreiben und zu löschen, benötigen Benutzer Berechtigungen für die folgenden Aktionen:

- `ec2:DescribeInstanceConnectEndpoints`
- `ec2:DeleteInstanceConnectEndpoint`

Sie können eine Richtlinie erstellen, die die Berechtigung zum Erstellen, Beschreiben, Ändern und Löschen von EC2 Instance Connect-Endpoints in allen Subnetzen erteilt. Alternativ können Sie Aktionen nur für bestimmte Subnetze einschränken, indem Sie das Subnetz ARNs als zulässig angeben `Resource` oder den Bedingungsschlüssel verwenden. `ec2:SubnetID` Sie können den `aws:ResourceTag`-Bedingungsschlüssel auch verwenden, um die Erstellung von Endpunkten mit bestimmten Tags explizit zuzulassen oder zu verweigern. Weitere Informationen finden Sie unter Richtlinien und Berechtigungen in IAM im -IAM-Benutzerhandbuch.

Beispiel für eine IAM-Richtlinie

In der folgenden Beispiel-IAM-Richtlinie erteilt der Abschnitt `Resource` die Berechtigung zum Erstellen, Ändern und Löschen von Endpunkten in allen Subnetzen, die durch das Sternchen (`*`) angegeben sind. `ec2:Describe*`-API-Aktionen unterstützen keine Berechtigungen auf Ressourcenebene. Aus diesem Grund ist in der obigen Anweisung der `*`-Platzhalter im `Resource`-Element erforderlich.

Berechtigungen zur Verwendung von EC2 Instance Connect Endpoint zum Herstellen einer Verbindung zu Instanzen

Die `ec2-instance-connect:OpenTunnel` Aktion gewährt die Erlaubnis, eine TCP-Verbindung zu einer Instanz herzustellen, um eine Connect über den EC2 Instance Connect-Endpunkt herzustellen. Sie können den zu verwendenden EC2 Instance Connect-Endpunkt angeben. Alternativ können Benutzer `Resource` mit einem Sternchen (`*`) jeden verfügbaren EC2 Instance Connect-Endpunkt verwenden. Sie können den Zugriff auf Instances auch einschränken, wenn Ressourcen-Tags als Bedingungsschlüssel vorhanden oder nicht vorhanden sind.

Bedingungen

- `ec2-instance-connect:remotePort` – Gibt den Port auf der Instance an, der für den Aufbau einer TCP-Verbindung verwendet werden kann. Wenn dieser Bedingungsschlüssel verwendet wird, führt der Versuch, eine Verbindung zu einer Instance an einem anderen Port als dem in der Richtlinie angegebenen Port herzustellen, zu einem Fehler.
- `ec2-instance-connect:privateIpAddress` – Gibt die private Ziel-IP-Adresse an, die der Instance zugeordnet ist, mit der Sie eine TCP-Verbindung herstellen möchten. Sie können eine einzelne IP-Adresse angeben, z. B.`10.0.0.1/32`, oder einen IPs Durchgangsbereich CIDRs, z. B. `10.0.1.0/28` Wenn dieser Bedingungsschlüssel verwendet wird, führt der Versuch, eine Verbindung zu einer Instance mit einer anderen privaten IP-Adresse oder außerhalb des CIDR-Bereichs herzustellen, zu einem Fehler.
- `ec2-instance-connect:maxTunnelDuration` – Gibt die maximale Dauer für eine hergestellte TCP-Verbindung an. Die Einheit ist Sekunden und die Dauer reicht von mindestens 1 Sekunde bis maximal 3 600 Sekunden (1 Stunde). Wenn die Bedingung nicht angegeben ist, ist die Standarddauer auf 3 600 Sekunden (1 Stunde) festgelegt. Der Versuch, länger als die in der IAM-Richtlinie angegebene Dauer oder länger als das Standardmaximum eine Verbindung zu einer Instance herzustellen, führt zu einem Fehler. Die Verbindung wird nach Ablauf der angegebenen Dauer getrennt.

Wenn `maxTunnelDuration` in der IAM-Richtlinie angegeben ist und der angegebene Wert weniger als 3 600 Sekunden beträgt (Standard), müssen Sie `--max-tunnel-duration` im Befehl angeben, wenn Sie eine Verbindung zu einer Instance herstellen. Weitere Information über das Verbinden mit einer Instance finden Sie unter Stellen Sie mithilfe von EC2 Instance Connect Endpoint eine Verbindung zu einer EC2 Amazon-Instance Connect.

Sie können einem Benutzer auch Zugriff gewähren, um Verbindungen zu Instanzen herzustellen, die auf dem Vorhandensein von Ressourcen-Tags auf dem EC2 Instance Connect-Endpunkt basieren. Weitere Informationen finden Sie unter Richtlinien und Berechtigungen in IAM im -IAM-Benutzerhandbuch.

Für Linux-Instances gewährt die Aktion `ec2-instance-connect:SendSSHPublicKey` die Erlaubnis, den öffentlichen Schlüssel auf eine Instance zu übertragen. Die `ec2:osuser`-Bedingung gibt den Namen des Betriebssystembenutzers an, der den öffentlichen Schlüssel per Push an die Instance übertragen kann. Verwenden Sie den Standardbenutzernamen der AMI, den Sie beim Starten der Instance verwendet haben. Weitere Informationen finden Sie unter Erteilen Sie IAM-Berechtigungen für EC2 Instance Connect.

Beispiel für eine IAM-Richtlinie

Die folgenden IAM-Beispielrichtlinien ermöglichen es einem IAM-Prinzipal, eine Connect zu einer Instance herzustellen, indem er nur den angegebenen EC2 Instance Connect-Endpunkt verwendet, der durch die angegebene Endpunkt-ID identifiziert wird. `eice-123456789abcdef` Die Verbindung wird nur erfolgreich hergestellt, wenn alle Bedingungen erfüllt sind.

> **Note**
>
> `ec2:Describe*`-API-Aktionen unterstützen keine Berechtigungen auf Ressourcenebene. Aus diesem Grund ist in der obigen Anweisung der `*`-Platzhalter im `Resource`-Element erforderlich.

Linux

In diesem Beispiel wird ausgewertet, ob die Verbindung zur Instance auf Port 22 (SSH) hergestellt wurde, ob die private IP-Adresse der Instance im Bereich von `10.0.1.0/31` (zwischen `10.0.1.0` und `10.0.1.1`) liegt und die `maxTunnelDuration` weniger als oder gleich `3600` Sekunden ist. Die Verbindung wird nach `3600` Sekunden (1 Stunden) getrennt.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                },
                "IpAddress": {
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
                }
            }
        },
        {
            "Sid": "SSHPublicKey",
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

Windows

In diesem Beispiel wird ausgewertet, ob die Verbindung zur Instance auf Port 3389 (RDP) hergestellt wurde, ob die private IP-Adresse der Instance im Bereich von `10.0.1.0/31` (zwischen `10.0.1.0` und `10.0.1.1`) liegt und die `maxTunnelDuration` weniger als oder gleich `3600` Sekunden ist. Die Verbindung wird nach `3600` Sekunden (1 Stunden) getrennt.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "3389"
                },
                "IpAddress": {
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

Herstellen von Verbindungen nur von einem bestimmten IP-Adressbereich berechtigen

Die folgende Beispiel-IAM-Richtlinie ermöglicht es einem IAM-Prinzipal, eine Verbindung zu einer Instance herzustellen, sofern er von einer IP-Adresse innerhalb des in der Richtlinie angegebenen IP-Adressbereichs aus eine Verbindung herstellt. Wenn der IAM-Prinzipal `OpenTunnel` von einer IP-Adresse aufruft, die nicht innerhalb des Bereichs `192.0.2.0/24` liegt (der Beispiel-IP-Adressbereich in dieser Richtlinie), wird die Antwort `Access Denied` sein. Weitere Informationen finden Sie unter `aws:SourceIp` im IAM-Benutzerhandbuch.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "192.0.2.0/24"
                },
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                }
            }
        },
        {
            "Sid": "SSHPublicKey",
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Resource": "*"
        }
    ]
}
```

Sicherheitsgruppen für EC2 Instance Connect Endpoint

Eine Sicherheitsgruppe steuert den Datenverkehr, der die Ressourcen erreichen und verlassen darf, mit denen er verknüpft ist. Beispielsweise verweigern wir den Datenverkehr zu und von einer EC2 Amazon-Instance, sofern er nicht ausdrücklich von den mit der Instance verknüpften Sicherheitsgruppen zugelassen wird.

Die folgenden Beispiele zeigen Ihnen, wie Sie die Sicherheitsgruppenregeln für den EC2 Instance Connect-Endpunkt und die Ziel-Instances konfigurieren.

Beispiele

- EC2 Sicherheitsgruppenregeln für Instance Connect Endpoint
- Ziel-Instance-Sicherheitsgruppenregeln

EC2 Sicherheitsgruppenregeln für Instance Connect Endpoint

Die Sicherheitsgruppenregeln für einen EC2 Instance Connect-Endpunkt müssen zulassen, dass ausgehender Datenverkehr, der für die Ziel-Instances bestimmt ist, den Endpunkt verlässt. Sie können entweder die Instanz-Sicherheitsgruppe IPv4 oder den IPv6 Adressbereich der VPC als Ziel angeben.

Der Datenverkehr zum Endpunkt stammt vom EC2 Instance Connect Endpoint Service und ist unabhängig von den Regeln für eingehende Nachrichten für die Endpunkt-Sicherheitsgruppe zulässig. Verwenden Sie eine IAM-Richtlinie, um zu steuern, wer EC2 Instance Connect Endpoint verwenden kann, um eine Verbindung zu einer Instance herzustellen. Weitere Informationen finden Sie unter Berechtigungen zur Verwendung von EC2 Instance Connect Endpoint zum Herstellen einer Verbindung zu Instanzen.

Beispiel für eine Ausgangsregel: Referenzierung von Sicherheitsgruppen

Im folgenden Beispiel wird auf Sicherheitsgruppen verwiesen, was bedeutet, dass das Ziel eine Sicherheitsgruppe ist, die den Ziel-Instances zugeordnet ist. Diese Regel erlaubt ausgehenden Datenverkehr vom Endpunkt zu allen Instances, die diese Sicherheitsgruppe verwenden.

Protocol (Protokoll)	Ziel	Port-Bereich	Comment
TCP	*ID of instance security group*	22	Erlaubt ausgehenden SSH-Verkehr zu allen Instances, die der Instance-Sicherheitsgruppe zugeordnet sind

Beispiel für eine ausgehende Regel: Adressbereich IPv4

Das folgende Beispiel erlaubt ausgehenden Verkehr in den angegebenen IPv4 Adressbereich. Die IPv4 Adressen einer Instance werden von ihrem Subnetz aus zugewiesen, sodass Sie den IPv4 Adressbereich der VPC verwenden können.

Protocol (Protokoll)	Ziel	Port-Bereich	Comment
TCP	*VPC IPv4 CIDR*	22	Erlaubt ausgehenden SSH-Verkehr zur VPC

Beispiel für eine ausgehende Regel: Adressbereich IPv6

Das folgende Beispiel erlaubt ausgehenden Verkehr in den angegebenen IPv6 Adressbereich. Die IPv6 Adressen einer Instance werden von ihrem Subnetz aus zugewiesen, sodass Sie den IPv6 Adressbereich der VPC verwenden können.

Protocol (Protokoll)	Ziel	Port-Bereich	Comment
TCP	*VPC IPv6 CIDR*	22	Erlaubt ausgehenden SSH-Verkehr zur VPC

Ziel-Instance-Sicherheitsgruppenregeln

Die Sicherheitsgruppenregeln für Ziel-Instances müssen eingehenden Datenverkehr vom EC2 Instance Connect-Endpunkt zulassen. Sie können entweder die Endpunkt-Sicherheitsgruppe IPv4 oder einen IPv6 Oder-Adressbereich als Quelle angeben. Wenn Sie einen IPv4 Adressbereich angeben, hängt die Quelle davon ab, ob die Client-IP-Erhaltung aus- oder aktiviert ist. Weitere Informationen finden Sie unter Überlegungen.

Da Sicherheitsgruppen statusbehaftet sind, darf der Antwortdatenverkehr die VPC unabhängig von den ausgehenden Regeln für die Instance-Sicherheitsgruppe verlassen.

Beispiel für eine Eingangsregel: Referenzierung von Sicherheitsgruppen

Im folgenden Beispiel wird auf Sicherheitsgruppen verwiesen, was bedeutet, dass das Ziel eine Sicherheitsgruppe ist, die den Ziel-Instances zugeordnet ist. Diese Regel erlaubt eingehenden SSH-Verkehr vom Endpunkt zu allen Instances, die diese Sicherheitsgruppe verwenden, unabhängig davon, ob die Client-IP-Erhaltung aktiviert oder deaktiviert ist. Wenn es keine anderen Regeln für eingehende Sicherheitsgruppen für SSH gibt, akzeptieren die Instances nur SSH-Verkehr vom Endpunkt.

Protocol (Protokoll)	Quelle	Port-Bereich	Comment
TCP	*ID of endpoint security group*	22	Lässt eingehenden SSH-Daten verkehr von den Ressourcen zu, die der Endpunkt-Sicherheitsgruppe zugeordnet sind

Beispiel für eine Eingangsregel: Client-IP-Erhaltung aus

Das folgende Beispiel lässt eingehenden SSH-Verkehr aus dem angegebenen IPv4 Adressbereich zu. Da die Client-IP-Erhaltung ausgeschaltet ist, ist die IPv4 Quelladresse die Adresse der Endpunkt-Netzwerkschnittstelle. Die Adresse der Endpunkt-Netzwerkschnittstelle wird von ihrem Subnetz aus zugewiesen, sodass Sie den IPv4 Adressbereich der VPC verwenden können, um Verbindungen zu allen Instances in der VPC zuzulassen.

Protocol (Protokoll)	Quelle	Port-Bereich	Comment
TCP	*VPC IPv4 CIDR*	22	Eingehenden SSH-Datenverkehr von der VPC zulassen

Beispiel für eine Eingangsregel: Client-IP-Erhaltung an

Das folgende Beispiel erlaubt eingehenden SSH-Verkehr aus dem angegebenen Adressbereich. IPv4 Da die Client-IP-Erhaltung aktiviert ist, ist die IPv4 Quelladresse die Adresse des Clients.

Protocol (Protokoll)	Quelle	Port-Bereich	Comment
TCP	*Public IPv4 address range*	22	Lässt eingehenden Datenverkehr aus dem angegebenen IPv4 Client-Ad ressbereich zu

Einen EC2 Instance Connect-Endpunkt erstellen

Sie können einen EC2 Instance Connect-Endpunkt erstellen, um eine sichere Verbindung zu Ihren Instances zu ermöglichen.

Überlegungen

- Geteilte Subnetze — Sie können einen EC2 Instance Connect-Endpunkt in einem mit Ihnen geteilten Subnetz erstellen. Sie können jedoch keine EC2 Instance Connect-Endpoints verwenden, die der VPC-Besitzer in einem mit Ihnen geteilten Subnetz erstellt hat.
- IP-Adresstypen — EC2 Instance Connect-Endpoints unterstützen die folgenden Adresstypen, die mit Ihrem Subnetz kompatibel sein müssen:
  - `ipv4`— Stellen Sie nur eine Verbindung zu EC2 Instances mit privaten IPv4 Adressen her.
  - `dualstack`— Connect zu EC2 Instances mit privaten IPv4 Adressen oder IPv6 Adressen her.
  - `ipv6`— Stellt nur Connect zu EC2 Instanzen mit IPv6 Adressen her.

Voraussetzungen

Sie benötigen die erforderlichen IAM-Berechtigungen, um einen EC2 Instance Connect-Endpoint zu erstellen. Weitere Informationen finden Sie unter Berechtigungen zum Erstellen, Beschreiben, Ändern und Löschen von EC2 Instance Connect-Endpoints.

Console

So erstellen Sie einen EC2 Instance Connect-Endpunkt

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im linken Navigationsbereich die Option Endpoints (Endpunkte) aus.
3. Wählen Sie Endpunkt erstellen aus und geben Sie dann die Endpunkteinstellungen wie folgt an:

   a. (Optional) Geben Sie unter Namens-Tag einen Namen für den Endpunkt ein.

   b. Wählen Sie als Typ die Option EC2Instance Connect Endpoint aus.

   c. Wählen Sie unter Netzwerkeinstellungen für VPC die VPC aus, die die Ziel-Instances enthält.

   d. (Optional) Um Client-IP-Adressen beizubehalten, erweitern Sie Zusätzliche Einstellungen und aktivieren Sie das Kontrollkästchen Client-IP beibehalten. Andernfalls wird standardmäßig die Netzwerkschnittstelle des Endpunkts als Client-IP-Adresse verwendet.

   > **Note**
   >
   > Diese Option ist nur verfügbar, wenn der IP-Adresstyp des Endpunkts als konfiguriert ist IPv4.

   e. (Optional) Wählen Sie für Sicherheitsgruppen die VPC-Sicherheitsgruppe aus, die der Option zugeordnet werden soll. Andernfalls wird standardmäßig die Standard-Sicherheitsgruppe für die VPC verwendet. Weitere Informationen finden Sie unter Sicherheitsgruppen für EC2 Instance Connect Endpoint.

   f. Wählen Sie für Subnetz das Subnetz aus, in dem der Endpunkt erstellt werden soll.

   g. Wählen Sie als IP-Adresstyp den IP-Adresstyp für den Endpunkt aus. Wählen Sie Dualstack, wenn Sie sowohl Verbindungen zu Ihren Instances als IPv4 auch IPv6 Verbindungen unterstützen müssen. Wählen Sie aus IPv4, ob Sie die Erhaltung der Client-IP unterstützen möchten.

h. (Optional) Sie fügen ein Tag hinzu, indem Sie neues Tag hinzufügen auswählen und den Schlüssel und den Wert für das Tag eingeben.

4. Überprüfen Sie die Einstellungen und wählen Sie dann Endpunkt erstellen.

   Der Anfangsstatus des Endpunkts ist Ausstehend. Bevor Sie über diesen Endpunkt eine Verbindung zu einer Instance herstellen können, warten Sie, bis der Status Verfügbar lautet. Dies kann einige Minuten dauern.

5. Informationen zum Herstellen einer Verbindung mit einer Instance über Ihren Endpunkt erhalten Sie unter Herstellen einer Verbindung zu einer -Instance.

AWS CLI

So erstellen Sie einen EC2 Instance Connect-Endpunkt

Verwenden Sie den Befehl create-instance-connect-endpoint.

```
aws ec2 create-instance-connect-endpoint \
    --subnet-id subnet-0123456789example
```

Um den Typ des Datenverkehrs anzugeben, den der Endpunkt unterstützt, geben Sie den Parameter `--ip-address-type` an. Gültige Werte sind `ipv4`, `dualstack` oder `ipv6`. Das Subnetz muss den von Ihnen angegebenen IP-Adresstyp unterstützen. Wenn der Parameter `--ip-address-type` weggelassen wird, wird der Standardwert durch den vom Subnetz unterstützten IP-Adresstyp bestimmt.

```
aws ec2 create-instance-connect-endpoint \
    --subnet-id subnet-0123456789example \
    --ip-address-type ipv4
```

Es folgt eine Beispielausgabe.

```
{
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "create-complete",
        "StateMessage": "",
```

```
        "DnsName": "eice-0123456789example.0123abcd.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com",
        "FipsDnsName": "eice-0123456789example.0123abcd.fips.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com",
        "NetworkInterfaceIds": [
            "eni-0123abcd"
        ],
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1a",
        "AvailabilityZoneId": "use1-az4",
        "CreatedAt": "2023-04-07T15:43:53.000Z",
        "SubnetId": "subnet-0123abcd",
        "PreserveClientIp": false,
        "SecurityGroupIds": [
            "sg-0123abcd"
        ],
        "Tags": [],
        "IpAddressType": "ipv4"
}
```

Den Erstellungsstatus überwachen

Der Anfangswert für das `State`-Feld ist `create-in-progress`. Bevor Sie über diesen Endpunkt eine Verbindung zu einer Instance herstellen können, warten Sie, bis der Status `create-complete` lautet. Verwenden Sie den describe-instance-connect-endpointsBefehl, um den Status des EC2 Instance Connect-Endpunkts zu überwachen. Der Parameter `--query` filtert die Ergebnisse in das `State`-Feld.

```
aws ec2 describe-instance-connect-endpoints --instance-connect-endpoint-
ids eice-0123456789example --query InstanceConnectEndpoints[*].State --output text
```

Es folgt eine Beispielausgabe.

```
create-complete
```

PowerShell

So erstellen Sie den EC2 Instance Connect-Endpunkt

Verwenden Sie das cmdlet New-EC2InstanceConnectEndpoint.

```
New-EC2InstanceConnectEndpoint -SubnetId subnet-0123456789example
```

Um den Typ des Datenverkehrs anzugeben, den der Endpunkt unterstützt, geben Sie den Parameter `-IpAddressType` an. Gültige Werte sind `ipv4`, `dualstack` oder `ipv6`. Das Subnetz muss den von Ihnen angegebenen IP-Adresstyp unterstützen. Wenn der Parameter `-IpAddressType` weggelassen wird, wird der Standardwert durch den vom Subnetz unterstützten IP-Adresstyp bestimmt.

```
New-EC2InstanceConnectEndpoint -SubnetId subnet-0123456789example -
IpAddressType ipv4
```

Es folgt eine Beispielausgabe.

```
OwnerId                     : 111111111111
InstanceConnectEndpointId   : eice-0123456789example
InstanceConnectEndpointArn  : arn:aws:ec2:us-east-1:111111111111:instance-connect-
endpoint/eice-0123456789example
State                       : create-complete
StateMessage                :
DnsName                     : eice-0123456789example.0123abcd.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com
FipsDnsName                 : eice-0123456789example.0123abcd.fips.ec2-instance-
connect-endpoint.us-east-1.amazonaws.com
NetworkInterfaceIds         : {eni-0123abcd}
VpcId                       : vpc-0123abcd
AvailabilityZone            : us-east-1a
AvailabilityZoneId          : use1-az4
CreatedAt                   : 4/7/2023 3:43:53 PM
SubnetId                    : subnet-0123abcd
PreserveClientIp            : False
SecurityGroupIds            : {sg-0123abcd}
Tags                        : {}
IpAddressType               : ipv4
```

Den Erstellungsstatus überwachen

Der Anfangswert für das `State`-Feld ist `create-in-progress`. Bevor Sie über diesen Endpunkt eine Verbindung zu einer Instance herstellen können, warten Sie, bis der Status `create-complete` lautet. Verwenden Sie das Get-EC2InstanceConnectEndpointCmdlet, um den Status des EC2 Instance Connect-Endpunkts zu überwachen. `.State.Value`filtert die Ergebnisse in das `State` Feld.

```
(Get-EC2InstanceConnectEndpoint -InstanceConnectEndpointId
 "eice-0123456789example").State.Value
```

Es folgt eine Beispielausgabe.

```
create-complete
```

Einen EC2 Instance Connect-Endpunkt ändern

Sie können bestehende EC2 Instance Connect-Endpoints mit dem AWS CLI oder einem SDK ändern. Die EC2 Amazon-Konsole unterstützt keine Endpunktmodifikation.

Bevor Sie beginnen, benötigen Sie die erforderlichen IAM-Berechtigungen. Weitere Informationen finden Sie unter Berechtigungen zum Erstellen, Beschreiben, Ändern und Löschen von EC2 Instance Connect-Endpoints.

Parameter, die Sie ändern können

Sie können die folgenden EC2 Instance Connect-Endpunktparameter ändern:

Sicherheitsgruppen

Sie können neue Sicherheitsgruppen für den EC2 Instance Connect-Endpunkt angeben. Die neuen Sicherheitsgruppen ersetzen die aktuellen Sicherheitsgruppen.

Wenn Sie die Sicherheitsgruppen ändern, müssen Sie Folgendes angeben:

- Mindestens eine Sicherheitsgruppe, auch wenn es sich nur um die Standardsicherheitsgruppe in der VPC handelt.
- Die IDs der Sicherheitsgruppen, nicht die Namen.

IP-Adresstyp

Sie können einen neuen IP-Adresstyp für den EC2 Instance Connect-Endpunkt angeben.

Zulässige Werte: `ipv4` | `dualstack` | `ipv6`

Client-IP-Einstellung beibehalten

Sie können angeben, ob die Client-IP-Adresse als Quelle beibehalten werden soll.

> **Note**
>
> Die Beibehaltung der Client-IP wird nur auf IPv4 EC2 Instance Connect-Endpunkten unterstützt. Bei der Aktivierung von `PreserveClientIp` muss entweder der vorhandene IP-Adresstyp des Endpunkts `ipv4` sein, oder wenn der IP-Adresstyp in derselben Anfrage geändert wird, muss der neue Wert `ipv4` sein.

AWS CLI

So ändern Sie einen EC2 Instance Connect-Endpunkt

Verwenden Sie den modify-instance-connect-endpointBefehl und geben Sie den EC2 Instance Connect-Endpunkt und die zu ändernden Parameter an. Im folgenden Beispiel werden alle Parameter in einer einzelnen Anforderung geändert.

```
aws ec2 modify-instance-connect-endpoint \
    --instance-connect-endpoint-id eice-0123456789example \
    --security-group-ids sg-0123456789example \
    --ip-address-type dualstack \
    --no-preserve-client-ip
```

Es folgt eine Beispielausgabe.

```
{
    "Return": true
}
```

So überwachen Sie den Status der Aktualisierung

Während der Änderung ändert sich der Status des EC2 Instance Connect-Endpunkts auf`update-in-progress`. Der Aktualisierungsvorgang wird asynchron ausgeführt und mit dem Status `update-complete` oder `update-failed` abgeschlossen. Der Endpunkt verwendet seine alte Konfiguration, bis der Status auf `update-complete` geändert wird.

Verwenden Sie den Befehl describe-instance-connect-endpoints, um den Aktualisierungsstatus zu überwachen. Der Parameter `--query` filtert die Ergebnisse in das `State`-Feld.

```
aws ec2 describe-instance-connect-endpoints \
    --instance-connect-endpoint-ids eice-0123456789example \
```

```
    --query InstanceConnectEndpoints[*].State --output text
```

Es folgt eine Beispielausgabe.

```
update-complete
```

PowerShell

So ändern Sie einen EC2 Instance Connect-Endpunkt

Verwenden Sie das Edit-EC2InstanceConnectEndpointCmdlet und geben Sie den EC2 Instance Connect-Endpunkt und die zu ändernden Parameter an. Im folgenden Beispiel werden alle Parameter in einer einzelnen Anforderung geändert.

```
Edit-EC2InstanceConnectEndpoint `
    -InstanceConnectEndpointId eice-0123456789example `
    -SecurityGroupIds sg-0123456789example `
    -IpAddressType dualstack `
    -PreserveClientIp $false
```

Es folgt eine Beispielausgabe.

```
True
```

So überwachen Sie den Status der Aktualisierung

Während der Änderung ändert sich der Status des EC2 Instance Connect-Endpunkts auf`update-in-progress`. Der Aktualisierungsvorgang wird asynchron ausgeführt und mit dem Status `update-complete` oder `update-failed` abgeschlossen. Der Endpunkt verwendet seine alte Konfiguration, bis der Status auf `update-complete` geändert wird.

Verwenden Sie den Befehl Get-EC2InstanceConnectEndpoint, um den Aktualisierungsstatus zu überwachen. `.State.Value` filtert die Ergebnisse in das `State`-Feld.

```
(Get-EC2InstanceConnectEndpoint -InstanceConnectEndpointId
 "eice-0123456789example").State.Value
```

Es folgt eine Beispielausgabe.

```
update-complete
```

Löschen Sie einen EC2 Instance Connect-Endpunkt

Wenn Sie mit einem EC2 Instance Connect-Endpunkt fertig sind, können Sie ihn löschen.

Sie benötigen die erforderlichen IAM-Berechtigungen, um einen EC2 Instance Connect-Endpoint zu erstellen. Weitere Informationen finden Sie unter Berechtigungen zum Erstellen, Beschreiben, Ändern und Löschen von EC2 Instance Connect-Endpoints.

Wenn Sie einen EC2 Instance Connect-Endpoint mithilfe der Konsole löschen, wechselt er in den Status Löschen. Wenn der Löschvorgang erfolgreich ist, wird der gelöschte Endpunkt nicht mehr angezeigt. Falls die Löschaktion fehlschlägt, ist der Status delete-failed und die Statusmeldung gibt die Fehlerursache an.

Wenn Sie einen EC2 Instance Connect-Endpunkt mit dem löschen AWS CLI, wechselt er in den `delete-in-progress` Status. Wenn der Löschvorgang erfolgreich ist, wechselt es in den `delete-complete`-Status. Schlägt die Löschaktion fehl, ist der Status `delete-failed` und `StateMessage` gibt die Fehlerursache an.

Console

So löschen Sie einen EC2 Instance Connect-Endpunkt

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im linken Navigationsbereich die Option Endpoints (Endpunkte) aus.
3. Wählen Sie den Endpunkt.
4. Wählen Sie Actions (Aktionen), Delete VPC Endpoint (VPC-Endpunkte löschen).
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein.
6. Wählen Sie Löschen aus.

AWS CLI

So löschen Sie einen EC2 Instance Connect-Endpunkt

Verwenden Sie den delete-instance-connect-endpointBefehl und geben Sie die ID des EC2 Instance Connect-Endpunkts an, den Sie löschen möchten.

```
aws ec2 delete-instance-connect-endpoint --instance-connect-endpoint-
id eice-03f5e49b83924bbc7
```

Es folgt eine Beispielausgabe.

```
{
    "InstanceConnectEndpoint": {
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "delete-in-progress",
        "StateMessage": "",
        "NetworkInterfaceIds": [],
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1d",
        "AvailabilityZoneId": "use1-az2",
        "CreatedAt": "2023-02-07T12:05:37+00:00",
        "SubnetId": "subnet-0123abcd"
    }
}
```

PowerShell

So löschen Sie einen EC2 Instance Connect-Endpunkt

Verwenden Sie das Remove-EC2InstanceConnectEndpointCmdlet und geben Sie die ID des zu löschenden EC2 Instance Connect-Endpunkts an.

```
Remove-EC2InstanceConnectEndpoint -InstanceConnectEndpointId eice-03f5e49b83924bbc7
```

Es folgt eine Beispielausgabe.

```
@{
    InstanceConnectEndpoint = @{
        OwnerId = "111111111111"
        InstanceConnectEndpointId = "eice-0123456789example"
        InstanceConnectEndpointArn = "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example"
        State = "delete-in-progress"
        StateMessage = ""
        NetworkInterfaceIds = @()
        VpcId = "vpc-0123abcd"
        AvailabilityZone = "us-east-1d"
        AvailabilityZoneId = "use1-az2"
        CreatedAt = "2023-02-07T12:05:37+00:00"
```

```
        SubnetId = "subnet-0123abcd"
    }
}
```

Stellen Sie mithilfe von EC2 Instance Connect Endpoint eine Verbindung zu einer EC2 Amazon-Instance Connect

Sie können EC2 Instance Connect Endpoint verwenden, um eine Verbindung zu einer EC2 Amazon-Instance herzustellen, die SSH oder RDP unterstützt.

Voraussetzungen

- Sie benötigen die erforderliche IAM-Berechtigung, um eine Connect zu einem EC2 Instance Connect-Endpunkt herzustellen. Weitere Informationen finden Sie unter Berechtigungen zur Verwendung von EC2 Instance Connect Endpoint zum Herstellen einer Verbindung zu Instanzen.
- Der EC2 Instance Connect-Endpunkt muss sich in einem der folgenden Zustände befinden:
  - create-complete für einen neuen Endpunkt
  - update-in-progress, Aktualisierung abgeschlossen oder Aktualisierung fehlgeschlagen für einen vorhandenen Endpunkt, der geändert wurde. Wenn ein Endpunkt geändert wird, verwendet er weiterhin seine ursprüngliche Konfiguration, bis sich der Status in update-complete ändert.

    Wenn Ihre VPC keinen EC2 Instance Connect-Endpunkt hat, können Sie einen erstellen. Weitere Informationen finden Sie unter Einen EC2 Instance Connect-Endpunkt erstellen.
- Der IP-Adresstyp EC2 Instance Connect Endpoint muss mit dem IP-Adresstyp der Instanz kompatibel sein. Wenn es sich bei Ihrem Endpunkt-IP-Adresstyp um einen Dual-Stack-Adresstyp handelt, kann er IPv4 sowohl für als auch für IPv6 Adressen funktionieren.
- (Linux-Instances) Um die EC2 Amazon-Konsole zu verwenden, um eine Verbindung zu Ihrer Instance herzustellen, oder um die CLI zu verwenden, um eine Verbindung herzustellen und EC2 Instance Connect den kurzlebigen Schlüssel verarbeiten zu lassen, muss Instance Connect auf Ihrer EC2 Instance installiert sein. Weitere Informationen finden Sie unter Installieren Sie EC2 Instance Connect.
- Stellen Sie sicher, dass die Sicherheitsgruppe der Instance eingehenden SSH-Verkehr vom EC2 Instance Connect-Endpunkt zulässt. Weitere Informationen finden Sie unter Ziel-Instance-Sicherheitsgruppenregeln.

Verbindungsoptionen

- Stellen Sie über die EC2 Amazon-Konsole eine Verbindung zu Ihrer Linux-Instance her
- Herstellen einer Verbindung zu Ihrer Linux-Instance mit SSH
- Stellen Sie mit der Instanz-ID eine Connect zu Ihrer Linux-Instance her, indem Sie AWS CLI
- Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von RDP
- Fehlerbehebung

Stellen Sie über die EC2 Amazon-Konsole eine Verbindung zu Ihrer Linux-Instance her

Sie können über die EC2 Amazon-Konsole (einen browserbasierten Client) wie folgt eine Verbindung zu einer Instance herstellen.

So stellen Sie über die EC2 Amazon-Konsole eine Verbindung zu Ihrer Instance her

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und klicken Sie auf Verbinden.
4. Wählen Sie den Tab EC2 Instance Connect.
5. Wählen Sie für Verbindungstyp die Option Mit einer privaten IP verbinden aus.
6. Wählen Sie entweder IPv4 Privatadresse oder IPv6Adresse. Die Optionen sind auf der Grundlage der IP-Adressen verfügbar, die Ihrer Instance zugewiesen wurden. Wenn eine Option nicht verfügbar ist, ist Ihrer Instance keine IP-Adresse dieses Typs zugewiesen.
7. Wählen Sie für EC2 Instance Connect Endpoint die ID des EC2 Instance Connect-Endpunkts aus.

   > **Note**
   >
   > Der EC2 Instance Connect-Endpunkt muss mit der IP-Adresse kompatibel sein, die Sie im vorherigen Schritt ausgewählt haben. Wenn es sich bei Ihrem Endpunkt-IP-Adresstyp um einen Dual-Stack-Adresstyp handelt, kann er IPv4 sowohl für als auch für IPv6 Adressen funktionieren. Weitere Informationen finden Sie unter Einen EC2 Instance Connect-Endpunkt erstellen.

8. Wenn das AMI, das Sie zum Starten der Instance verwendet haben, einen anderen Benutzernamen als `ec2-user` verwendet, geben Sie unter Benutzername den richtigen Benutzernamen ein.

9. Geben Sie für Max. Tunneldauer (Sekunden) die maximal zulässige Dauer für die SSH-Verbindung ein.

   Die Dauer muss den in der IAM-Richtlinie festgelegten `maxTunnelDuration`-Bedingungen entsprechen. Wenn Sie keinen Zugriff zur IAM-Richtlinie haben, wenden Sie sich an Ihren Administrator.
10. Wählen Sie Connect aus. Dadurch wird ein Terminalfenster für Ihre Instance geöffnet.

Herstellen einer Verbindung zu Ihrer Linux-Instance mit SSH

Sie können SSH verwenden, um eine Verbindung zu Ihrer Linux-Instance herzustellen, und den `open-tunnel`-Befehl verwenden, um einen privaten Tunnel einzurichten. Sie können `open-tunnel` im Einzelverbindungsmodus oder im Mehrfachverbindungsmodus verwenden. Sie können Ihre Instance-ID, eine private IPv4 Adresse oder eine IPv6 Adresse angeben.

Informationen zur Verwendung von AWS CLI , um über SSH eine Verbindung zu Ihrer Instance herzustellen, finden Sie unterConnect mit dem her AWS CLI.

Im folgenden Beispiel wird OpenSSH verwendet. Sie können jeden anderen SSH-Client verwenden, der einen Proxy-Modus unterstützt.

Einzelne -Verbindung

So erlauben Sie nur eine einzige Verbindung zu einer Instance über SSH und den Befehl **`open-tunnel`**

Verwenden Sie `ssh` und den open-tunnel AWS CLI Befehl wie folgt. Der `-o`-Proxy-Befehl umfasst den `open-tunnel`-Befehl, der den privaten Tunnel zur Instance erstellt.

```
ssh -i my-key-pair.pem ec2-user@i-1234567890abcdef0 \
    -o ProxyCommand='aws ec2-instance-connect open-tunnel --instance-
id i-1234567890abcdef0'
```

Für:

- `-i` – Geben Sie das Schlüsselpaar an, das zum Starten der Instance verwendet wurde.
- *`ec2-user`*`@`*`i-1234567890abcdef0`* – Geben Sie den Benutzernamen des AMI an, das zum Starten der Instance verwendet wurde, und die Instance-ID. Bei Instances mit einer IPv6 Adresse müssen Sie die IPv6 Adresse anstelle der Instanz-ID angeben.

- `--instance-id` – Geben Sie die ID der Instance, zu der eine Verbindung hergestellt werden soll, an. Alternativ können Sie auch %h angeben, wodurch die Instance-ID des Benutzers extrahiert wird. Ersetzen `--instance-id` *i-1234567890abcdef0* Sie bei Instanzen mit einer IPv6 Adresse durch`--private-ip-address` *2001:db8::1234:5678:1.2.3.4*.

Mehrfachverbindung

Um mehrere Verbindungen zu einer Instance zuzulassen, führen Sie zuerst den open-tunnel AWS CLI Befehl aus, um auf neue TCP-Verbindungen zu warten, und verwenden Sie ihn dann, `ssh` um eine neue TCP-Verbindung und einen privaten Tunnel zu Ihrer Instance zu erstellen.

So erlauben Sie mehrere Verbindungen zu Ihrer Instance mit SSH und dem Befehl **`open-tunnel`**

1. Führen Sie den folgenden Befehl aus, um auf Ihrem lokalen Computer auf neue TCP-Verbindungen am angegebenen Port zu horchen.

   ```
   aws ec2-instance-connect open-tunnel \
       --instance-id i-1234567890abcdef0 \
       --local-port 8888
   ```

   Erwartete Ausgabe:

   ```
   Listening for connections on port 8888.
   ```

2. Führen Sie in einem neuen Terminalfenster den folgenden `ssh`-Befehl aus, um eine neue TCP-Verbindung und einen privaten Tunnel zu Ihrer Instance zu erstellen.

   ```
   ssh -i my-key-pair.pem ec2-user@localhost -p 8888
   ```

   Erwartete Ausgabe – Im ersten Terminalfenster sehen Sie Folgendes:

   ```
   [1] Accepted new tcp connection, opening websocket tunnel.
   ```

   Möglicherweise wird auch Folgendes angezeigt:

   ```
   [1] Closing tcp connection.
   ```

Stellen Sie mit der Instanz-ID eine Connect zu Ihrer Linux-Instance her, indem Sie AWS CLI

Wenn Sie nur Ihre Instance-ID kennen, können Sie den AWS CLI Befehl ec2-instance-connect ssh verwenden, um über einen SSH-Client eine Verbindung zu Ihrer Instance herzustellen. Weitere Informationen finden Sie unter Connect mit dem her AWS CLI.

Voraussetzungen

- Installieren Sie AWS CLI Version 2 und konfigurieren Sie sie mit Ihren Anmeldeinformationen. Weitere Informationen finden Sie unter Installieren oder Aktualisieren auf die neueste Version von AWS CLI und Konfiguration der AWS CLI im AWS Command Line Interface -Benutzerhandbuch.
- Alternativ können Sie AWS CLI Befehle in der vorauthentifizierten Shell öffnen AWS CloudShell und ausführen.

So Connect Sie mithilfe der Instanz-ID und eines Instance Connect-Endpunkts eine Verbindung zu einer EC2 Instance her

Wenn Sie nur die Instanz-ID kennen, verwenden Sie den Befehl ec2-instance-connect ssh CLI und geben Sie den `ssh` Befehl, die Instanz-ID und den `--connection-type` Parameter mit dem `eice` Wert an, um einen Instance Connect-Endpunkt zu verwenden. EC2 Wenn die Instanz nur eine IPv6 Adresse hat, müssen Sie auch den Parameter mit der `--instance-ip` Adresse angeben. IPv6

- Wenn die Instanz eine private IPv4 Adresse hat (sie kann auch eine IPv6 Adresse haben), verwenden Sie den folgenden Befehl und die folgenden Parameter:

```
aws ec2-instance-connect ssh \
    --instance-id i-1234567890example \
    --os-user ec2-user \
    --connection-type eice
```

- Wenn die Instanz nur eine IPv6 Adresse hat, fügen Sie den `--instance-ip` Parameter der IPv6 Adresse hinzu:

```
aws ec2-instance-connect ssh \
    --instance-id i-1234567890example \
    --instance-ip 2001:db8::1234:5678:1.2.3.4 \
    --os-user ec2-user \
    --connection-type eice
```

> **Tip**
>
> Wenn Sie eine Fehlermeldung erhalten, stellen Sie sicher, dass Sie AWS CLI Version 2 verwenden. Der `ssh` Parameter ist nur in AWS CLI Version 2 verfügbar. Weitere Informationen zu finden Sie unter Über AWS CLI Version 2 im AWS Command Line Interface -Benutzerhandbuch.

Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von RDP

Sie können Remote Desktop Protocol (RDP) über EC2 Instance Connect Endpoint verwenden, um eine Verbindung zu einer Windows-Instanz ohne öffentliche IPv4 Adresse oder öffentlichen DNS-Namen herzustellen.

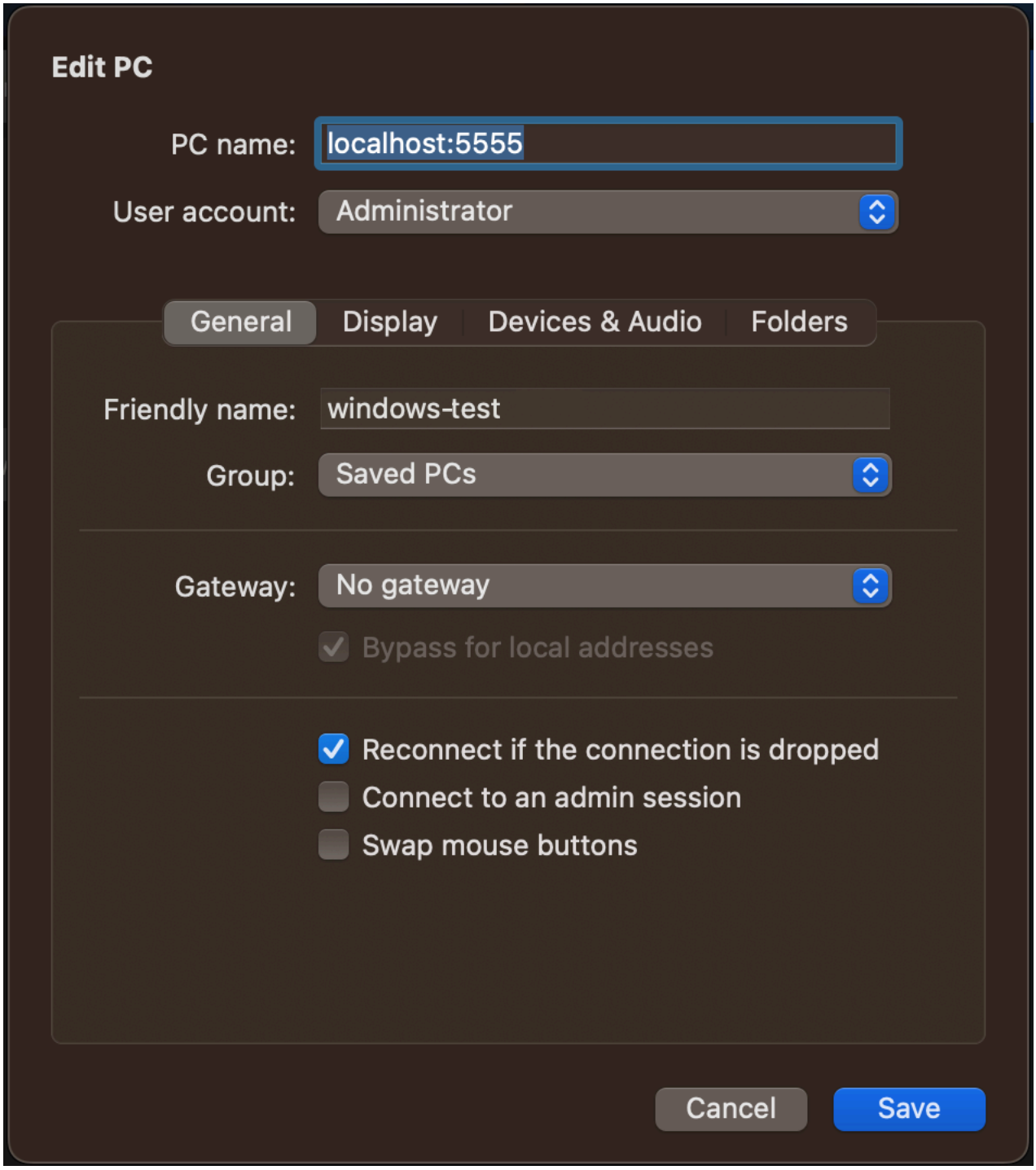
Verwenden Sie einen RDP Client, um sich mit Ihrer Windows-Instance zu verbinden.

1. Führen Sie die Schritte 1–8 unter Herstellen einer Verbindung mit Ihrer Windows-Instance über RDP aus. Nachdem Sie die RDP-Desktop-Datei in Schritt 8 heruntergeladen haben, erhalten Sie die Meldung Verbindung nicht möglich. Dies ist zu erwarten, da Ihre Instance keine öffentliche IP-Adresse hat.
2. Führen Sie den folgenden Befehl aus, um einen privaten Tunnel zu der VPC einzurichten, in der sich die Instance befindet. `--remote-port` muss `3389` sein, weil RDP standardmäßig Port 3389 verwendet.

   ```
   aws ec2-instance-connect open-tunnel \
       --instance-id i-1234567890abcdef0 \
       --remote-port 3389 \
       --local-port any-port
   ```

3. Suchen Sie in Ihrem Downloads-Ordner nach der RDP-Desktop-Datei, die Sie heruntergeladen haben, und ziehen Sie sie in das RDP-Clientfenster.
4. Klicken Sie mit der rechten Maustaste auf die RDP-Datei und wählen Sie Bearbeiten aus.
5. Geben Sie im Fenster PC bearbeiten als PC-Name (die Instance, zu der eine Verbindung hergestellt werden soll) `localhost:`*`local-port`* ein, wobei *`local-port`* den gleichen Wert wie in Schritt 2 verwendet, und wählen Sie dann Speichern aus.

Beachten Sie, dass der folgende Screenshot des Fensters PC bearbeiten von Microsoft Remote Desktop auf einem Mac stammt. Wenn Sie einen Windows-Client verwenden, sieht das Fenster eventuell anders aus.



6. Klicken Sie im RDP-Client mit der rechten Maustaste auf den PC (den Sie gerade konfiguriert haben) und wählen Sie Verbinden, um eine Verbindung zu Ihrer Instance herzustellen.

7. Geben Sie an der Eingabeaufforderung das unverschlüsselte Passwort für das Administratorkonto ein.

Fehlerbehebung

Verwenden Sie die folgenden Informationen, um Probleme zu diagnostizieren und zu beheben, die auftreten können, wenn Sie EC2 Instance Connect Endpoint verwenden, um eine Instance zu verbinden.

Kann nicht zu Ihrer Instance verbinden

Nachfolgend finden Sie die häufigsten Gründe, warum Sie möglicherweise keine Verbindung zu Ihrer Instance herstellen können.

- Sicherheitsgruppen — Überprüfen Sie die Sicherheitsgruppen, die dem EC2 Instance Connect-Endpunkt und Ihrer Instance zugewiesen sind. Weitere Informationen zu Sicherheitsgruppenregeln finden Sie unter Sicherheitsgruppen für EC2 Instance Connect Endpoint.
- Instance-Status – Stellen Sie sicher, dass sich Ihre Instance im `running`-Status befindet.
- Schlüsselpaar – Wenn der Befehl, den Sie zum Herstellen einer Verbindung verwenden, einen privaten Schlüssel erfordert, stellen Sie sicher, dass Ihre Instance über einen öffentlichen Schlüssel verfügt und dass Sie über den entsprechenden privaten Schlüssel verfügen.
- IAM-Berechtigungen – Stellen Sie sicher, dass Sie über die erforderlichen IAM-Berechtigungen verfügen. Weitere Informationen finden Sie unter Erteilen Sie Berechtigungen zur Verwendung von EC2 Instance Connect Endpoint.

Weitere Tipps zur Fehlerbehebung für Linux-Instances finden Sie unter Fehlersuche bei Verbindungsproblemen mit Ihrer Amazon-EC2-Linux-Instance. Weitere Tipps zur Fehlerbehebung für Windows-Instances finden Sie unter the section called “RDP-Probleme mit der Windows-Instance”.

ErrorCode: AccessDeniedException

Wenn Sie einen `AccessDeniedException`-Fehler erhalten und die `maxTunnelDuration`-Bedingung in der IAM-Richtlinie angegeben ist, geben Sie den `--max-tunnel-duration`-Parameter unbedingt an, wenn Sie eine Verbindung zu einer Instance herstellen. Weitere Informationen zu Parametern finden Sie unter open-tunnel in der AWS CLI - Befehlsreferenz.

Über den EC2 Instance Connect-Endpunkt hergestellte Verbindungen protokollieren

Sie können Ressourcenoperationen protokollieren und Verbindungen, die über den EC2 Instance Connect-Endpunkt hergestellt wurden, mit AWS CloudTrail Protokollen überprüfen.

Weitere Informationen zur Verwendung AWS CloudTrail mit Amazon EC2 finden Sie unterAmazon-EC2-API-Aufrufe mit AWS CloudTrail protokollieren.

API-Aufrufe von EC2 Instance Connect Endpoint protokollieren mit AWS CloudTrail

EC2 Ressourcenoperationen von Instance Connect Endpoint werden CloudTrail als Verwaltungsereignisse protokolliert. Wenn die folgenden API-Aufrufe getätigt werden, wird die Aktivität als CloudTrail Ereignis im Ereignisverlauf aufgezeichnet:

- `CreateInstanceConnectEndpoint`
- `DescribeInstanceConnectEndpoints`
- `DeleteInstanceConnectEndpoint`

Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Wird verwendet AWS CloudTrail , um Benutzer zu überprüfen, die über Instance Connect Endpoint eine Verbindung zu einer EC2 Instance herstellen

Verbindungsversuche zu Instanzen über EC2 Instance Connect Endpoint werden CloudTrail im Eventverlauf protokolliert. Wenn eine Verbindung zu einer Instance über einen EC2 Instance Connect-Endpunkt initiiert wird, wird die Verbindung als CloudTrail Verwaltungsereignis mit dem Wert `eventName` of protokolliert`OpenTunnel`.

Sie können EventBridge Amazon-Regeln erstellen, die das CloudTrail Ereignis an ein Ziel weiterleiten. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Im Folgenden finden Sie ein Beispiel für ein `OpenTunnel` Verwaltungsereignis, das angemeldet wurde CloudTrail.

```
{
    "eventVersion": "1.08",
```

```
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
        "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
        "accountId": "123456789012",
        "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
        "userName": "IAM-friendly-name"
    },
    "eventTime": "2023-04-11T23:50:40Z",
    "eventSource": "ec2-instance-connect.amazonaws.com",
    "eventName": "OpenTunnel",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.2.3.4",
    "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
    "requestParameters": {
        "instanceConnectEndpointId": "eici-0123456789EXAMPLE",
        "maxTunnelDuration": "3600",
        "remotePort": "22",
        "privateIpAddress": "10.0.1.1"
    },
    "responseElements": null,
    "requestID": "98deb2c6-3b3a-437c-a680-03c4207b6650",
    "eventID": "bbba272c-8777-43ad-91f6-c4ab1c7f96fd",
    "readOnly": false,
    "resources": [{
        "accountId": "123456789012",
        "type": "AWS::EC2::InstanceConnectEndpoint",
        "ARN": "arn:aws:ec2:us-east-1:123456789012:instance-connect-endpoint/
eici-0123456789EXAMPLE"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


Serviceverknüpfte Rolle für EC2 Instance Connect Endpoint

Amazon EC2 verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon verknüpft ist. EC2 Servicebezogene Rollen sind von Amazon vordefiniert EC2 und beinhalten alle Berechtigungen, die Amazon EC2 benötigt, um andere in AWS-Services Ihrem Namen anzurufen. Weitere Informationen finden Sie unter Serviceverknüpfte Rollen im IAM-Benutzerhandbuch.

Dienstbezogene Rollenberechtigungen für EC2 Instance Connect Endpoint

Amazon EC2 verwendet AWSServiceRoleForEC2InstanceConnect, um Netzwerkschnittstellen in Ihrem Konto zu erstellen und zu verwalten, die für EC2 Instance Connect Endpoint erforderlich sind.

Die serviceverknüpfte Rolle AWSServiceRoleForEC2InstanceConnect vertraut darauf, dass der folgende Service die Rolle annimmt:

- `ec2-instance-connect.amazonaws.com`

Die AWSServiceRoleForEC2InstanceConnectserviceverknüpfte Rolle verwendet die folgende verwaltete Richtlinie:

- Ec2 InstanceConnectEndpoint

Informationen zu den Berechtigungen für die verwaltete Richtlinie finden Sie unter Ec2 InstanceConnectEndpoint in der Referenz für AWS verwaltete Richtlinien.

Eine serviceverknüpfte Rolle für EC2 Instance Connect Endpoint erstellen

Sie müssen diese serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie einen EC2 Instance Connect-Endpunkt erstellen, EC2 erstellt Amazon die serviceverknüpfte Rolle für Sie.

Eine serviceverknüpfte Rolle für EC2 Instance Connect Endpoint bearbeiten

EC2 Mit Instance Connect Endpoint können Sie die AWSServiceRoleForEC2InstanceConnectserviceverknüpfte Rolle nicht bearbeiten.

Löschen Sie eine serviceverknüpfte Rolle für EC2 Instance Connect Endpoint

Wenn Sie EC2 Instance Connect Endpoint nicht mehr verwenden müssen, empfehlen wir Ihnen, die AWSServiceRoleForEC2InstanceConnectserviceverknüpfte Rolle zu löschen.

Sie müssen alle EC2 Instance Connect-Endpunktressourcen löschen, bevor Sie die serviceverknüpfte Rolle löschen können.

Informationen zum Löschen der serviceverknüpften Rolle finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Sie müssen Berechtigungen konfigurieren, um einer IAM-Entität (z. B. Benutzer, Gruppe oder Rolle) zu erlauben, eine serviceverknüpfte Rolle zu erstellen, zu bearbeiten oder zu löschen. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Kontingente für den EC2 Instance Connect-Endpunkt

Ihr AWS-Konto hat Standardkontingente, früher als Limits bezeichnet, für jeden AWS Dienst. Sofern nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region.

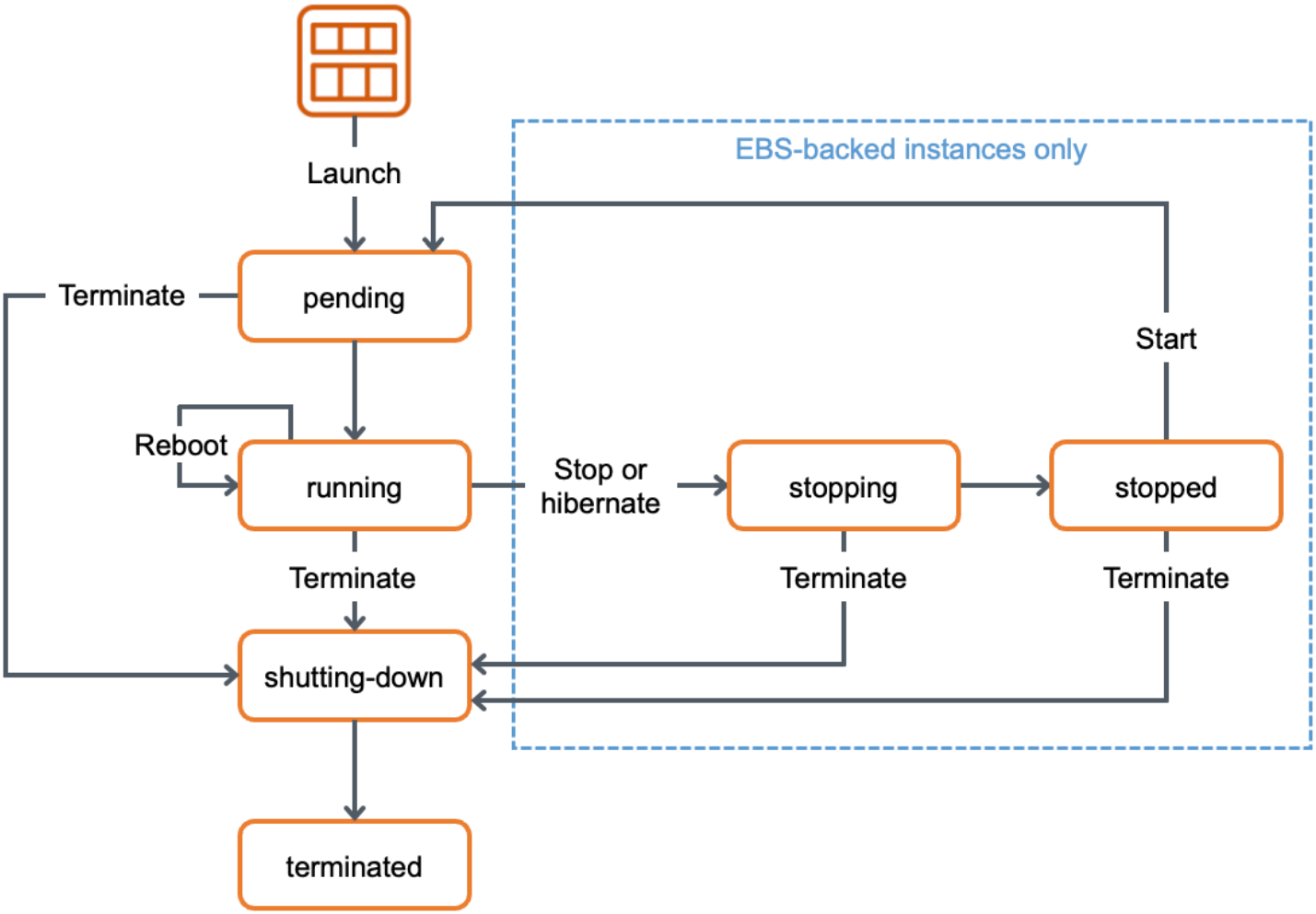
Ihr AWS-Konto hat die folgenden Kontingente in Bezug auf EC2 Instance Connect Endpoint.

Name	Standard	Anpassbar
Maximale Anzahl von EC2 Instance Connect-Endpunkten pro AWS-Konto AWS-Region	5	Nein
Maximale Anzahl von EC2 Instance Connect-Endpunkten pro VPC	1	Nein
Maximale Anzahl von EC2 Instance Connect-Endpunkten pro Subnetz	1	Nein
Maximale Anzahl gleichzeitiger Verbindungen pro EC2 Instance Connect-Endpunkt	20	Nein

Amazon-EC2-Instance-Statusänderungen

Eine Amazon EC2-Instance wechselt durch verschiedene Zustände von dem Zeitpunkt, an dem Sie sie starten, bis zu ihrer Beendigung.

In der folgenden Abbildung sind die Übergänge zwischen den Instances dargestellt.



Sie können benachrichtigt werden, wenn Ihre Instances ihren Status ändern. Weitere Informationen finden Sie unter the section called “Statusänderungsereignisse”.

Abrechnung nach Instance-Status

In der folgenden Tabelle finden Sie eine kurze Beschreibung der einzelnen Instance-Statuszustände. Es wird außerdem angegeben, ob sie abgerechnet werden. Für einige AWS-Ressourcen, wie z. B. Amazon-EBS-Volumes und elastische IP-Adressen, fallen Gebühren unabhängig vom Instance-Status an. Weitere Informationen finden Sie unter Unerwartete Gebühren vermeiden im AWS Billing-Benutzerhandbuch.

Instance-Status	Beschreibung	Abrechnung für Instance-Nutzung
`pending`	Die Instance bereitet sich darauf vor, in den Status `running` überzugehen. Eine Instance wechselt in den Status `pending`, wenn sie gestartet wird oder wenn sie sich im Status `stopped` befand und dann gestartet wird.	Nicht berechnet
`running`	Die Instance wird ausgeführt und ist bereit zur Nutzung.	Berechnet
`stopping`	Die Instance bereitet sich darauf vor, angehalten zu werden.	Nicht berechnet **Note** Wenn Sie eine Instance in den Ruhezustand versetzen, wird Ihnen die Rechnung gestellt, solange sich die Instance im `stopping`-Status befindet.
`stopped`	Die Instance wird beendet und kann nicht genutzt werden. Die Instance kann jederzeit gestartet werden.	Nicht berechnet
`shutting-down`	Die Instance bereitet sich darauf vor, beendet zu werden.	Nicht berechnet
`terminated`	Die Instance wurde dauerhaft gelöscht und	Nicht berechnet

Instance-Status	Beschreibung	Abrechnung für Instance-Nutzung
	kann nicht gestartet werden.	**Note** Reserved Instances, die sich auf beendete Instances beziehen, werden bis zum Ende ihrer Laufzeit entsprechend ihrer Zahlungsoption abgerechnet. Weitere Informationen finden Sie unter Überblick über Reserved Instances für Amazon EC2

Ausstehende Instances

Wenn Sie eine Instance starten, erhält diese den Status `pending`. Der von Ihnen beim Start festgelegte Instance-Typ bestimmt die Hardware des Host-Computers für Ihre Instance. Um die Instance zu starten, verwenden wir das von Ihnen beim Start angegebene Amazon Machine Image (AMI). Wenn die Instance bereit ist, verfügt sie über den Status `running`. Sie können eine Verbindung mit Ihrer laufenden Instance herstellen und sie wie einen normalen Computer verwenden.

Sobald Ihre Instance in den Status `running` übergeht, wird Ihnen jede Sekunde (und mindestens eine Minute) der Betriebszeit der Instance in Rechnung gestellt, auch wenn sich die Instance im Leerlauf befindet und Sie keine Verbindung zu ihr herstellen.

Angehaltene Instances

Wenn eine Statusprüfung Ihrer Instance fehlschlägt oder Ihre Anwendungen auf der Instance nicht wie erwartet ausgeführt werden und wenn das Stamm-Volume Ihrer Instance ein Amazon EBS-Volume ist, können Sie Ihre Instance anhalten und starten, um das Problem zu beheben.

Wenn Sie Ihre Instance anhalten, wird sie zunächst in den Status the `stopping` und anschließend in den Status `stopped` versetzt. Wenn Ihre Instance `stopped` ist, werden Ihnen keine Nutzungs- oder Datenübertragungsgebühren berechnet. Für die Speicherung etwaiger Amazon-EBS-Volumes fallen Gebühren an. Während sich die Instance im Status `stopped` befindet, können Sie bestimmte Attribute der Instance ändern, z. B. auch den Instance-Typ.

Wenn Sie Ihre Instance starten, wechselt sie in den `pending`-Status und wird auf einen neuen Host-Computer verschoben (in einigen Fällen verbleibt sie jedoch auf dem aktuellen Host). Wenn Sie Ihre Instance anhalten und starten, verlieren Sie alle Daten auf den Instance-Speicher-Volumes, die dem vorherigen Host-Computer angefügt waren.

Ihre Instance behält ihre private IPv4-Adresse, was bedeutet, dass eine Elastic-IP-Adresse, die der privaten IPv4-Adresse oder der Benutzeroberfläche zugeordnet ist, mit Ihrer Instance verbunden bleibt. Wenn Ihre Instance über eine IPv6-Adresse verfügt, behält sie die IPv6-Adresse bei.

Jedes Mal, wenn Sie eine Instance von `stopped` auf `running` umstellen, werden Ihnen Gebühren pro Sekunde bei Ausführung der Instance berechnet, mindestens jedoch eine Minute pro Instance-Start.

Weitere Informationen zum Anhalten und Starten von Instances finden Sie unter Stoppen und starten Sie EC2 Amazon-Instances.

Instances im Ruhezustand

Wenn Sie eine Instance in den Ruhezustand versetzen, erhält das Betriebssystem ein Signal, die Instance in den Ruhezustand zu versetzen ("suspend-to-disk"). Hierdurch wird der Inhalt des Instance-Arbeitsspeichers (RAM) auf Ihrem Amazon EBS-Stamm-Volume gespeichert. Das Amazon EBS-Stamm-Volume der Instance und alle angefügten Amazon EBS-Daten-Volumens bleiben erhalten. Wenn Sie die Instance starten, wird das Amazon EBS-Stamm-Volume im vorherigen Zustand wiederhergestellt und der RAM-Inhalt wird neu geladen. Zuvor angefügte Daten-Volumes werden erneut zugewiesen und die Instance behält ihre Instance-ID bei.

Wenn Sie Ihre Instance in den Ruhezustand versetzen, wird sie zunächst in den Status the `stopping` und anschließend in den Status `stopped` versetzt. Wir berechnen keine Nutzung für eine im Ruhezustand befindliche Instance, wenn sie sich im Zustand `stopped` befindet. Während sie sich im Zustand `stopping` befindet wird jedoch eine Berechnung durchgeführt (im Gegensatz zum Anhalten einer Instance, ohne sie in den Ruhezustand zu versetzen). Wir stellen für die Datenübertragung keine Gebühren in Rechnung. Für Speicher für Amazon EBS-Volumes, einschließlich Speicher für den RAM-Daten, fallen jedoch Gebühren an.

Wenn Sie Ihre Instance im Ruhezustand starten, wird sie in den Zustand `pending` versetzt, und wir verschieben die Instance auf einen neuen Host-Computer (in einigen Fällen verbleibt sie jedoch auf dem aktuellen Host).

Ihre Instance behält ihre private IPv4-Adresse. Dies bedeutet, dass eine mit der privaten IPv4-Adresse oder Netzwerkschnittstelle verknüpfte Elastic IP-Adresse immer noch mit Ihrer Instance verknüpft ist. Wenn Ihre Instance über eine IPv6-Adresse verfügt, behält sie die IPv6-Adresse bei.

Weitere Informationen finden Sie unter Versetzen Sie Ihre Amazon-Instance in den Ruhezustand EC2 .

Neustarten von Instances

Sie können einen Neustart Ihrer Instance mit der Amazon EC2-Konsole, einem Befehlszeilen-Tool und der Amazon EC2-API durchführen. Wir empfehlen Ihnen, Amazon EC2 zum erneuten Starten Ihrer Instance zu verwenden, anstatt den Neustart-Befehl für das Betriebssystem auf Ihrer Instance auszuführen.

Ein Neustart einer Instance entspricht einem Neustart des Betriebssystems. Die Instance verbleibt auf demselben Host-Computer und behält ihren öffentlichen DNS-Namen, ihre private IP-Adresse sowie alle Daten auf ihren Instance-Speicher-Volumes. Es dauert i. d. R. einige Minuten, bis der Neustart abgeschlossen ist. Die Dauer des Neustarts hängt jedoch von der Konfiguration der Instance ab.

Beim Neustart einer Instance wird kein neuer Abrechnungszeitraum gestartet; es wird weiterhin sekundengenau und ohne weitere Mindestgebühr von einer Minute abgerechnet.

Weitere Informationen finden Sie unter Eine Amazon-EC2-Instance neu starten.

Beendete Instances

Wenn Sie sich entschieden haben, dass Sie eine Instance nicht mehr benötigen, können Sie sie beenden. Sobald der Status einer Instance zu `shutting-down` oder `terminated` wechselt, fallen für diese Instance keine Gebühren mehr an.

Bei aktiviertem Beendigungsschutz können Sie die Instance nicht mithilfe der Konsole, der CLI oder der API beenden.

Nachdem Sie eine Instance beendet haben, bleibt sie in der Konsole noch für kurze Zeit sichtbar, bevor der Eintrag automatisch gelöscht wird. Sie können eine beendete Instance auch mithilfe der CLI und API beschreiben. Ressourcen (z. B. Tags (Markierungen)) werden nach und nach von der beendeten Instance getrennt, sodass sie nach kurzer Zeit auf der beendeten Instance ggf. nicht mehr sichtbar sind. Sie können keine Verbindung mehr mit einer beendeten Instance herstellen oder diese wiederherstellen.

Jede Amazon EBS-gestützte Instance unterstützt das Attribut `InstanceInitiatedShutdownBehavior`, mit dem gesteuert wird, ob die Instance angehalten oder beendet wird, wenn Sie innerhalb der Instance das Herunterfahren initiieren (z. B. über den Befehl shutdown unter Linux). Das Standardverhalten ist das Anhalten der Instance. Sie können die Einstellungen für dieses Attribut ändern, während die Instance in Betrieb oder angehalten ist.

Jedes Amazon EBS-Volume unterstützt das Attribut `DeleteOnTermination`. Hiermit wird gesteuert, ob das Volume gelöscht wird oder erhalten bleibt, wenn Sie die zugehörige Instance beenden. Standardmäßig wird das Root-Volume gelöscht und alle anderen EBS-Volumes bleiben erhalten.

Weitere Informationen finden Sie unter EC2 Amazon-Instances beenden.

Unterschiede zwischen Instance-Status

In der folgenden Tabelle sind die wichtigsten Unterschiede zwischen Neustart, Anhalten, Ruhezustand und Beenden Ihrer Instance zusammengefasst.

Merkmal	Neustart	Anhalten/Starten (nur Amazon EBS-gestützte Instances)	Ruhezustand (nur durch Amazon EBS gesicherte Instances)	Beenden
Host-Computer	Die Instance verbleibt auf demselben Host-Computer.	Wir verschieben die Instance auf einen neuen Host-Computer (in einigen Fällen verbleibt sie jedoch auf dem aktuellen Host).	Wir verschieben die Instance auf einen neuen Host-Computer (in einigen Fällen verbleibt sie jedoch auf dem aktuellen Host).	Keine
Private IPv4-Adresse	EC2-VPC: Die Instance behält ihre private IPv4-Adresse.	EC2-VPC: Die Instance behält ihre private IPv4-Adresse.	EC2-VPC: Die Instance behält ihre private IPv4-Adresse.	Keine
Öffentliche IPv4-Adresse	Die Instance behält ihre	Die Instance erhält eine neue öffentliche IPv4-	Die Instance erhält eine neue öffentliche IPv4-Adresse,	Keine

Merkmal	Neustart	Anhalten/Starten (nur Amazon EBS-gestützte Instances)	Ruhezustand (nur durch Amazon EBS gesicherte Instances)	Beenden
	öffentliche IPv4-Adresse.	Adresse, außer sie verfügt über eine sekundäre Netzwerkschnittstelle oder eine sekundäre private IPv4-Adresse, die einer Elastic-IP-Adresse zugeordnet ist.	außer sie verfügt über eine sekundäre Netzwerkschnittstelle oder eine sekundäre private IPv4-Adresse, die einer Elastic-IP-Adresse zugeordnet ist.	
Elastic IP-Adresse (IPv4)	Die Elastic IP-Adresse bleibt der Instance zugeordnet.	Die Elastic IP-Adresse bleibt der Instance zugeordnet.	Die Elastic IP-Adresse bleibt der Instance zugeordnet.	Die Zuordnung der Elastic IP-Adresse zur Instance wird aufgehoben.
IPv6-Adresse	Die Instance behält ihre IPv6-Adresse.	Die Instance behält ihre IPv6-Adresse.	Die Instance behält ihre IPv6-Adresse.	Keine
Instance-Speicher-Volumes	Die Daten bleiben erhalten.	Die Daten werden gelöscht.	Die Daten werden gelöscht.	Die Daten werden gelöscht.
Stammvolumen	Das Volume bleibt erhalten.	Das Volume bleibt erhalten.	Das Volume bleibt erhalten.	Das Volume wird standardmäßig gelöscht.
RAM (Inhalt des Speichers)	RAM wird gelöscht	RAM wird gelöscht	RAM wird in einer Datei auf dem Root-Volume gespeichert	RAM wird gelöscht

Merkmal	Neustart	Anhalten/Starten (nur Amazon EBS-gestützte Instances)	Ruhezustand (nur durch Amazon EBS gesicherte Instances)	Beenden
Fakturierung	Die Instance-Abrechnungsstunde ändert sich nicht	Sobald der Status einer Instance zu wechselt, fallen für diese Instance keine Gebühren mehr a `stopping`. Bei jedem Übergang einer Instance von `stopped` zu `running` wird ein neuer Abrechnungszeitraum gestartet ; für jeden Start der Instance wird eine Mindestgebühr von einer Minute abgerechnet.	Ihnen werden Gebühren berechnet, während sich die Instance im Zustand `stopping` befindet. Es werden jedoch keine Gebühren berechnet, wenn sich die Instance im Zustand `stopped` befindet. Bei jedem Übergang einer Instance von `stopped` zu `running` wird ein neuer Abrechnungszeitraum gestartet ; für jeden Start der Instance wird eine Mindestgebühr von einer Minute abgerechnet.	Sobald der Status einer Instance zu `shutting-down` wechselt, fallen für diese Instance keine Gebühren mehr an

Instances mit einem Instance-Speicher-Root-Volume werden durch den Befehl zum Herunterfahren des Betriebssystems immer beendet. Sie können steuern, ob eine Instance mit einem EBS–Root-Volume durch den Befehl zum Herunterfahren des Betriebssystems angehalten oder beendet werden sollen. Weitere Informationen finden Sie unter Ändern des durch die Instance initiierten Abschaltverhaltens.

Stoppen und starten Sie EC2 Amazon-Instances

Sie können die Instance anhalten und starten, wenn das Root-Volume ein Amazon-EBS-Volume ist. Wenn Sie eine Instance anhalten, wird sie heruntergefahren. Wenn Sie eine Instance starten, wird sie in der Regel auf einen neuen zugrundeliegenden Host-Computer migriert und ihr wird eine neue öffentliche IPv4 Adresse zugewiesen.

Ein Instance-Stopp kann vom Benutzer initiiert werden (wobei Sie die Instance manuell beenden) oder initiiert werden AWS (als Reaktion auf ein geplantes Stopp-Ereignis, bei dem ein irreparabler Ausfall des zugrunde liegenden Hosts für Ihre Instance AWS festgestellt wird).

Für vom Benutzer initiierte Stopps empfehlen wir, die EC2 Amazon-Konsole, CLI oder API zu verwenden, anstatt den Stopp-Befehl des Betriebssystems von Ihrer Instance aus auszuführen. Wenn Sie Amazon verwenden EC2 und die Instance nicht innerhalb weniger Minuten ordnungsgemäß heruntergefahren wird, EC2 führt Amazon einen Hard-Shutdown durch. Darüber hinaus AWS CloudTrail erstellt es einen API-Datensatz darüber, wann Ihre Instance gestoppt wurde.

In diesem Thema wird beschrieben, wie Sie ein benutzerinitiiertes Anhalten durchführen. Hinweise zu einem Stopp, der von ausgeführt wurde AWS, finden Sie unter EC2 Amazon-Instances verwalten, deren Stopp oder Stilllegung geplant ist.

Wenn Sie eine Instance anhalten, wird sie nicht gelöscht. Wenn Sie eine Instance nicht mehr benötigen, können Sie sie löschen. Weitere Informationen finden Sie unter EC2 Amazon-Instances beenden. Informationen darüber wie Sie eine Instance in den Ruhezustand versetzen können, um den Inhalt des Instance-Speichers (RAM) zu speichern, finden Sie unter Versetzen Sie Ihre Amazon-Instance in den Ruhezustand EC2 . Informationen zu den Unterscheidungen zwischen den Aktionen des Instance-Lebenszyklus finden Sie unter Unterschiede zwischen Instance-Status.

Inhalt

- So funktioniert das Stoppen und Starten einer EC2 Instanz
- Methoden zum Anhalten einer Instance
- Manuelles Anhalten und Starten Ihrer Instances
- Automatisches Anhalten und Starten Ihrer Instances
- Alle ausgeführten und angehaltenen Instances suchen
- Die ersten und letzten Startzeiten finden
- Aktivieren Sie den Stop-Schutz für Ihre EC2 Instances

So funktioniert das Stoppen und Starten einer EC2 Instanz

Wenn Sie eine EC2 Amazon-Instance beenden, werden Änderungen auf Betriebssystemebene (OS) der Instance registriert, einige Ressourcen gehen verloren und einige Ressourcen bleiben bestehen. Wenn Sie eine Instance starten, werden die Änderungen auf Instance-Ebene registriert.

Themen

- Was geschieht, wenn Sie eine Instance anhalten?
- Was geschieht, wenn Sie eine Instance starten?
- Testen der Reaktion der Anwendung auf Stopp und Start
- Kosten im Zusammenhang mit dem Starten und Anhalten einer Instance

Was geschieht, wenn Sie eine Instance anhalten?

Im Folgenden wird beschrieben, was normalerweise passiert, wenn Sie eine Instance mit der standardmäßigen Anhaltemethode beenden. Beachten Sie, dass einige Aspekte je nach verwendeter Anhaltemethode variieren können.

Auf Betriebssystemebene registrierte Änderungen

- Die API-Anfrage sendet ein Tastendruck-Ereignis an den Gast.
- Verschiedene Systemservices werden infolge des Tastendruck-Ereignisses gestoppt. Ein ordnungsgemäßes Herunterfahren des Betriebssystems wird durch das ACPI-Maustastendruck-Ereignis zum Herunterfahren vom Hypervisor ausgelöst.
- Das Herunterfahren des ACPI wird initiiert.
- Die Instance wird heruntergefahren, wenn der Prozess zum ordnungsgemäßen Herunterfahren des Betriebssystems beendet ist. Die Zeit zum Herunterfahren des Betriebssystems kann nicht konfiguriert werden.
- Wenn das Instance-Betriebssystem nicht innerhalb weniger Minuten sauber heruntergefahren wird, wird ein Hard Shutdown durchgeführt.
- Die Instance wird nicht mehr ausgeführt.
- Der Instance-Status ändert sich zu `stopping` und dann zu `stopped`.
- [Amazon EC2 Auto Scaling] Wenn sich Ihre Instance in einer Amazon EC2 Auto Scaling-Gruppe befindet, wenn sich die Instance in einem anderen EC2 Amazon-Bundesstaat befindet als `running` oder wenn ihr Status für die Statusprüfungen lautet`impaired`, betrachtet Amazon EC2

Auto Scaling die Instance als fehlerhaft und ersetzt sie. Weitere Informationen finden Sie unter Zustandsprüfungen für Instances in einer Amazon EC2 Auto Scaling Scaling-Gruppe im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

- [Windows-Instances] Wenn Sie eine Windows Instance anhalten und starten, führt der Start-Agent Aufgaben auf der Instance aus, z. B. das Ändern der Laufwerksbuchstaben für alle angefügten Amazon-EBS-Volumes. Weitere Informationen zu diesen Standardeinstellungen und deren Änderung finden Sie unter the section called “EC2Launch v2”.

Verlorene Ressourcen

- Im Arbeitsspeicher gespeicherte Daten.
- Auf den Instance-Speicher-Volumes gespeicherte Daten.
- Die öffentliche IPv4 Adresse, die Amazon der Instance beim Start oder Start EC2 automatisch zugewiesen hat. Um eine öffentliche IPv4 Adresse beizubehalten, die sich nie ändert, können Sie Ihrer Instance eine Elastic IP-Adresse zuordnen.

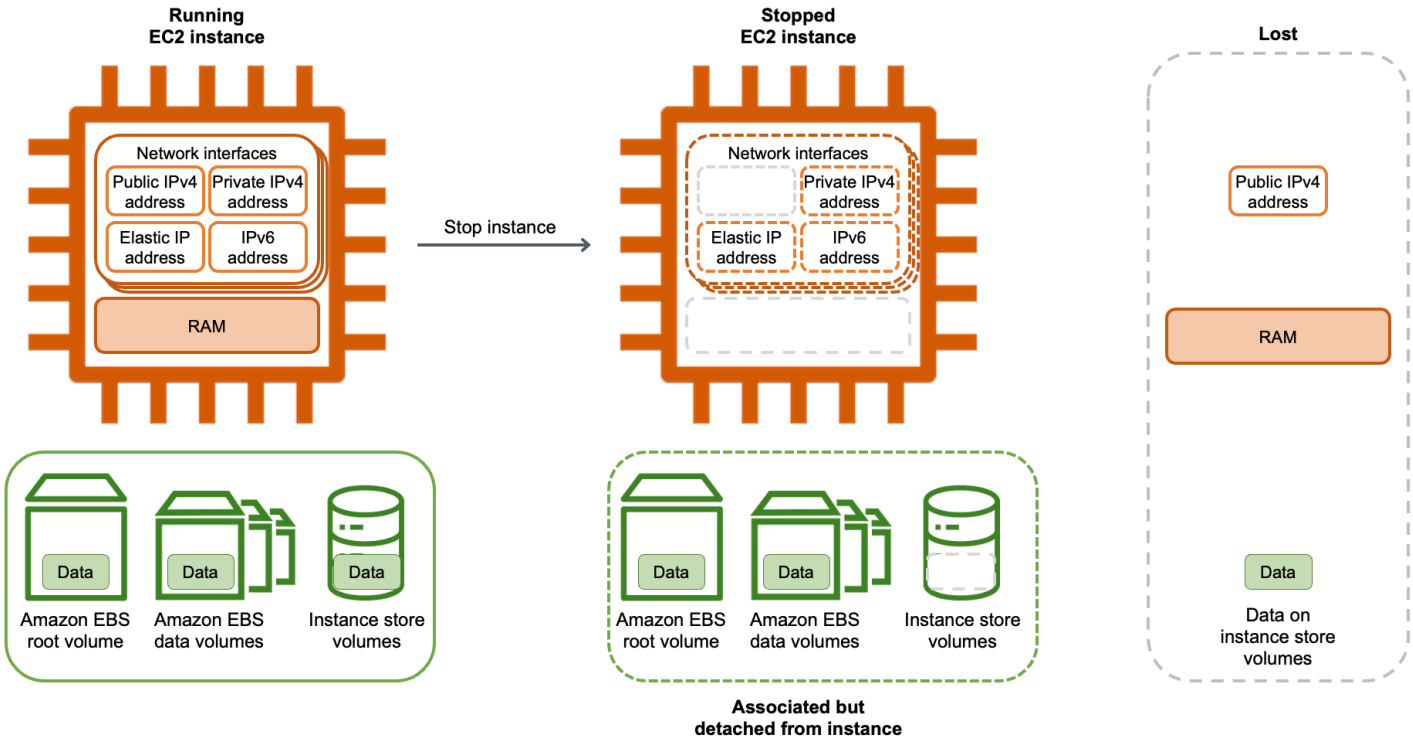
Ressourcen, die fortbestehen

- Alle angehängten Amazon-EBS-Root- und -Daten-Volumes.
- Daten, die in den Amazon-EBS-Volumes gespeichert sind.
- Alle angehängten Netzwerkschnittstellen.

  Eine Netzwerkschnittstelle umfasst die folgenden Ressourcen, die ebenfalls bestehen:

  - Private IPv4 Adressen.
  - IPv6 Adressen.
  - elastische IP-Adressen, die der Instance zugeordnet sind Beachten Sie, dass Ihnen beim Anhalten der Instance die Gebühren für die zugeordneten Elastic-IP-Adressen in Rechnung gestellt werden.

Das folgende Diagramm zeigt, was bestehen bleibt und was verloren geht, wenn eine EC2 Instanz gestoppt wird. Das Diagramm ist in drei Teile gegliedert: Der erste Teil mit der Bezeichnung Running EC2 instance zeigt die Instanz im `running` Status mit ihren Ressourcen. Der zweite Teil mit der Bezeichnung Stopped EC2 instance zeigt die Instanz im `stopped` Status mit den Ressourcen, die bestehen bleiben. Der dritte Teil mit der Bezeichnung Verloren zeigt die Ressourcen, die verloren gehen, wenn die Instance angehalten wird.



Weitere Informationen darüber, was passiert, wenn Sie eine Mac-Instance anhalten, finden Sie unter Beenden oder beenden Sie Ihre Amazon EC2 Mac-Instance.

Was geschieht, wenn Sie eine Instance starten?

- In den meisten Fällen wird die Instance auf einen neuen zugrundeliegenden Host-Computer migriert (in einigen Fällen, z. B. wenn eine Instance einem Host in einer Dedicated- Host-Konfiguration zugewiesen wird, verbleibt sie jedoch auf dem aktuellen Host).
- Die zugeordneten EBS-Volumes und Netzwerkschnittstellen werden wieder an die Instance angehängt.
- Amazon EC2 weist der Instance eine neue öffentliche IPv4 Adresse zu, wenn die Instance so konfiguriert ist, dass sie eine öffentliche IPv4 Adresse empfängt, es sei denn, sie hat eine sekundäre Netzwerkschnittstelle oder eine sekundäre private IPv4 Adresse, die mit einer Elastic IP-Adresse verknüpft ist.
- Wenn Sie eine Instance in einer Placement-Gruppe anhalten und dann wieder starten, wird sie in der Placement-Gruppe weiterhin ausgeführt. Der Startvorgang schlägt aber fehl, wenn für die Instance nicht genügend Kapazität vorhanden ist. Wenn Sie beim Starten einer Instance in einer Placement-Gruppe, in der bereits Instances ausgeführt werden, einen Kapazitätsfehler erhalten, beenden Sie alle Instances in der Placement-Gruppe und starten Sie sie alle erneut. Wenn Sie die

Instances starten, werden diese unter Umständen zu Hardware migriert, die über Kapazität für alle angeforderten Instances verfügt.

Testen der Reaktion der Anwendung auf Stopp und Start

Sie können AWS Fault Injection Service damit testen, wie Ihre Anwendung reagiert, wenn Ihre Instance gestoppt und gestartet wird. Weitere Informationen finden Sie im AWS Fault Injection Service -Benutzerhandbuch.

Kosten im Zusammenhang mit dem Starten und Anhalten einer Instance

Die folgenden Kosten sind mit dem Anhalten und Starten einer Instance verbunden.

Anhalten – Sobald sich der Status einer Instance zu `shutting-down` oder `terminated` ändert, fallen für die Instance keine Gebühren mehr an. Für eine angehaltene Instance werden Ihnen keine Nutzungs- oder Datenübertragungsgebühren in Rechnung gestellt. Für die Speicherung von Amazon-EBS-Speichervolumes fallen Gebühren an.

Starten – Jedes Mal, wenn Sie eine angehaltene Instance starten, wird Ihnen mindestens eine Minute Nutzungsdauer in Rechnung gestellt. Nach einer Minute werden Ihnen nur die genutzten Sekunden in Rechnung gestellt. Wenn Sie beispielsweise eine Instance 20 Sekunden lang ausführen und sie dann anhalten, wird Ihnen eine Nutzungsminute in Rechnung gestellt. Wenn Sie eine Instance 3 Minuten und 40 Sekunden lang ausführen, werden Ihnen 3 Minuten und 40 Sekunden Nutzungsdauer in Rechnung gestellt.

Methoden zum Anhalten einer Instance

Es gibt vier Möglichkeiten, eine vom Benutzer initiierte Anhaltung durchzuführen: Standard-Anhaltung, Anhaltung beim Herunterfahren des Betriebssystems, erzwungene Anhaltung und erzwungene Anhaltung mit Überspringen des Herunterfahrens des Betriebssystems. Die folgende Tabelle vergleicht die wichtigsten Unterschiede zwischen den Anhaltemethoden.

Anhaltem thode	Hauptzweck	Anwendungsfall	CLI-Befehl
Standard Anhalten	Normales Herunterfahren der Instance mit versuchtem ordnungsgemäßem Herunterfahren des Betriebssystems.	Typisches Anhalten einer Instance.	`aws ec2 stop-instances \`

Anhaltem thode	Hauptzweck	Anwendungsfall	CLI-Befehl
			`--instance-id i-1234567890abcdef0`
Anhalten mit Überspringen des Herunterfahrens des Betriebssystems	Umgeht das ordnungsgemäße Herunterfahren des Betriebssystems beim Anhalten einer Instance.	Wenn die Umgehung des ordnungsgemäßen Herunterfahrens des Betriebssystems erforderlich ist.	`aws ec2 stop-instances \ --instance-id i-1234567890abcdef0 \ --skip-os-shutdown`
Stoppen erzwingen	Behandelt eingefrorene Instances. Versucht zuerst ein Standard-Anhalten. Wenn die Instance nicht angehalten wird, wird das Anhalten der Instance erzwungen.	Wenn die Instance im Status `stopping` feststeckt.	`aws ec2 stop-instances \ --instance-id i-1234567890abcdef0 \ --force`
Erzwungenes Anhalten mit Überspringen des Herunterfahrens des Betriebssystems	Erzwing das Anhalten und umgeht das ordnungsgemäße Herunterfahren des Betriebssystems beim Anhalten einer Instance.	Wenn ein erzwungenes Anhalten und die Umgehung des ordnungsgemäßen Herunterfahrens des Betriebssystems erforderlich ist.	`aws ec2 stop-instances \ --instance-id i-1234567890abcdef0 \ --force \ --skip-os-shutdown`

Anweisungen zur Verwendung der einzelnen Methoden finden Sie im Folgenden:

- Eine Instance mit einem ordnungsgemäßen Herunterfahren des Betriebssystems anhalten
- Eine Instance anhalten und das ordnungsgemäße Herunterfahren des Betriebssystems umgehen
- Erzwingung des Stopps einer Instance

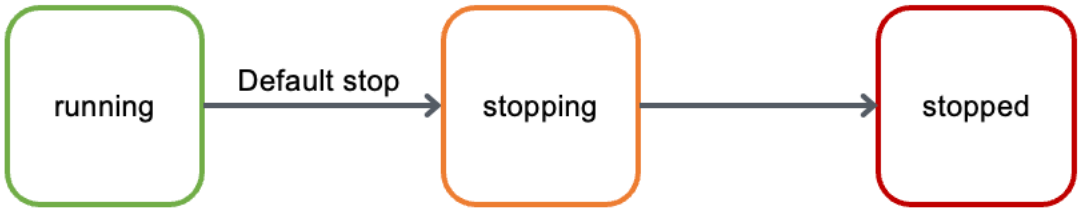
Anhaltemethoden:

- Standard-Anhalten
- Anhalten mit Überspringen des Herunterfahrens des Betriebssystems
- Stoppen erzwingen
- Erzwungenes Anhalten mit Überspringen des Herunterfahrens des Betriebssystems

Die folgenden Abschnitte enthalten detailliertere Informationen zu den vier verschiedenen vom Benutzer initiierten Anhaltemethoden.

Standard-Anhalten

Die Standard-Anhaltemethode ist die Standardmethode zum Anhalten einer Instance. Wenn Sie den StopInstances Befehl ausführen, wechselt die Instanz vom `running` Status zu `stopping` und schließlich zu`stopped`, wie in der folgenden Abbildung dargestellt:



Zweck: Normales Herunterfahren der Instance mit versuchtem ordnungsgemäßem Herunterfahren des Betriebssystems.

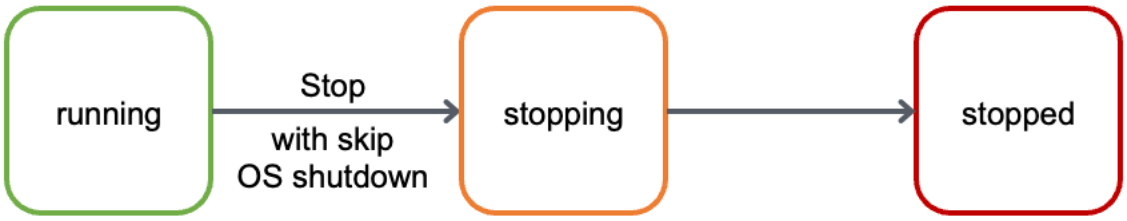
Auswirkung auf die Daten: Daten auf dem EBS-Root-Volume und den Daten-Volumes bleiben erhalten. Daten auf den Instance-Speicher-Volumes gehen verloren.

Verwendungszweck: Erster Anhalteversuch für typische Anhaltungen.

> **Note**
>
> Wenn Sie bereits eine Anhaltung mit Überspringen des Herunterfahrens des Betriebssystems versucht haben, führt eine nachfolgende Standard-Anhaltung während derselben Statusübergangssitzung nicht zu einem ordnungsgemäßen Herunterfahren des Betriebssystems. Das Umgehen des ordnungsgemäßen Herunterfahrens des Betriebssystems ist für die aktuelle Sitzung der Instance irreversibel.

Anhalten mit Überspringen des Herunterfahrens des Betriebssystems

Wenn das ordnungsgemäße Herunterfahren des Betriebssystems umgangen werden muss, kann die Methode „Anhalten mit Überspringen des Herunterfahren des Betriebssystems“ verwendet werden, um eine Instance anzuhalten und das ordnungsgemäße Herunterfahren des Betriebssystems zu umgehen, wie in der folgenden Abbildung dargestellt:



> **Warning**
>
> Das Umgehen des ordnungsgemäßen Herunterfahrens des Betriebssystems kann zu Datenverlust oder Beschädigung führen (z. B. wenn Speicherinhalte nicht auf die Festplatte geschrieben werden oder während der Übertragung verloren gehen IOs) oder dass Shutdown-Skripten übersprungen werden.

Zweck: Umgeht das ordnungsgemäße Herunterfahren des Betriebssystems beim Anhalten einer Instance.

Auswirkung auf die Daten: Kann zu Datenverlust oder Beschädigung führen. Der Inhalt des Speichers wird möglicherweise nicht auf die Festplatte geschrieben und kann während des Betriebs verloren gehen. IOs Skripts zum Herunterfahren könnten übersprungen werden.

Verwendungszweck: Wenn die Umgehung des ordnungsgemäßen Herunterfahrens des Betriebssystems erforderlich ist. Wenn diese Option verwendet wird, während ein standardmäßiges

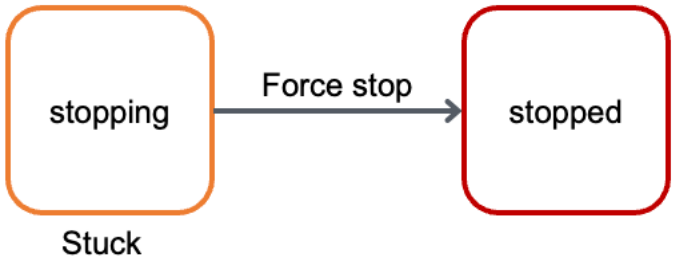
Anhalten mit ordnungsgemäßem Herunterfahren des Betriebssystems ausgeführt wird, wird das ordnungsgemäße Herunterfahren des Betriebssystems umgangen.

> **Note**
>
> Das Umgehen des ordnungsgemäßen Herunterfahrens des Betriebssystems ist für die aktuelle Statusübergangssitzung der Instance irreversibel. Bei einer nachfolgenden Standard-Anhaltung während dieser Sitzung wird nicht versucht, das Betriebssystem ordnungsgemäß herunterzufahren.

Stoppen erzwingen

Die Methode des erzwungenen Anhaltens wird verwendet, um Instances zu verarbeiten, die im Status `stopping` feststecken. Eine Instance bleibt in der Regel aufgrund eines zugrunde liegenden Hardwareproblems hängen (was durch eine fehlgeschlagene Systemstatusprüfung angezeigt wird).

Bei der Methode des erzwungenen Anhaltens wird zunächst ein standardmäßiges Anhalten versucht. Bleibt die Instance im Status `stopping` hängen, wird die Instance durch den Parameter `force` zwangsweise heruntergefahren und die Instance wird in den Status `stopped` versetzt, wie in der folgenden Abbildung dargestellt:



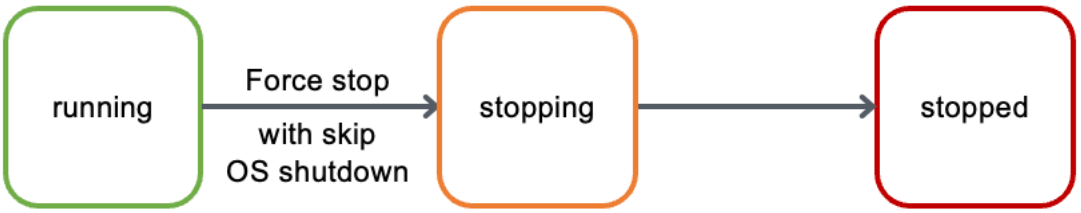
Zweck: Behandelt Instances, die im Status `stopping` feststecken. Versucht zuerst eine Standard-Anhaltung. Wenn die Instance nicht angehalten werden kann, wird die Instance zwangsweise heruntergefahren.

Auswirkung auf die Daten: Versucht zuerst eine Standard-Anhaltung, aber wenn die erzwungene Anhaltung aktiviert wird, kann dies zu Datenverlust oder Beschädigung führen. In seltenen Fällen führt dies zu Schreibvorgängen auf EBS-Volumes oder andere gemeinsam genutzte Ressourcen nach dem Anhalten.

Verwendungszweck: Zweiter Anhalteversuch, wenn eine Instance nach einer Standard-Anhaltung hängen bleibt. Weitere Informationen finden Sie unter Beheben Sie Probleme beim Anhalten von Amazon-EC2-Instances.

Erzwungenes Anhalten mit Überspringen des Herunterfahrens des Betriebssystems

Wenn eine erzwungene Anhaltung und das Umgehen des ordnungsgemäßen Herunterfahrens des Betriebssystems erforderlich ist, kann die Methode zum erzwungenen Anhalten ohne das Betriebssystem herunterzufahren verwendet werden, um eine Instance in den Status `stopped` zu versetzen, wie in der folgenden Abbildung dargestellt:



Zweck: Kombiniert das erzwungene Anhalten mit der Umgehung eines ordnungsgemäßen Herunterfahrens des Betriebssystems beim Anhalten einer Instance.

Auswirkung auf die Daten: Das Überspringen des Herunterfahrens des Betriebssystems kann zu Datenverlust oder -beschädigung führen. Der Inhalt des Speichers wird möglicherweise nicht auf die Festplatte geschrieben und kann während der Übertragung verloren gehen. IOs Skripts zum Herunterfahren könnten übersprungen werden. Wenn das erzwungene Anhalten aktiviert wird, kann dies zu zusätzlichem Datenverlust oder -beschädigung führen. In seltenen Fällen führt dies zu Schreibvorgängen auf EBS-Volumes oder andere gemeinsam genutzte Ressourcen nach dem Anhalten.

Verwendungszweck: Wenn Sie sichergehen möchten, dass Ihre Instance beendet wird und Sie das ordnungsgemäße Herunterfahren des Betriebssystems umgehen möchten. Wenn diese Option verwendet wird, während ein standardmäßiges Anhalten mit ordnungsgemäßem Herunterfahren des Betriebssystems ausgeführt wird, wird das ordnungsgemäße Herunterfahren des Betriebssystems umgangen.

Manuelles Anhalten und Starten Ihrer Instances

Sie können Ihre Amazon-EBS-gestützten Instances (Instances mit EBS-Root-Volumes) anhalten und starten. Sie können Instances mit einem Instance-Speicher-Root-Volume nicht anhalten und starten.

Wenn Sie die Standardmethode zum Anhalten einer Instance verwenden, wird versucht, das Betriebssystem ordnungsgemäß herunterzufahren. Sie können das ordnungsgemäße Herunterfahren des Betriebssystems umgehen. Dies könnte jedoch die Datenintegrität gefährden.

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Stellen Sie vor dem Anhalten einer Instance sicher, dass Sie alle benötigten Daten aus den Instance-Speicher-Volumes in den persistenten Speicher kopiert haben, z. B. Amazon EBS oder Amazon S3.

[Linux-Instances] Die Nutzung des Betriebssystembefehls halt von einer Instance aus initiiert kein Herunterfahren. Wenn Sie den Befehl halt verwenden, wird die Instance nicht angehalten. Stattdessen wird die CPU in den HLT versetzt, wodurch der CPU-Betrieb unterbrochen wird. Die Instance wird weiterhin ausgeführt.

Mit den Betriebssystembefehlen shutdown oder poweroff können Sie ein Herunterfahren einleiten. Wenn Sie einen Betriebssystembefehl verwenden, wird die Instance standardmäßig angehalten. Sie können dieses Verhalten ändern. Weitere Informationen finden Sie unter Ändern des durch die Instance initiierten Abschaltverhaltens.

> **Note**
>
> Wenn Sie eine von Amazon EBS unterstützte Instance angehalten haben und diese im `stopping`-Status „hängen bleibt“, können Sie das Anhalten erzwingen. Weitere Informationen finden Sie unter Beheben Sie Probleme beim Anhalten von Amazon-EC2-Instances.

Methoden zum Anhalten und Starten

- Eine Instance mit einem ordnungsgemäßen Herunterfahren des Betriebssystems anhalten
- Eine Instance anhalten und das ordnungsgemäße Herunterfahren des Betriebssystems umgehen
- Starten einer Instance

Eine Instance mit einem ordnungsgemäßen Herunterfahren des Betriebssystems anhalten

Sie können eine Instance mit der standardmäßigen Methode anhalten, die auch den Versuch eines ordnungsgemäßen Herunterfahrens des Betriebssystems beinhaltet. Weitere Informationen finden Sie unter Standard-Anhalten.

Console

So halten Sie eine Instance mit der Standardmethode an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich Instances und dann die Instance aus.
3. Wählen Sie Instance state (Instance-Status), Stop instance (Instance anhalten). Wenn diese Option deaktiviert ist, wurde die Instance entweder bereits angehalten oder das Root-Volume ist ein Instance-Speicher-Volume.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Stop aus. Das Anhalten der Instance kann einige Minuten dauern.

AWS CLI

So halten Sie eine Instance mit der Standardmethode an

Verwenden Sie den Befehl stop-instances.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

PowerShell

So halten Sie eine Instance mit der Standardmethode an

Verwenden Sie das Stop-EC2InstanceCmdlet

```
Stop-EC2Instance -InstanceId i-1234567890abcdef0
```

Eine Instance anhalten und das ordnungsgemäße Herunterfahren des Betriebssystems umgehen

Sie können das ordnungsgemäße Herunterfahren des Betriebssystems beim Anhalten einer Instance umgehen. Weitere Informationen finden Sie unter Anhalten mit Überspringen des Herunterfahrens des Betriebssystems.

> **Warning**
>
> Das Umgehen des ordnungsgemäßen Herunterfahrens des Betriebssystems kann zu Datenverlust oder Beschädigung führen (z. B. wenn Speicherinhalte nicht auf die Festplatte geschrieben werden oder während der Übertragung verloren gehen) oder dass Shutdown-Skripten übersprungen werden. IOs

Console

So halten Sie eine Instance an und umgehen das ordnungsgemäße Herunterfahren des Betriebssystems

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie die Instance aus.
3. Wählen Sie Instance state (Instance-Status), Stop instance (Instance anhalten).
4. Aktivieren Sie unter Herunterfahren des Betriebssystems überspringen das Kontrollkästchen Herunterfahren des Betriebssystems überspringen. Wenn diese Option nicht in der Konsole angezeigt wird, ist sie in der aktuellen Region in der Konsole noch nicht verfügbar. Sie können jedoch mit der AWS CLI oder dem SDK auf dieses Feature zugreifen oder eine andere Region in der Konsole ausprobieren.
5. Wählen Sie Beenden aus.

AWS CLI

So halten Sie eine Instance an und umgehen das ordnungsgemäße Herunterfahren des Betriebssystems

Verwenden Sie den Befehl stop-instances mit `--skip-os-shutdown`.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --skip-os-shutdown
```

PowerShell

So halten Sie eine Instance an und umgehen das ordnungsgemäße Herunterfahren des Betriebssystems

Verwenden Sie das Stop-EC2InstanceCmdlet mit. `-SkipOsShutdown $true`

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -SkipOsShutdown $true
```

Starten einer Instance

Sie können eine angehaltene Instance starten.

Console

So starten Sie eine Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. Wählen Sie die Instance und dann Instance-Status, Instance starten aus.

   Es kann einige Minuten dauern, bis die Instance in den Zustand `running` übergeht.

AWS CLI

So starten Sie eine Instance

Verwenden Sie den Befehl start-instances.

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

PowerShell

So starten Sie eine Instance

Verwenden Sie das cmdlet Start-EC2Instance.

```
Start-EC2Instance -InstanceId i-1234567890abcdef0
```

Automatisches Anhalten und Starten Ihrer Instances

Sie können das Anhalten und Starten von Instances mit den folgenden Services automatisieren:

Instance Scheduler aktiviert AWS

Sie können Instance Scheduler on verwenden AWS , um das Starten und Stoppen von EC2 Instances zu automatisieren. Weitere Informationen finden Sie unter Wie verwende ich Instance Scheduler, um Instances CloudFormation zu planen? EC2 Beachten Sie, dass zusätzliche Kosten anfallen.

AWS Lambda und eine EventBridge Amazon-Regel

Sie können Lambda und eine EventBridge Regel verwenden, um Ihre Instances nach einem Zeitplan zu beenden und zu starten. Weitere Informationen finden Sie unter Wie verwende ich Lambda, um EC2 Amazon-Instances in regelmäßigen Abständen zu beenden und zu starten?

Amazon EC2 Auto Scaling

Um sicherzustellen, dass Ihnen die richtige Anzahl von EC2 Amazon-Instances zur Verfügung steht, um die Last für eine Anwendung zu bewältigen, erstellen Sie Auto Scaling Scaling-Gruppen. Amazon EC2 Auto Scaling stellt sicher, dass Ihre Anwendung immer über die richtige Kapazität verfügt, um den Datenverkehrsbedarf zu bewältigen, und spart Kosten, indem Instances nur dann gestartet werden, wenn sie benötigt werden. Beachten Sie, dass Amazon EC2 Auto Scaling nicht benötigte Instances nicht anhält, sondern beendet. Informationen zum Einrichten von Auto Scaling-Gruppen finden Sie unter Erste Schritte mit Amazon EC2 Auto Scaling.

Alle ausgeführten und angehaltenen Instances suchen

Mit Amazon EC2 Global View finden Sie alle Ihre laufenden und gestoppten Instances AWS-Regionen auf einer einzigen Seite. Diese Funktion ist besonders nützlich für die Bestandsaufnahme und das Auffinden vergessener Instances. Informationen zur Verwendung von Global View finden Sie unter Mit AWS Global View können Sie Ressourcen regionsübergreifend anzeigen.

Alternativ können Sie in jeder Region, in der Sie Instances haben, einen Befehl oder ein cmdlet ausführen.

AWS CLI

Um die Anzahl der EC2 Instances in einer Region zu ermitteln

Verwenden Sie den folgenden describe-instances-Befehl, um die Instances in der aktuellen Region zu zählen. Sie müssen diesen Befehl in jeder Region ausführen, in der Sie Instances haben.

```
aws ec2 describe-instances \
    --region us-east-2 \
    --query "length(Reservations[].Instances[])"
```

Es folgt eine Beispielausgabe.

```
27
```

Um zusammenfassende Informationen über Ihre EC2 Instances in einer Region zu erhalten

Verwenden Sie den folgenden describe-instances-Befehl. Sie müssen diesen Befehl in jeder Region ausführen, in der Sie Instances haben.

```
aws ec2 describe-instances \
    --region us-east-2 \
    --query "Reservations[].Instances[].[InstanceId,InstanceType,PrivateIpAddress]"
 \
    --output table
```

Es folgt eine Beispielausgabe.

```
-------------------------------------------------------
|                  DescribeInstances                  |
+---------------------+---------------+----------------+
|  i-0e3e777f4362f1bf7|  t2.micro     |  10.0.12.9     |
|  i-09453945dcf1529e9|  t2.micro     |  10.0.143.213  |
|  i-08fd74f3f1595fdbd|  m7i.4xlarge  |  10.0.1.103    |
+---------------------+---------------+----------------+
```

PowerShell

Um die Anzahl der EC2 Instanzen in einer Region zu ermitteln

Verwenden Sie das cmdlet Get-EC2Instance.

```
(Get-EC2Instance -Region us-east-2).Instances.Length
```

Es folgt eine Beispielausgabe.

```
27
```

Um zusammenfassende Informationen über Ihre EC2 Instances in einer Region zu erhalten

Verwenden Sie das cmdlet Get-EC2Instance. Sie müssen diesen Befehl in jeder Region ausführen, in der Sie Instances haben.

```
(Get-EC2Instance).Instances | Select InstanceId, InstanceType, PrivateIpAddress
```

Es folgt eine Beispielausgabe.

```
InstanceId          InstanceType PrivateIpAddress
----------          ------------ ----------------
i-0e3e777f4362f1bf7 t2.micro     10.0.12.9
i-09453945dcf1529e9 t2.micro     10.0.143.213
i-08fd74f3f1595fdbd m7i.4xlarge  10.0.1.103
```

Die ersten und letzten Startzeiten finden

Wenn Sie eine Instance beschreiben, ist die Startzeit für die Instance die letzte Startzeit. Nachdem Sie eine Instance anhalten und wieder starten, entspricht sie der Startzeit der neuen Instance. Um die anfängliche Startzeit für eine Instance zu ermitteln, auch nach dem Stoppen und Starten, sehen Sie sich den Zeitpunkt an, zu dem die primäre Netzwerkschnittstelle mit der Instance verbunden wurde.

Console

So finden Sie die letzte Startzeit

Wählen Sie die Instance aus und suchen Sie auf der Registerkarte Details die Startzeit unter Instance-Details.

So finden Sie die erste Startzeit

Wählen Sie die Instance aus und suchen Sie auf der Registerkarte Netzwerk unter Netzwerkschnittstellen nach der primären Netzwerkschnittstelle (Geräteindex ist 0).

AWS CLI

So finden Sie die ersten und letzten Startzeiten

Führen Sie mithilfe des folgenden describe-instances-Befehl aus, um sowohl die erste Startzeit als auch die letzte Startzeit für die angegebene Instance anzuzeigen.

```
aws ec2 describe-instances \
    --instance-id i-1234567890abcdef0 \
    --query 'Reservations[].Instances[].
{InstanceID:InstanceId,InitialLaunch:NetworkInterfaces[0].Attachment.AttachTime,LastLaunch:L
```

Es folgt eine Beispielausgabe.

```
[
    {
        "InstanceID": "i-1234567890abcdef0",
        "InitialLaunch": "2024-04-19T00:47:08+00:00",
        "LastLaunch": "2024-05-27T06:24:06+00:00"
    }
]
```

PowerShell

So finden Sie die letzte Startzeit

Verwenden Sie das cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.LaunchTime
```

Es folgt eine Beispielausgabe.

```
Monday, May 27, 2024 6:24:06 AM
```

So finden Sie die erste Startzeit

Verwenden Sie das cmdlet Get-EC2Instance.

```
(Get-EC2Instance -
InstanceId i-1234567890abcdef0).Instances.NetworkInterfaces.Attachment.AttachTime
```

Es folgt eine Beispielausgabe.

```
Friday, April 19, 2024 12:47:08 AM
```

Aktivieren Sie den Stop-Schutz für Ihre EC2 Instances

Um zu verhindern, dass eine Instance versehentlich angehalten wird, können Sie einen Anhalte-Schutz für die Instance aktivieren. Der Stopp-Schutz schützt Ihre Instance auch vor versehentlichen Beendigungen.

Das `DisableApiStop` Attribut der EC2 `ModifyInstanceAttribute`Amazon-API steuert, ob die Instance mithilfe der EC2 Amazon-Konsole, der oder der AWS CLI EC2 Amazon-API gestoppt werden kann. Sie können den Wert dieses Attributs beim Starten der Instance festlegen, während die Instance in Betrieb oder angehalten ist.

Überlegungen

- Die Aktivierung des Stopp-Schutzes verhindert nicht, dass Sie eine Instance versehentlich stoppen, indem Sie mit einem Betriebssystembefehl wie shutdown oder poweroff ein Herunterfahren der Instance einleiten.
- Die Aktivierung des Stopp-Schutzes AWS verhindert nicht, dass die Instance gestoppt wird, wenn es ein geplantes Ereignis zum Stoppen der Instance gibt.
- Die Aktivierung des Stop-Schutzes verhindert nicht, dass Amazon EC2 Auto Scaling eine Instance beendet, wenn die Instance fehlerhaft ist oder wenn Scale-In-Ereignisse auftreten. Sie können steuern, ob eine Auto-Scaling-Gruppe eine bestimmte Instance beim Abskalieren beenden kann, indem Sie den Instance-Skalierungsschutz verwenden.
- Der Stop-Schutz verhindert nicht nur, dass Ihre Instance versehentlich gestoppt wird, sondern auch, dass Ihre Instance versehentlich beendet wird, wenn Sie die Konsole oder API verwenden. AWS CLI Es ändert jedoch nicht automatisch das `DisableApiTermination`-Attribut. Beachten Sie, dass, wenn das `DisableApiStop` Attribut auf gesetzt ist`false`, die `DisableApiTermination` Attributeinstellung bestimmt, ob die Instance mithilfe der Konsole oder der API beendet werden kann. AWS CLI Weitere Informationen finden Sie unter EC2 Amazon-Instances beenden.
- Sie können den Anhalteschutz nicht für eine Instance mit einem Instance-Speicher-Root-Volume aktivieren.
- Sie können den Stopp-Schutz nicht für Spot Instances aktivieren.
- Die EC2 Amazon-API folgt einem Konsistenzmodell, wenn Sie den Stop-Schutz aktivieren oder deaktivieren. Dies bedeutet, dass das Ergebnis der Ausführung von Befehlen zum Festlegen des Attributs Anhalte-Schutz möglicherweise nicht sofort für alle nachfolgenden Befehle, die Sie ausführen, sichtbar ist. Weitere Informationen finden Sie unter Eventual Consistency im Amazon EC2 Developer Guide.

Schutzaufgaben anhalten

- Aktivieren des Stopp-Schutzes für eine Instance beim Starten
- Aktivieren des Stopp-Schutzes für eine laufende oder gestoppte Instance
- Deaktivieren des Stopp-Schutzes für eine laufende oder angehaltene Instance

Aktivieren des Stopp-Schutzes für eine Instance beim Starten

Sie können den Anhalteschutz für eine Instance aktivieren, wenn Sie die Instance starten.

Console

So aktivieren Sie den Stopp-Schutz für eine Instance beim Starten

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf dem Dashboard Launch Instance (Instance starten) aus.
3. Konfigurieren Sie Ihre Instance im neuen Launch Instance Wizard.
4. Aktivieren Sie im Assistenten den Anhalte-Schutz, indem Sie unter Erweiterte Details die Option Aktivieren für Anhalte-Schutz auswählen.

AWS CLI

So aktivieren Sie den Stopp-Schutz für eine Instance beim Starten

Verwenden Sie den Befehl run-instances, um die Instance zu starten. Fügen Sie den folgenden Parameter hinzu.

```
--disable-api-stop
```

PowerShell

So aktivieren Sie den Stopp-Schutz für eine Instance beim Starten

Verwenden Sie das New-EC2InstanceCmdlet, um die Instance zu starten. Fügen Sie den folgenden Parameter hinzu.

```
-DisableApiStop $true
```

Aktivieren des Stopp-Schutzes für eine laufende oder gestoppte Instance

Sie können den Anhalteschutz für eine Instance aktivieren, wenn die Instance ausgeführt wird oder angehalten ist.

Console

So aktivieren Sie den Anhalteschutz für eine Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. Wählen Sie die Instance aus und wählen Sie dann Aktionen>Instance-Einstellungen>Anhalte-Schutz ändern.
4. Aktivieren Sie das Kontrollkästchen EAktivieren und wählen Sie dann Speichern aus.

AWS CLI

So aktivieren Sie den Anhalteschutz für eine Instance

Verwenden Sie den Befehl modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --disable-api-stop
```

PowerShell

So aktivieren Sie den Anhalteschutz für eine Instance

Verwenden Sie das cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -DisableApiStop $true
```

Deaktivieren des Stopp-Schutzes für eine laufende oder angehaltene Instance

Sie können den Stopp-Schutz für eine laufende oder gestoppte Instance mit einer der folgenden Methoden deaktivieren.

Console

So deaktivieren Sie den Anhalte-Schutz für eine laufende oder angehaltene Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. Wählen Sie die Instance und dann Actions (Aktionen) rechts oben, Instance Settings (Instance-Einstellungen), Change stop protection (Stopp-Schutz ändern).
4. Deaktivieren Sie das Kontrollkästchen Aktivieren und wählen Sie dann Speichern aus.

AWS CLI

So deaktivieren Sie den Anhalte-Schutz für eine laufende oder angehaltene Instance

Verwenden Sie den Befehl modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --no-disable-api-stop
```

PowerShell

So deaktivieren Sie den Anhalteschutz für eine Instance

Verwenden Sie das cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -DisableApiStop $false
```

Versetzen Sie Ihre Amazon-Instance in den Ruhezustand EC2

Wenn Sie eine Instance in den Ruhezustand versetzen, EC2 signalisiert Amazon dem Betriebssystem, den Ruhezustand durchzuführen (). suspend-to-disk Hierdurch wird der Inhalt des Instance-Arbeitsspeichers (RAM) auf dem Amazon-Elastic-Block-Store (Amazon EBS)-Stamm-Volume gespeichert. Amazon speichert das EBS-Root-Volume der Instance und alle angehängten EBS-Datenvolumes EC2 dauerhaft. Wenn Ihre Instance gestartet wird:

- Das EBS-Stamm-Volume wird in seinem vorherigen Zustand wiederhergestellt.

- Die RAM-Inhalte werden neu geladen.
- Die zuvor auf der Instance ausgeführten Prozesse werden fortgesetzt.
- Zuvor angefügte Daten-Volumes werden erneut angefügt und die Instance behält ihre Instance-ID bei.

Sie können eine Instance nur dann in den Ruhezustand versetzen, wenn sie für den Ruhezustand aktiviert ist und die Voraussetzungen für den Ruhezustand erfüllt.

Wenn das Bootstrapping und Erstellen des Arbeitsspeichers bei einer Instance sehr lange dauern, bevor sie voll produktiv ist, können Sie die Instance mithilfe des Ruhezustands vorbereiten. So bereiten Sie die Instance vor:

1. Starten Sie die Instance mit aktiviertem Ruhezustand.
2. Aktivieren Sie einen gewünschten Instance-Status.
3. Setzen Sie sie in den Ruhezustand, damit sie bereit ist, in den gewünschten Status wieder aufgenommen zu werden.

Die Instance-Nutzung für eine Instance im Ruhezustand, wenn sie sich im `stopped`-Staus befindet, oder für die Datenübertragung, wenn der Inhalt des RAM auf das EBS-Root-Volume übertragen wird, wird Ihnen nicht in Rechnung gestellt. Ihnen werden Gebühren für das Speichern aller EBS-Volumes berechnet, einschließlich für das Speichern der RAM-Inhalte.

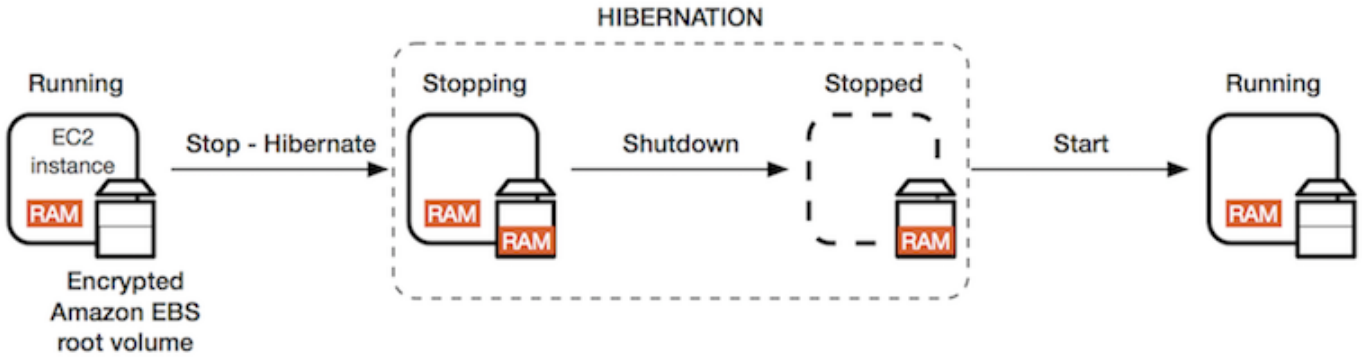
Wenn Sie eine Instance nicht mehr benötigen, können Sie sie jederzeit beenden, auch wenn sie sich im Zustand `stopped` (Ruhezustand) befindet. Weitere Informationen finden Sie unter EC2 Amazon-Instances beenden.

Inhalt

- So funktioniert der Ruhezustand von EC2 Amazon-Instances
- EC2 Voraussetzungen für den Ruhezustand der Instance
- Ein Linux-AMI zum Unterstützen des Ruhezustands konfigurieren
- Ruhezustand für eine Amazon-Instance aktivieren EC2
- Deaktivieren von KASLR auf einer Instance (nur Ubuntu)
- Eine Amazon-Instance in den Ruhezustand versetzen EC2
- Starten Sie eine Amazon-Instance im Ruhezustand EC2
- Fehlerbehebung beim Ruhezustand der EC2 Amazon-Instance

So funktioniert der Ruhezustand von EC2 Amazon-Instances

Das folgende Diagramm zeigt einen grundlegenden Überblick über den Hibernation-Prozess für Instances. EC2



Was geschieht, wenn Sie eine Instance in den Ruhezustand versetzen

Wenn Sie eine Instance in den Ruhezustand versetzen, geschieht Folgendes:

- Die Instance wechselt in den Status `stopping`. Amazon EC2 signalisiert dem Betriebssystem, den Ruhezustand auszuführen ()suspend-to-disk. Für den Ruhezustand werden alle Prozesse angehalten, der Inhalt des Instance-Arbeitsspeichers (RAM) wird auf dem EBS-Stamm-Volume gespeichert und dann wird die Instance regulär heruntergefahren.
- Nachdem die Instance vollständig heruntergefahren wurde, wechselt sie in den Zustand `stopped`.
- Alle EBS-Volumes bleiben der Instance angefügt und die Daten bleiben erhalten, auch der gespeicherte RAM-Inhalt.
- Alle EC2 Amazon-Instance-Speicher-Volumes bleiben an die Instance angehängt, aber die Daten auf den Instance-Speicher-Volumes gehen verloren.
- In den meisten Fällen wird die Instance beim Start zu einem neuen Basis-Host-Computer migriert. Dies geschieht auch, wenn Sie eine Instance anhalten und starten.
- Wenn die Instance gestartet wird, wird die Instance hochgefahren und das Betriebssystem liest den Inhalt des RAM vom EBS-Root-Volume ein, bevor es Prozesse aufhebt, um den Status wiederherzustellen.
- Die Instance behält ihre privaten IPv4 Adressen und alle IPv6 Adressen. Wenn die Instanz gestartet wird, behält die Instanz weiterhin ihre privaten IPv4 Adressen und alle IPv6 Adressen bei.
- Amazon EC2 veröffentlicht die öffentliche IPv4 Adresse. Wenn die Instance gestartet wird, EC2 weist Amazon der Instance eine neue öffentliche IPv4 Adresse zu.

- Die Instance behält die zugeordneten Elastic IP-Adressen bei. Für Elastic IP-Adressen, die einer Instance im Ruhezustand zugeordnet sind, fallen Gebühren an.

Informationen zum Unterschied zwischen Ruhezustand und Neustart, Anhalten und Beenden finden Sie unter Unterschiede zwischen Instance-Status.

Einschränkungen

- Wenn Sie eine Instance in den Ruhezustand versetzen, gehen sämtliche Daten auf allen Instance-Speicher-Volumes verloren.
- (Linux-Instances) Sie können eine Linux-Instance mit mehr als 150 GiB RAM nicht in den Ruhezustand versetzen.
- (Windows-Instances) Sie können eine Windows-Instance mit mehr als 16 GiB RAM nicht in den Ruhezustand versetzen.
- Solange sich Ihre Instance im Ruhezustand befindet, können Sie sie nicht ändern. Dies unterscheidet sich von einer angehaltenen Instance, die sich nicht im Ruhezustand befindet, bei der Sie bestimmte Attribute wie Typ oder Größe der Instance ändern.
- Wenn Sie einen Snapshot oder ein AMI aus einer Instance erstellen, die im Ruhezustand ist oder den Ruhezustand aktiviert hat, können Sie möglicherweise keine Verbindung mit einer neuen Instance herstellen, die aus dem AMI oder aus einem AMI, das aus dem Snapshot erstellt wurde, gestartet wird.
- (Nur Spot-Instances) Wenn Amazon Ihre Spot-Instance EC2 in den Ruhezustand versetzt, EC2 kann nur Amazon Ihre Instance wieder aufnehmen. Wenn Sie Ihre Spot Instance in den Ruhezustand versetzen (vom Benutzer initiierter Ruhezustand), können Sie Ihre Instance fortsetzen. Eine Spot Instance im Ruhezustand kann nur wieder aufgenommen werden, wenn Kapazität verfügbar ist und der Spot-Preis kleiner oder gleich Ihrem angegebenen Höchstpreis ist.
- Sie können eine Instance, die sich in einer Amazon EC2 Auto Scaling Scaling-Gruppe befindet oder von Amazon ECS verwendet wird, nicht in den Ruhezustand versetzen. Wenn sich Ihre Instance in einer Amazon EC2 Auto Scaling-Gruppe befindet und Sie versuchen, sie in den Ruhezustand zu versetzen, markiert der Amazon EC2 Amazon EC2 Auto Scaling-Service die gestoppte Instance als fehlerhaft und beendet sie möglicherweise und startet eine Ersatz-Instance. Weitere Informationen finden Sie unter Zustandsprüfungen für Instances in einer Amazon EC2 Auto Scaling Scaling-Gruppe im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.
- Sie können keine Instance in den Ruhezustand versetzen, die für den UEFI-Startmodus mit UEFI Secure Boot aktiviert konfiguriert ist.

- Wenn Sie eine Instance in den Ruhezustand versetzen, die in eine Kapazitätsreservierung gestartet wurde, stellt das Kapazitätsreservierung nicht sicher, dass die Instance im Ruhezustand fortgesetzt werden kann, nachdem Sie versucht haben, sie zu starten.
- Sie können eine Instance, die einen Kernel unter 5.10 verwendet, nicht in den Ruhezustand versetzen, wenn der Federal Information Processing Standard (FIPS)-Modus aktiviert ist.
- Das Aufrechterhalten des Ruhezustands einer Instance für mehr als 60 Tagse wird nicht unterstützt. Wenn der Ruhezustand länger als 60 Tage beibehalten werden soll, müssen Sie die in den Ruhezustand versetzte Instance starten, anhalten und starten.
- Unsere Plattform wird regelmäßig mit Upgrades und Sicherheits-Patches aktualisiert, was zu Konflikten mit vorhandenen Instances im Ruhezustand führen kann. Sie werden über kritische Updates benachrichtigt, für die Instances im Ruhezustand gestartet werden müssen, damit die Instance heruntergefahren oder neu gestartet werden kann, um erforderliche Upgrades und Sicherheits-Patches anzuwenden.

Überlegungen zum Ruhezustand einer Spot Instance

- Wenn Sie Ihre Spot Instance in den Ruhezustand versetzen, können Sie sie neu starten, sofern Kapazität verfügbar ist und der Spot-Preis kleiner oder gleich Ihrem angegebenen Höchstpreis ist.
- Wenn Amazon Ihre Spot-Instance in EC2 den Ruhezustand versetzt:
  - Nur Amazon EC2 kann Ihre Instance fortsetzen.
  - Amazon EC2 nimmt die Spot-Instance im Ruhezustand wieder auf, wenn Kapazität mit einem Spot-Preis verfügbar wird, der unter Ihrem angegebenen Höchstpreis liegt oder diesem entspricht.
  - Bevor Amazon Ihre Spot-Instance EC2 in den Ruhezustand versetzt, erhalten Sie zwei Minuten vor Beginn des Ruhezustands eine Unterbrechungsbenachrichtigung.

  Weitere Informationen finden Sie unter Spot-Instance-Unterbrechungen.

EC2 Voraussetzungen für den Ruhezustand der Instance

Sie können die Unterstützung für den Ruhezustand für eine On-Demand-Instance oder eine Spot-Instance aktivieren, wenn Sie sie starten. Sie können den Ruhezustand nicht auf einer vorhandenen Instance (ausgeführt oder angehalten) aktivieren. Weitere Informationen finden Sie unter Instance-Ruhezustand aktivieren.

Anforderungen zum Versetzen einer Instance in den Ruhezustand

- AWS-Regionen
- AMIs
- -Instance-Familien
- Instance-RAM-Größe
- Root-Volume-Typ
- Root-Volume-Größe
- Root-Volume-Verschlüsselung
- EBS-Volume-Typ
- Spot-Instance-Anforderungen

AWS-Regionen

Sie können den Ruhezustand für alle Instances verwenden. AWS-Regionen

AMIs

Sie müssen ein HVM-AMI verwenden, das den Ruhezustand unterstützt. Folgendes AMIs unterstützt den Ruhezustand:

Linux AMIs

AMIs für Intel- und AMD-Instance-Typen

- AL2023 AMI veröffentlicht 2023.09.20 oder später [1]
- Amazon Linux 2 AMI ab 29.08.2019
- Amazon Linux AMI 2018.03, veröffentlicht ab 16.11.2018
- CentOS Version 8 AMI [2] (Zusätzliche Konfiguration ist erforderlich)
- Fedora Version 34 oder höher AMI [2] (Zusätzliche Konfiguration ist erforderlich)
- Red Hat Enterprise Linux (RHEL) 9 AMI [2] (Zusätzliche Konfiguration ist erforderlich)
- Red Hat Enterprise Linux (RHEL) 8 AMI [2] (Zusätzliche Konfiguration ist erforderlich)
- Ubuntu 22.04.2 LTS (Jammy Jellyfish) AMI mit einer Seriennummer ab 20230303 oder höher [3]
- Ubuntu 20.04 LTS (Focal Fossa)-AMI mit einer Seriennummer ab 20210820 oder höher [3]
- Ubuntu 18.04 LTS (Bionic Beaver)-AMI mit einer Seriennummer ab 20190722.1 oder höher [3] [5]
- Ubuntu 16.04 LTS (Xenial Xerus)-AMI [3] [4] [5] (Zusätzliche Konfiguration ist erforderlich)

AMIs für Graviton-Instance-Typen

- AL2023 AMI (64-Bit-Arm) veröffentlicht 2024.07.01 oder später [1]
- Amazon-Linux-2-AMI (64 Bit Arm) ab 20.06.2024 oder höher
- Ubuntu 22.04.2 LTS (64 Bit Arm) (Jammy Jellyfish)-AMI mit einer Seriennummer ab 20240701 oder höher [3]
- Ubuntu 20.04 LTS (64-bit Arm) (Focal Fossa)-AMI mit einer Seriennummer ab 20240701 oder höher [3]

[1] Für minimales AMI AL2 023 ist eine zusätzliche Konfiguration erforderlich.

[2] Für CentOS, Fedora und Red Hat Enterprise Linux wird der Ruhezustand nur auf Nitro-basierten Instances unterstützt.

[3] Wir empfehlen, KASLR auf Instances mit Ubuntu 22.04.2 LTS (Jammy Jellyfish), Ubuntu 20.04 LTS (Focal Fossa), Ubuntu 18.04 LTS (Bionic Beaver) und Ubuntu 16.04 LTS (Xenial Xerus) zu deaktivieren. Weitere Informationen finden Sie unter Deaktivieren von KASLR auf einer Instance (nur Ubuntu).

[4] Für das Ubuntu 16.04 LTS (Xenial Xerus)-AMI wird der Ruhezustand auf `t3.nano`-Instance-Typen nicht unterstützt. Es wird kein Patch zur Verfügung gestellt, da Ubuntu (Xenial Xerus) die Unterstützung im April 2021 beendet hat. Wenn Sie `t3.nano`-Instance-Typen nutzen möchten empfehlen wir, auf Ubuntu 22.04.2 LTS (Jammy Jellyfish) AMI, Ubuntu 20.04 LTS (Focal Fossa) AMI oder Ubuntu 18.04 LTS (Bionic Beaver) AMI upzugraden.

[5] Support für Ubuntu 18.04 LTS (Bionic Beaver) und Ubuntu 16.04 LTS (Xenial Xerus) hat das Ende der Lebensdauer erreicht.

Informationen zum Konfigurieren eines eigenen AMI zum Unterstützen des Ruhezustands finden Sie unter Ein Linux-AMI zum Unterstützen des Ruhezustands konfigurieren.

Die Unterstützung für andere Versionen von Ubuntu sowie für andere Betriebssysteme folgt in Kürze.

Windows AMIs

- Windows Server 2022-AMI ab 13.09.2023
- Windows Server 2019-AMI ab 11.09.2019
- Windows Server 2016-AMI ab 11.09.2019

- Windows Server 2012 R2-AMI ab 11.09.2019
- Windows Server 2012-AMI ab 11.09.2019

-Instance-Familien

Sie müssen eine Instance-Familie verwenden, die den Ruhezustand unterstützt. Bare-Metal-Instances werden jedoch nicht unterstützt.

- Allzweck: M3, M4, M5, M5a, M5ad, M5d, M6a, M6g, M6gd, M6i, M6id, M6idn, M6in, M7a, M7g, M7gd, M7i, M7i-flex, M8a, M8g, M8gd, M8i, M8i-flex, T2, T3, T3a, T4g
- Computeroptimiert: C3, C4, C5, C5d, C6a, C6g, C6gd, C6Gn, C6i, C6id, C6in, C7a, C7g, C7gd, C7gn, C7i, C7i-Flex, C8a, C8g, C8GB, C8GD, C8gn, C8i, C8i-Flex
- Speicheroptimiert: R3, R4, R5, R5a, R5ad, R5d, R6a, R6g, R6gd, R6idn, R6in, R7a, R7g, R7gd, R7i, R7iz, R8a, R8g, R8GB, R8gd, R8gn, R8i, R8i-Flex, x2GD, X8 AEDZ
- Speicheroptimiert: I3, I3en, I4g, I7i, I7ie, I8g, I8ge, Im4gn, Is4gen

Console

So rufen Sie die Instance-Typen ab, die den Ruhezustand unterstützen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instance Types (Instance-Typen) aus.
3. Fügen Sie den Filter Unterstützung für On-Demand-Ruhezustand = wahr hinzu.
4. (Optional) Fügen Sie Filter hinzu, um den Anwendungsbereich auf bestimmte Instance-Typen von Interesse zu erweitern.

AWS CLI

So rufen Sie die Instance-Typen ab, die den Ruhezustand unterstützen

Verwenden Sie den Befehl describe-instance-types. Beachten Sie, dass die verfügbaren Instance-Typen je nach Region variieren.

```
aws ec2 describe-instance-types \
    --filters Name=hibernation-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

PowerShell

So rufen Sie die Instance-Typen ab, die den Ruhezustand unterstützen

Verwenden Sie das cmdlet Get-EC2InstanceType. Beachten Sie, dass die verfügbaren Instance-Typen je nach Region variieren.

```
(Get-EC2InstanceType `
    -Filter @{Name="hibernation-supported"; Values="true"}).InstanceType | Sort-
Object
```

Instance-RAM-Größe

Linux-Instances – müssen kleiner als 150 GB sein.

Windows-Instances – müssen kleiner oder gleich 16 GiB sein. Für den Ruhezustand einer T3- oder T3a-Windows-Instance empfehlen wir mindestens 1 GB RAM.

Root-Volume-Typ

Bei dem Root-Volume muss es sich um ein EBS-Volume handeln, nicht um ein Instance-Speicher-Volume.

Root-Volume-Größe

Das Root-Volume muss groß genug sein, um den RAM-Inhalt zu speichern und die von Ihnen erwartete Nutzung, beispielsweise das Betriebssystem oder Anwendungen, aufzunehmen. Wenn Sie den Ruhezustand aktivieren, wird beim Starten Speicherplatz auf dem Stamm-Volume zugewiesen, um den RAM zu speichern.

Root-Volume-Verschlüsselung

Das Root-Volume muss verschlüsselt werden, um den Schutz sensibler Inhalte zu gewährleisten, die sich zum Zeitpunkt des Ruhezustands im Speicher befinden. Wenn RAM-Daten auf das EBS-Stamm-Volume verschoben werden, werden sie immer verschlüsselt. Die Verschlüsselung des Stamm-Volumes wird beim Starten der Instance erzwungen.

Verwenden Sie eine der folgenden drei Optionen, um sicherzustellen, dass das Stammvolume ein verschlüsseltes EBS-Volume ist:

- EBS-Verschlüsselung standardmäßig — Sie können die EBS-Verschlüsselung standardmäßig aktivieren, um sicherzustellen, dass alle in Ihrem AWS Konto neu erstellten EBS-Volumes

verschlüsselt sind. Auf diese Weise können Sie den Ruhezustand für Ihre Instances aktivieren, ohne die Verschlüsselungsabsicht beim Instance-Start anzugeben. Weitere Informationen finden Sie unter Verschlüsselung als Standard aktivieren.

- EBS-Verschlüsselung in einem Schritt — Sie können verschlüsselte EBS-gestützte EC2 Instances von einem unverschlüsselten AMI aus starten und gleichzeitig den Ruhezustand aktivieren. Weitere Informationen finden Sie unter Verwenden der Verschlüsselung mit EBS-gestützten AMIs.
- Verschlüsseltes AMI: Sie können die EBS-Verschlüsselung unter Verwendung eines verschlüsselten AMI zum Starten Ihrer Instance aktivieren. Wenn Ihr AMI über kein verschlüsseltes Stamm-Snapshot verfügt, können Sie es auf ein neues AMI kopieren und Verschlüsselung anfordern. Weitere Informationen erhalten Sie unter Verschlüsseln eines unverschlüsselten Images während des Kopierens und Kopieren eines AMI.

EBS-Volume-Typ

Die EBS-Volumes müssen einen der folgenden EBS-Volume-Typen verwenden:

- Allzweck-SSD (`gp2` und `gp3`)
- Bereitgestellte IOPS SSD (`io1` und `io2`)

Wenn Sie einen Volume-Typ Provisioned IOPS SSD wählen, müssen Sie das EBS-Volume mit den entsprechenden IOPS bereitstellen, um eine optimale Leistung für den Ruhezustand zu erzielen. Weitere Informationen finden Sie unter Amazon-EBS-Volume-Typen im Amazon-EBS-Benutzerhandbuch.

Spot-Instance-Anforderungen

Für Spot Instances gelten folgende Anforderungen:

- Der Spot Instance-Anfrage-Typ muss `persistent` sein.
- Sie können in der Spot-Instance-Anforderung keine Startgruppe angeben.

Ein Linux-AMI zum Unterstützen des Ruhezustands konfigurieren

Das folgende Linux AMIs kann den Ruhezustand einer EC2 Amazon-Instance unterstützen, sofern Sie die in diesem Abschnitt beschriebenen zusätzlichen Konfigurationsschritte ausführen.

Zusätzliche Konfigurationsschritte sind erforderlich für:

- AL2023 Minimal AMI veröffentlicht 2023.09.20 oder später
- Mindest-AMI für Amazon Linux 2, veröffentlicht am 29.08.2019 oder später
- Amazon Linux 2 veröffentlicht vor 29.08.2019
- Amazon Linux veröffentlicht vor 16.11.2018
- CentOS Version 8 oder neuer
- Fedora Version 34 oder höher
- Red Hat Enterprise Linux 8 oder 9
- Ubuntu 20.04 (Focal Fossa) veröffentlicht vor Seriennummer 20210820
- Ubuntu 18.04 (Bionic Beaver) veröffentlicht vor Seriennummer 20190722.1
- Ubuntu 16.04 (Xenial Xerus)

Informationen zu Linux und Windows AMIs , die den Ruhezustand unterstützen und für die keine zusätzliche Konfiguration erforderlich ist, finden Sie unter. AMIs

Weitere Informationen finden Sie unter Aktualisieren von Instance-Software auf Ihrer Amazon-Linux-2-Instance.

AL2023 Minimal AMI veröffentlicht 2023.09.20 oder später

So konfigurieren Sie ein minimales AL2 023-AMI, veröffentlicht 2023.09.20 oder höher, um den Ruhezustand zu unterstützen

1. Installieren des `ec2-hibinit-agent`-Paket aus den Repositories.

```
[ec2-user ~]$ sudo dnf install ec2-hibinit-agent
```

2. Den Service neu starten.

```
[ec2-user ~]$ sudo systemctl start hibinit-agent
```

Mindest-AMI für Amazon Linux 2, veröffentlicht am 29.08.2019 oder später

So konfigurieren Sie ein Mindest-AMI für Amazon Linux 2, das 2019.08.29 oder später veröffentlicht wurde, zur Unterstützung des Ruhezustands

1. Installieren des `ec2-hibinit-agent`-Paket aus den Repositories.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

2. Den Service neu starten.

```
[ec2-user ~]$ sudo systemctl start hibinit-agent
```

Amazon Linux 2 veröffentlicht vor 29.08.2019

So konfigurieren Sie ein Amazon-Linux-2-AMI vor 29.08.2019 zum Unterstützen des Ruhezustands

1. Aktualisieren Sie den Kernel auf `4.14.138-114.102` oder höher.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installieren des `ec2-hibinit-agent`-Paket aus den Repositories.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

4. Überprüfen Sie, ob die Kernel-Version auf `4.14.138-114.102` oder höher aktualisiert wurde.

```
[ec2-user ~]$ uname -a
```

5. Halten Sie die Instance an und erstellen Sie ein AMI. Weitere Informationen finden Sie unter Ein Amazon-EBS-gestütztes AMI erstellen.

Amazon Linux veröffentlicht vor 16.11.2018

So konfigurieren Sie ein Amazon Linux-AMI, veröffentlicht vor 16.11.2018, zum Unterstützen des Ruhezustands

1. Aktualisieren Sie den Kernel auf `4.14.77-70.59` oder höher.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installieren des `ec2-hibinit-agent`-Paket aus den Repositories.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

4. Bestätigen Sie, dass die Kernel-Version auf `4.14.77-70.59` oder höher aktualisiert wurde.

```
[ec2-user ~]$ uname -a
```

5. Halten Sie die Instance an und erstellen Sie ein AMI. Weitere Informationen finden Sie unter Ein Amazon-EBS-gestütztes AMI erstellen.

CentOS Version 8 oder neuer

So konfigurieren Sie ein AMI der CentOS Version 8 oder höher zur Unterstützung des Ruhezustands

1. Aktualisieren Sie den Kernel auf `4.18.0-305.7.1.el8_4.x86_64` oder höher.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installieren Sie das EPEL-Repository (Fedora Extra Packages for Enterprise Linux).

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-
latest-8.noarch.rpm
```

3. Installieren des `ec2-hibinit-agent`-Paket aus den Repositories.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Aktivieren Sie den Ruhezustand des Agenten, um beim Booten zu starten.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

6. Bestätigen Sie, dass die Kernel-Version auf `4.18.0-305.7.1.el8_4.x86_64` oder später aktualisiert wurde.

```
[ec2-user ~]$ uname -a
```

Fedora Version 34 oder höher

So konfigurieren Sie ein AMI der Fedora Version 34 oder höher zur Unterstützung des Ruhezustands

1. Aktualisieren Sie den Kernel auf `5.12.10-300.fc34.x86_64` oder höher.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installieren des `ec2-hibinit-agent`-Paket aus den Repositories.

```
[ec2-user ~]$ sudo dnf install ec2-hibinit-agent
```

3. Aktivieren Sie den Ruhezustand des Agenten, um beim Booten zu starten.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

4. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

5. Bestätigen Sie, dass die Kernel-Version auf `5.12.10-300.fc34.x86_64` oder später aktualisiert wurde.

```
[ec2-user ~]$ uname -a
```

Red Hat Enterprise Linux 8 oder 9

So konfigurieren Sie ein AMI des Red Hat Enterprise Linux 8 oder 9 zur Unterstützung des Ruhezustands

1. Aktualisieren Sie den Kernel auf `4.18.0-305.7.1.el8_4.x86_64` oder höher.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installieren Sie das EPEL-Repository (Fedora Extra Packages for Enterprise Linux).

RHEL-Version 8:

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

RHEL-Version 9:

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

3. Installieren des `ec2-hibinit-agent`-Paket aus den Repositories.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Aktivieren Sie den Ruhezustand des Agenten, um beim Booten zu starten.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

6. Bestätigen Sie, dass die Kernel-Version auf `4.18.0-305.7.1.el8_4.x86_64` oder später aktualisiert wurde.

```
[ec2-user ~]$ uname -a
```

Ubuntu 20.04 (Focal Fossa) veröffentlicht vor Seriennummer 20210820

Ein Ubuntu 20.04 LTS (Focal Fossa)-AMI, das vor der Seriennummer 20210820 veröffentlicht wurde, für die Unterstützung der Ruhezustandsfunktion konfigurieren

1. Aktualisieren Sie das linux-aws-kernel auf `5.8.0-1038.40` oder höher und grub2 auf oder später. `2.04-1ubuntu26.13`

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt dist-upgrade
```

2. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

3. Bestätigen Sie, dass die Kernel-Version auf `5.8.0-1038.40` oder später aktualisiert wurde.

```
[ec2-user ~]$ uname -a
```

4. Bestätigen Sie, dass die grub2-Version auf `2.04-1ubuntu26.13` oder eine neuere Version aktualisiert wurde.

```
[ec2-user ~]$ dpkg --list | grep grub2-common
```

Ubuntu 18.04 (Bionic Beaver) veröffentlicht vor Seriennummer 20190722.1

So konfigurieren Sie ein Ubuntu 18.04 LTS-AMI, das vor der Seriennummer 20190722.1 veröffentlicht wurde, um den Ruhezustand zu unterstützen

1. Aktualisieren Sie den Kernel auf `4.15.0-1044` oder höher.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt dist-upgrade
```

2. Installieren des `ec2-hibinit-agent`-Paket aus den Repositories.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

4. Bestätigen Sie, dass die Kernel-Version auf `4.15.0-1044` oder später aktualisiert wurde.

```
[ec2-user ~]$ uname -a
```

Ubuntu 16.04 (Xenial Xerus)

Um Ubuntu 16.04 LTS für die Unterstützung des Ruhezustands zu konfigurieren, müssen Sie das linux-aws-hwe Kernel-Paket Version 4.15.0-1058-aws oder höher und den ec2-hibinit-Agenten installieren.

> **Important**
>
> Das Kernelpaket `linux-aws-hwe` wird von Canonical unterstützt. Die Standardunterstützung für Ubuntu 16.04 LTS endete im April 2021 und das Paket erhält keine regelmäßigen Updates mehr. Es wird jedoch zusätzliche Sicherheitsupdates erhalten, bis der erweiterte Sicherheitswartungs-Support 2024 endet. Weitere Informationen finden Sie unter Amazon EC2 Hibernation für Ubuntu 16.04 LTS, jetzt verfügbar im Canonical Ubuntu-Blog. Es wird empfohlen, auf Ubuntu 20.04 LTS (Focal Fossa)-AMI oder Ubuntu 18.04 LTS (Bionic Beaver)-AMI upzugraden.

So konfigurieren Sie ein Ubuntu 16.04 LTS AMI zur Unterstützung des Ruhezustands

1. Aktualisieren Sie den Kernel auf `4.15.0-1058-aws` oder höher.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt install linux-aws-hwe
```

2. Installieren des `ec2-hibinit-agent`-Paket aus den Repositories.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

4. Bestätigen Sie, dass die Kernel-Version auf `4.15.0-1058-aws` oder später aktualisiert wurde.

```
[ec2-user ~]$ uname -a
```

Ruhezustand für eine Amazon-Instance aktivieren EC2

Um eine Instance in den Ruhezustand zu setzen, müssen Sie sie zunächst beim Starten der Instance für den Ruhezustand aktivieren.

> **Important**
>
> Für einmal gestartete Instances kann der Ruhezustand nicht mehr aktiviert oder deaktiviert werden.

Aufgaben

- Aktivieren des Ruhezustands für On-Demand-Instances
- Aktivieren des Ruhezustands für Spot Instances
- Anzeigen, ob eine Instance für den Ruhezustand aktiviert ist

Aktivieren des Ruhezustands für On-Demand-Instances

Sie können den Ruhezustand für On-Demand-Instances aktivieren.

Console

So aktivieren Sie den Ruhezustand für eine On-Demand-Instance

1. Folgen Sie den Anweisungen zum Starten einer Instance, aber starten Sie die Instance erst, nachdem Sie die folgenden Schritte zur Aktivierung des Ruhezustands ausgeführt haben.
2. Um den Ruhezustand zu aktivieren, konfigurieren Sie die folgenden Felder im Launch Instance Wizard:

   a. Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) ein AMI aus, das den Ruhezustand unterstützt. Weitere Informationen finden Sie unter AMIs.

   b. Wählen Sie unter Instance type (Instance-Typ) einen unterstützten Instance-Typ aus. Weitere Informationen finden Sie unter -Instance-Familien.

   c. Wählen Sie unter Configure storage (Speicher konfigurieren) die Option Advanced (Erweitert) (rechts) und geben Sie die folgenden Informationen für das Root-Volume an:

      - Geben Sie unter Größe (GiB) die Größe des EBS-Stamm-Volumes ein. Das Volume muss groß genug sein, um den RAM-Inhalt zu speichern und der erwarteten Nutzung gerecht zu werden.
      - Wählen Sie unter Volume type (Volume-Typ) einen unterstützten EBS-Volume-Typ aus Allzweck-SSD (`gp2` und `gp3`) oder bereitgestellte IOPS-SSD (`io1` und `io2`).

- Wählen Sie für Encrypted (Verschlüsselt) die Option Yes (Ja) aus. Wenn Sie die Verschlüsselung in dieser AWS Region standardmäßig aktiviert haben, ist Ja ausgewählt.
- Wählen Sie für KMS key (KMS-Schlüssel) den Verschlüsselungsschlüssel für das Volume. Wenn Sie die Verschlüsselung in dieser AWS Region standardmäßig aktiviert haben, wird der Standard-Verschlüsselungsschlüssel ausgewählt.

Weitere Informationen zu den Voraussetzungen für das Stamm-Volume finden Sie unter EC2 Voraussetzungen für den Ruhezustand der Instance.

d. Erweitern Sie Advanced details (Erweiterte Details) und wählen Sie für Stop – Hibernate behavior (Stopp – Ruhezustand) die Option Enable (Aktivieren) aus.

3. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten.

AWS CLI

So aktivieren Sie den Ruhezustand für eine On-Demand-Instance

Starten Sie mit dem Befehl run-instances eine Instance. Geben Sie die EBS-Stamm-Volume-Parameter mithilfe des `--block-device-mappings file://mapping.json`-Parameters an und aktivieren Sie den Ruhezustand mithilfe des `--hibernation-options Configured=true`-Parameters.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type m5.large \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
```

Geben Sie in Folgendes a `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
```

```
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

Der Wert für `DeviceName` muss mit dem Namen des Stammgeräts übereinstimmen, der dem AMI zugeordnet ist. Um den Namen des Stammgeräts zu finden, verwenden Sie den Befehl describe-images.

```
aws ec2 describe-images --image-id ami-0abcdef1234567890
```

Wenn Sie die Verschlüsselung in dieser AWS Region standardmäßig aktiviert haben, können Sie sie weglassen`"Encrypted": true`.

PowerShell

So aktivieren Sie den Ruhezustand für eine On-Demand-Instance

Verwenden Sie den New-EC2InstanceBefehl, um eine Instance zu starten. Geben Sie das EBS-Stamm-Volume an, indem Sie zuerst die Blockgerät-Zuweisung definieren und sie dann mit dem `-BlockDeviceMappings`-Parameter dem Befehl hinzufügen. Aktivieren Sie den Ruhezustand mit dem Parameter `-HibernationOptions_Configured $true`.

```
$ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
$ebs_encrypt.DeviceName = "/dev/xvda"
$ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
$ebs_encrypt.Ebs.VolumeSize = 30
$ebs_encrypt.Ebs.VolumeType = "gp2"
$ebs_encrypt.Ebs.Encrypted = $true

New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType m5.large `
    -BlockDeviceMappings $ebs_encrypt `
    -HibernationOptions_Configured $true `
    -MinCount 1 `
    -MaxCount 1 `
    -KeyName MyKeyPair
```

Der Wert für `DeviceName` muss mit dem Namen des Stammgeräts übereinstimmen, der dem AMI zugeordnet ist. Verwenden Sie den Get-EC2ImageBefehl, um den Namen des Root-Geräts zu ermitteln.

```
Get-EC2Image -ImageId ami-0abcdef1234567890
```

Wenn Sie die Verschlüsselung in dieser AWS Region standardmäßig aktiviert haben, können Sie sie bei der Zuordnung `Encrypted = $true` von Blockgeräten weglassen.

Aktivieren des Ruhezustands für Spot Instances

Sie können den Ruhezustand für Spot Instances aktivieren. Weitere Informationen zum Ruhezustand einer Spot Instance bei einer Unterbrechung finden Sie unter Spot-Instance-Unterbrechungen.

Console

So aktivieren Sie den Ruhezustand für eine Spot Instance

1. Befolgen Sie das Verfahren zum Anfordern einer Spot Instance mithilfe des Launch Instance Wizard. Starten Sie die Instance jedoch erst, wenn Sie die folgenden Schritte zum Aktivieren des Ruhezustands ausgeführt haben.
2. Um den Ruhezustand zu aktivieren, konfigurieren Sie die folgenden Felder im Launch Instance Wizard:

   a. Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) ein AMI aus, das den Ruhezustand unterstützt. Weitere Informationen finden Sie unter AMIs.

   b. Wählen Sie unter Instance type (Instance-Typ) einen unterstützten Instance-Typ aus. Weitere Informationen finden Sie unter -Instance-Familien.

   c. Wählen Sie unter Configure storage (Speicher konfigurieren) die Option Advanced (Erweitert) (rechts) und geben Sie die folgenden Informationen für das Root-Volume an:

      - Geben Sie unter Größe (GiB) die Größe des EBS-Stamm-Volumes ein. Das Volume muss groß genug sein, um den RAM-Inhalt zu speichern und der erwarteten Nutzung gerecht zu werden.
      - Wählen Sie unter Volume type (Volume-Typ) einen unterstützten EBS-Volume-Typ aus Allzweck-SSD (`gp2` und `gp3`) oder bereitgestellte IOPS-SSD (`io1` und `io2`).

- Wählen Sie für Encrypted (Verschlüsselt) die Option Yes (Ja) aus. Wenn Sie die Verschlüsselung in dieser AWS Region standardmäßig aktiviert haben, ist Ja ausgewählt.
- Wählen Sie für KMS key (KMS-Schlüssel) den Verschlüsselungsschlüssel für das Volume. Wenn Sie die Verschlüsselung in dieser AWS Region standardmäßig aktiviert haben, wird der Standard-Verschlüsselungsschlüssel ausgewählt.

Weitere Informationen zu den Voraussetzungen für das Stamm-Volume finden Sie unter EC2 Voraussetzungen für den Ruhezustand der Instance.

d. Erweitern Sie Erweiterte Details und führen Sie zusätzlich zu den Feldern zum Konfigurieren einer Spot Instance folgende Schritte aus:

i. Wählen Sie als Anforderungstyp die Option Persistent aus.

ii. Wählen Sie für Verhalten bei Unterbrechungen die Option Ruhezustand aus. Alternativ können Sie für das Verhalten Anhalten – Ruhezustand die Option Aktivieren wählen. Beide Felder aktivieren den Ruhezustand auf Ihrer Spot Instance. Sie müssen nur eine davon konfigurieren.

3. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten.

AWS CLI

So aktivieren Sie den Ruhezustand für eine Spot Instance

Starten Sie mit dem Befehl run-instances eine Spot Instance. Geben Sie die EBS-Stamm-Volume-Parameter mithilfe des `--block-device-mappings file://mapping.json`-Parameters an und aktivieren Sie den Ruhezustand mithilfe des `--hibernation-options Configured=true`-Parameters. Der Anfrage-Typ (`SpotInstanceType`) der Spot Instance muss `persistent` sein.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c4.xlarge \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
```

```
    --key-name MyKeyPair
    --instance-market-options
        {
           "MarketType":"spot",
           "SpotOptions":{
              "MaxPrice":"1",
              "SpotInstanceType":"persistent"
            }
        }
```

Geben Sie die Parameter des EBS-Root-Volumes in `mapping.json` wie folgt an.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

Der Wert für `DeviceName` muss mit dem Namen des Stammgeräts übereinstimmen, der dem AMI zugeordnet ist. Um den Namen des Stammgeräts zu finden, verwenden Sie den Befehl describe-images.

```
aws ec2 describe-images --image-id ami-0abcdef1234567890
```

Wenn Sie die Verschlüsselung in dieser AWS Region standardmäßig aktiviert haben, können Sie sie weglassen`"Encrypted": true`.

PowerShell

So aktivieren Sie den Ruhezustand für eine Spot Instance

Verwenden Sie den New-EC2InstanceBefehl, um eine Spot-Instance anzufordern. Geben Sie das EBS-Stamm-Volume an, indem Sie zuerst die Blockgerät-Zuweisung definieren und sie dann mit dem `-BlockDeviceMappings`-Parameter dem Befehl hinzufügen. Aktivieren Sie den Ruhezustand mit dem Parameter `-HibernationOptions_Configured $true`.

```
$ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
```

```
$ebs_encrypt.DeviceName = "/dev/xvda"
$ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
$ebs_encrypt.Ebs.VolumeSize = 30
$ebs_encrypt.Ebs.VolumeType = "gp2"
$ebs_encrypt.Ebs.Encrypted = $true

New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType m5.large `
    -BlockDeviceMappings $ebs_encrypt `
    -HibernationOptions_Configured $true `
    -MinCount 1 `
    -MaxCount 1 `
    -KeyName MyKeyPair `
    -InstanceMarketOption @(
        MarketType = spot;
        SpotOptions @{
        MaxPrice = 1;
        SpotInstanceType = persistent}
    )
```

Der Wert für `DeviceName` muss mit dem Namen des Stammgeräts übereinstimmen, der dem AMI zugeordnet ist. Verwenden Sie den Get-EC2ImageBefehl, um den Namen des Root-Geräts zu ermitteln.

```
Get-EC2Image -ImageId ami-0abcdef1234567890
```

Wenn Sie die Verschlüsselung in dieser AWS Region standardmäßig aktiviert haben, können Sie sie bei der Zuordnung `Encrypted = $true` von Blockgeräten weglassen.

Anzeigen, ob eine Instance für den Ruhezustand aktiviert ist

Sie können überprüfen. ob eine Instance für den Ruhezustand aktiviert ist.

Console

So zeigen Sie an, ob eine Instance für den Ruhezustand aktiviert ist

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.

3. Wählen Sie die Instance aus und überprüfen Sie auf der Registerkarte Details im Bereich Instance-Details das Stop-Hibernate-Verhalten. Enabled (Aktiviert) gibt an, dass die Instance für den Ruhezustand aktiviert ist.

AWS CLI

So zeigen Sie an, ob eine Instance für den Ruhezustand aktiviert ist

Verwenden Sie den Befehl describe-instances und geben Sie den Parameter `--filters "Name=hibernation-options.configured,Values=true"` an, um die für den Ruhezustand aktivierten Instances zu filtern.

```
aws ec2 describe-instances \
    --filters "Name=hibernation-options.configured,Values=true"
```

Das folgende Feld in der Ausgabe gibt an, dass die Instance für den Ruhezustand aktiviert wurde.

```
"HibernationOptions": {
    "Configured": true
}
```

PowerShell

So zeigen Sie an, ob eine Instance für den Ruhezustand aktiviert ist

Verwenden Sie das Get-EC2InstanceCmdlet und filtern Sie Instances, die für den Ruhezustand aktiviert sind.

```
(Get-EC2Instance `
    -Filter @{Name="hibernation-options.configured"; Values="true"}).Instances
```

Deaktivieren von KASLR auf einer Instance (nur Ubuntu)

Um den Ruhezustand auf einer neu gestarteten Instance mit Ubuntu 16.04 LTS (Xenial Xerus), Ubuntu 18.04 LTS (Bionic Beaver) mit Seriennummer 20190722.1 oder höher oder Ubuntu 20.04 LTS (Focal Fossa) mit Seriennummer 20210820 oder höher auszuführen, raten wir dazu, KASLR (Kernel Address Space Layout Randomization) zu deaktivieren. Unter Ubuntu 16.04 LTS, Ubuntu 18.04 LTS oder Ubuntu 20.04 LTS ist KASLR standardmäßig aktiviert

KASLR ist ein standardmäßiges Linux-Kernel-Sicherheitsfeature, die Sie dabei unterstützt, Risiken und Auswirkungen noch nicht erkannter Schwachstellen des Speicherzugriffs zu reduzieren, indem der Wert der Basisadresse des Kernels randomisiert wird. Wenn KASLR aktiviert ist, besteht die Möglichkeit, dass die Instance nicht mehr gestartet wird, nachdem sie in den Ruhezustand versetzt wurde.

Weitere Informationen über KASLR finden Sie unter Ubuntu-Features.

So deaktivieren Sie KASLR auf einer Instance, die mit Ubuntu gestartet wurde

1. Stellen Sie per SSH eine Verbindung mit Ihrer Instance her. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance mit SSH.
2. Öffnen Sie die Datei `/etc/default/grub.d/50-cloudimg-settings.cfg` mit einem Editor Ihrer Wahl. Bearbeiten Sie die Zeile `GRUB_CMDLINE_LINUX_DEFAULT` so, dass die Option `nokaslr` an ihrem Ende angefügt wird wie im folgenden Beispiel veranschaulicht.

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
    nvme_core.io_timeout=4294967295 nokaslr"
   ```
3. Speichern Sie die Datei und beenden Sie den Editor.
4. Führen Sie den folgenden Befehl aus, um die Grub-Konfiguration erneut zu erstellen.

   ```
   sudo update-grub
   ```
5. Starten Sie die Instance neu.

   ```
   sudo reboot
   ```
6. Führen Sie den folgenden Befehl aus, um zu bestätigen, dass `nokaslr` hinzugefügt wurde.

   ```
   cat /proc/cmdline
   ```

   Die Befehlsausgabe sollte die Option `nokaslr` enthalten.

Eine Amazon-Instance in den Ruhezustand versetzen EC2

Sie können den Ruhezustand für eine On-Demand-Instance oder Spot Instance einleiten, wenn es sich bei der Instance um eine EBS-gestützte Instance handelt, sie für den Ruhezustand aktiviert ist

und die Voraussetzungen für den Ruhezustand erfüllt. Wenn eine Instance nicht erfolgreich in den Ruhezustand versetzt werden kann, wird sie regulär heruntergefahren.

Console

So versetzen Sie eine Instance in den Ruhezustand

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie eine Instance und dann Instance state (Instance-Status), Hibernate instance (Instance in den Ruhezustand versetzen) aus. Falls Instance in Ruhezustand versetzen deaktiviert ist, wurde die Instance entweder bereits in den Ruhezustand versetzt oder angehalten oder sie kann nicht in den Ruhezustand versetzt werden. Weitere Informationen finden Sie unter EC2 Voraussetzungen für den Ruhezustand der Instance.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Hibernate (Ruhezustand). Das Versetzen der Instance in den Ruhezustand kann einige Minuten dauern. Der Instance-Status wechselt zuerst zu Stopping (Wird angehalten) und sobald der Ruhezustand erreicht wurde, ist der Zustand Stopped (Angehalten).

AWS CLI

So versetzen Sie eine Instance in den Ruhezustand

Verwenden Sie den Befehl stop-instances und geben Sie den Parameter `--hibernate` an.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --hibernate
```

PowerShell

So versetzen Sie eine Instance in den Ruhezustand

Verwenden Sie das cmdlet Stop-EC2Instance.

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Hibernate $true
```

Sie können überprüfen, ob der Ruhezustand für eine Instance initiiert wurde.

Console

So zeigen Sie an, ob der Ruhezustand für eine Instance initiiert wurde

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und überprüfen Sie auf der Registerkarte Details im Abschnitt Instance-Details den Wert für Statusübergangsmeldung.

   Kunde. UserInitiatedHibernate: Der vom Benutzer initiierte Ruhezustand gibt an, dass Sie den Ruhezustand auf der On-Demand-Instance oder Spot-Instance initiiert haben.

AWS CLI

So zeigen Sie an, ob der Ruhezustand für eine Instance initiiert wurde

Verwenden Sie den Befehl describe-instances und geben Sie den Filter `state-reason-code` an, um die Instances anzuzeigen, bei denen der Ruhezustand initiiert wurde.

```
aws ec2 describe-instances \
    --filters "Name=state-reason-code,Values=Client.UserInitiatedHibernate"
```

Das folgende Feld in der Ausgabe gibt an, dass der Ruhezustand auf der On-Demand-Instance oder Spot Instance initiiert wurde.

```
"StateReason": {
    "Code": "Client.UserInitiatedHibernate"
}
```

PowerShell

So zeigen Sie an, ob der Ruhezustand für eine Instance initiiert wurde

Verwenden Sie das Get-EC2InstanceCmdlet und geben Sie den `state-reason-code` Filter an, um die Instances zu sehen, auf denen der Ruhezustand initiiert wurde.

```
Get-EC2Instance `
```

```
    -Filter @{Name="state-reason-code";Value="Client.UserInitiatedHibernate"}
```

Starten Sie eine Amazon-Instance im Ruhezustand EC2

Sie können eine in den Ruhezustand versetzte Instance genauso wie eine angehaltene Instance starten.

Wenn Amazon bei Spot-Instances die Instance in den EC2 Ruhezustand versetzt hat, EC2 kann sie nur von Amazon wieder aufgenommen werden. Sie können eine in den Ruhezustand versetzte Spot Instance nur dann wieder aufnehmen, wenn Sie sie in den Ruhezustand versetzt haben. Spot Instances können nur dann wieder aufgenommen werden, wenn Kapazität verfügbar ist und der Spot-Preis kleiner oder gleich Ihrem angegebenen Höchstpreis ist.

Console

So starten Sie eine in den Ruhezustand versetzte Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie eine in den Ruhezustand versetzte Instance und dann Instance state (Instance-Status), Start instance (Instance starten) aus. Es kann einige Minuten dauern, bis die Instance in den Zustand `running` übergeht. Während dieser Zeit zeigen die Statusprüfungen der Instance, dass sie sich in einem fehlerhaften Zustand befindet, bis sie gestartet wurde.

AWS CLI

So starten Sie eine in den Ruhezustand versetzte Instance

Verwenden Sie den Befehl start-instances.

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

PowerShell

So starten Sie eine in den Ruhezustand versetzte Instance

Verwenden Sie das cmdlet Start-EC2Instance.

```
Start-EC2Instance -InstanceId i-1234567890abcdef0
```

Fehlerbehebung beim Ruhezustand der EC2 Amazon-Instance

Nutzen Sie diese Informationen für die Diagnose von Problemen, die beim Versetzen einer Instance in den Ruhezustand auftreten können.

Probleme mit dem Ruhezustand

- Versetzen in den Ruhezustand direkt nach dem Starten ist nicht möglich
- Der Übergang von stopping zu stopped dauert zu lange und der Speicherzustand wird nach dem Starten nicht wiederhergestellt
- Instance "hängt" im Zustand stopping
- Spot Instance kann nicht unmittelbar nach dem Ruhezustand gestartet werden
- Fehler beim Fortsetzen von Spot Instances

Versetzen in den Ruhezustand direkt nach dem Starten ist nicht möglich

Wenn Sie eine Instance zu kurz nach dem Starten in den Ruhezustand versetzen möchten, wird eine Fehlermeldung angezeigt.

Sie müssen nach dem Starten ungefähr zwei Minuten bei Linux-Instances und ungefähr fünf Minuten bei Windows-Instances warten, bevor Sie eine Instance in den Ruhezustand versetzen.

Der Übergang von stopping zu stopped dauert zu lange und der Speicherzustand wird nach dem Starten nicht wiederhergestellt

Wenn es bei einer Instance, die in den Ruhezustand versetzt wird, zu lange dauert, um vom Zustand `stopping` in den Zustand `stopped` zu wechseln, und der Speicherzustand nach dem Starten nicht wiederhergestellt wird, kann dies ein Hinweis darauf sein, dass der Ruhezustand nicht richtig konfiguriert wurde.

Linux-Instances

Suchen Sie im Systemprotokoll der Instance nach Meldungen, die mit dem Ruhezustand in Zusammenhang stehen. Um auf das Systemprotokoll zuzugreifen, stellen Sie eine Verbindung zur Instance her oder verwenden Sie den get-console-outputBefehl. Suchen Sie die Protokollzeilen zu `hibinit-agent`. Wenn die Protokollzeilen auf einen Fehler hinweisen oder fehlen, ist höchstwahrscheinlich ein Fehler beim Konfigurieren des Ruhezustands beim Start aufgetreten.

Die folgende Fehlermeldung gibt z. B. an, dass das Stamm-Volume der Instance nicht groß genug ist: `hibinit-agent: Insufficient disk space. Cannot create setup for hibernation. Please allocate a larger root device.`

Wenn die letzte Protokollzeile von `hibinit-agent` `hibinit-agent: Running: swapoff / swap` lautet, wurde der Ruhezustand erfolgreich konfiguriert.

Wenn Sie keine Protokolle zu diesen Prozessen sehen, unterstützt das AMI möglicherweise keinen Ruhezustand. Informationen zur unterstützten Version AMIs finden Sie unter EC2 Voraussetzungen für den Ruhezustand der Instance. Wenn Sie ein eigenes Linux-AMI verwenden haben, stellen Sie sicher, dass Sie die Anleitungen unter Ein Linux-AMI zum Unterstützen des Ruhezustands konfigurieren befolgt haben.

Windows Server 2016 und höher

Suchen Sie im EC2 Startprotokoll nach Meldungen, die sich auf den Ruhezustand beziehen. Um auf das EC2 Startprotokoll zuzugreifen, stellen Sie eine Verbindung zur Instance her und öffnen Sie die `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\Ec2Launch.log` Datei in einem Texteditor. Wenn Sie EC2 Launch v2 verwenden, öffnen Sie`C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> Windows blendet Dateien und Ordner unter `C:\ProgramData` standardmäßig aus. Um EC2 Startverzeichnisse und -Dateien anzuzeigen, geben Sie den Pfad im Windows Explorer ein oder ändern Sie die Ordnereigenschaften, sodass versteckte Dateien und Ordner angezeigt werden.

Suchen Sie die Protokollzeilen zum Ruhezustand. Wenn die Protokollzeilen auf einen Fehler hinweisen oder fehlen, ist höchstwahrscheinlich ein Fehler beim Konfigurieren des Ruhezustands beim Start aufgetreten.

Die folgende Meldung weist beispielsweise darauf hin, dass der Ruhezustand nicht konfiguriert werden konnte: `Message: Failed to enable hibernation.` Wenn die Fehlermeldung ASCII-Dezimalwerte enthält, können Sie die ASCII-Werte in Klartext konvertieren, um die vollständige Fehlermeldung zu lesen.

Wenn die Protokollzeile `HibernationEnabled: true` enthält, wurde der Ruhezustand erfolgreich konfiguriert.

Windows Server 2012 R2 und früher

Suchen Sie im EC2 Konfigurationsprotokoll nach Meldungen, die sich auf den Ruhezustand beziehen. Um auf das EC2 Konfigurationsprotokoll zuzugreifen, stellen Sie eine Verbindung zur Instanz her und öffnen Sie die `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt` Datei in einem Texteditor. Suchen Sie die Protokollzeilen für `SetHibernateOnSleep`. Wenn die Protokollzeilen auf einen Fehler hinweisen oder fehlen, ist höchstwahrscheinlich ein Fehler beim Konfigurieren des Ruhezustands beim Start aufgetreten.

Die folgende Fehlermeldung gibt z. B. an, dass das Stamm-Volume der Instance nicht groß genug ist: `SetHibernateOnSleep: Failed to enable hibernation: Hibernation failed with the following error: There is not enough space on the disk.`

Wenn die Protokollzeile `SetHibernateOnSleep: HibernationEnabled: true` lautet, wurde der Ruhezustand erfolgreich konfiguriert.

Windows-Instances-Größe

Wenn Sie eine T3- oder T3a-Windows-Instance mit weniger als 1 GB RAM verwenden, erhöhen Sie die Größe der Instance auf eine, die über mindestens 1 GB RAM verfügt.

Instance "hängt" im Zustand stopping

Wenn Sie eine Instance in den Ruhezustand versetzt haben und sie im Zustand `stopping` "festhängt", können Sie das Anhalten erzwingen. Weitere Informationen finden Sie unter Beheben Sie Probleme beim Anhalten von Amazon-EC2-Instances.

Spot Instance kann nicht unmittelbar nach dem Ruhezustand gestartet werden

Wenn Sie versuchen, eine Spot Instance zu starten, die innerhalb der letzten zwei Minuten in den Ruhezustand versetzt wurde, wird möglicherweise die folgende Fehlermeldung angezeigt:

`You failed to start the Spot Instance because the associated Spot Instance request is not in an appropriate state to support start.`

Warten Sie etwa zwei Minuten für Linux-Instances und ungefähr fünf Minuten für Windows-Instances und versuchen Sie dann erneut, die Instance zu starten.

Fehler beim Fortsetzen von Spot Instances

Wenn Ihre Spot Instance erfolgreich in den Ruhezustand versetzt wurde, aber nicht fortgesetzt werden konnte und stattdessen komplett neu gestartet wurde, sodass der Ruhezustand nicht erhalten bleibt, enthielten die Benutzerdaten möglicherweise das folgende Skript:

```
/usr/bin/enable-ec2-spot-hibernation
```

Entfernen Sie dieses Skript aus dem Feld Benutzerdaten in der Startvorlage und fordern Sie dann eine neue Spot Instance an.

Hinweis: Selbst wenn die Instance nicht fortgesetzt werden konnte und der Ruhezustand nicht erhalten geblieben ist, kann die Instance auf die gleiche Weise gestartet werden wie beim Starten mit dem Zustand `stopped`.

Eine Amazon-EC2-Instance neu starten

Ein Neustart einer Instance entspricht einem Neustart des Betriebssystems. In den meisten Fällen dauert es nur wenige Minuten, um die Instance neu zu starten.

Wenn Sie eine Instance neu starten, wird Folgendes beibehalten:

- Öffentlicher DNS-Name (IPv4)
- Private IPv4-Adresse
- Öffentliche IPv4-Adresse
- IPv6-Adresse (falls zutreffend)
- Alle Daten auf den Instance-Speicher-Volumes

Mit dem erneuten Hochfahren einer Instance beginnt kein neuer Instance-Fakturierungszeitraum, im Gegensatz zum Anhalten und Starten der Instance (bei dem ein neuer Fakturierungszeitraum mit einer Mindestabrechnung von einer Minuten beginnt).

Ein Instance-Neustart kann vom Benutzer initiiert werden (wobei Sie die Instance manuell neu starten) oder von AWS (für die automatische Instance-Wiederherstellung oder als Reaktion auf ein geplantes Neustart-Ereignis für notwendige Wartungsarbeiten, z. B. um Updates zu installieren, die einen Neustart erfordern) initiiert werden.

Für benutzerinitiierte Neustarts empfehlen wir, die Amazon-EC2-Konsole, -CLI oder -API zu verwenden, anstatt den Befehl zum Neustart des Betriebssystems auf der Instance auszuführen.

Wenn Sie Amazon EC2 verwenden und die Instance nicht innerhalb weniger Minuten problemlos herunterfährt, führt Amazon EC2 einen erzwungenen Neustart durch. AWS CloudTrail erstellt außerdem einen API-Datensatz darüber, wann Ihre Instance neu gestartet wurde.

In diesem Thema wird beschrieben, wie Sie einen benutzerinitiierten Neustart durchführen. Weitere Informationen über von AWS durchgeführte Neustarts finden Sie unter Automatische Instance-Wiederherstellung und EC2 Amazon-Instances verwalten, die für den Neustart geplant sind.

> **Important**
>
> Wenn auf der Instance Updates installiert werden, wird empfohlen, die Instance nicht mithilfe der Amazon-EC2-Konsole oder der Befehlszeile neu zu starten oder herunterzufahren, solange nicht alle Updates installiert sind. Wenn Sie die Amazon EC2-Konsole oder die Befehlszeile für den Neustart oder das Herunterfahren Ihrer Instance verwenden, besteht das Risiko, dass ein "harter" Neustart Ihrer Instance ausgeführt wird. Ein solcher harter Neustart während der Installation von Updates könnte Ihre Instance in einen instabilen Zustand versetzen.

Console

So starten Sie eine Instance neu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance und anschließend die Optionen Instance State (Instance-Status) und Reboot instance (Instance neu starten) aus.
4. Wählen Sie Reboot (Neu starten) aus, wenn Sie zum Bestätigen aufgefordert werden.

   Die Instance verbleibt im Status `running` (wird ausgeführt).

AWS CLI

So starten Sie eine Instance neu

Verwenden Sie den Befehl reboot-instances.

```
aws ec2 reboot-instances --instance-ids i-1234567890abcdef0
```

PowerShell

So starten Sie eine Instance neu

Verwenden Sie das cmdlet Restart-EC2Instance.

```
Restart-EC2Instance -InstanceId i-1234567890abcdef0
```

Experiment mit Fehlersimulation ausführen

Sie können mit AWS Fault Injection Service testen, wie Ihre Anwendung reagiert, wenn Ihre Instance neu gestartet wird. Weitere Informationen finden Sie im AWS Fault Injection Service-Benutzerhandbuch.

EC2 Amazon-Instances beenden

> **Warning**
>
> Das Beenden einer Instance ist dauerhaft und irreversibel.
> Nachdem Sie eine Instance beendet haben, können Sie keine Verbindung mehr zu ihr herstellen und sie kann nicht wiederhergestellt werden. Alle angehängten Amazon-EBS-Volumes, die so konfiguriert sind, dass sie beim Beenden gelöscht werden, werden ebenfalls dauerhaft gelöscht und können nicht wiederhergestellt werden. Alle auf den Instance-Speicher-Volumes gespeicherten Daten gehen dauerhaft verloren. Weitere Informationen finden Sie unter Wie die Kündigung von Instances funktioniert.
> Bevor Sie eine Instance beenden, stellen Sie sicher, dass Sie alle Daten, die Sie nach der Beendigung behalten müssen, im persistenten Speicher gesichert haben.

Wenn Sie Ihre Instance nicht mehr benötigen, können Sie sie löschen. Dies wird als Beenden Ihrer Instance bezeichnet. Sobald der Status einer Instance zu `shutting-down` oder `terminated` wechselt, fallen für diese Instance keine Gebühren mehr an.

Sie können mit einer Instance keine Verbindung herstellen oder sie starten, nachdem Sie sie beendet haben. Sie können jedoch mit derselben AMI neue Instances starten.

Wenn Sie eine Instance lieber anhalten oder in den Ruhezustand versetzen möchten, lesen Sie Stoppen und starten Sie EC2 Amazon-Instances oder Versetzen Sie Ihre Amazon-Instance in den Ruhezustand EC2 . Weitere Informationen finden Sie unter Unterschiede zwischen Instance-Status.

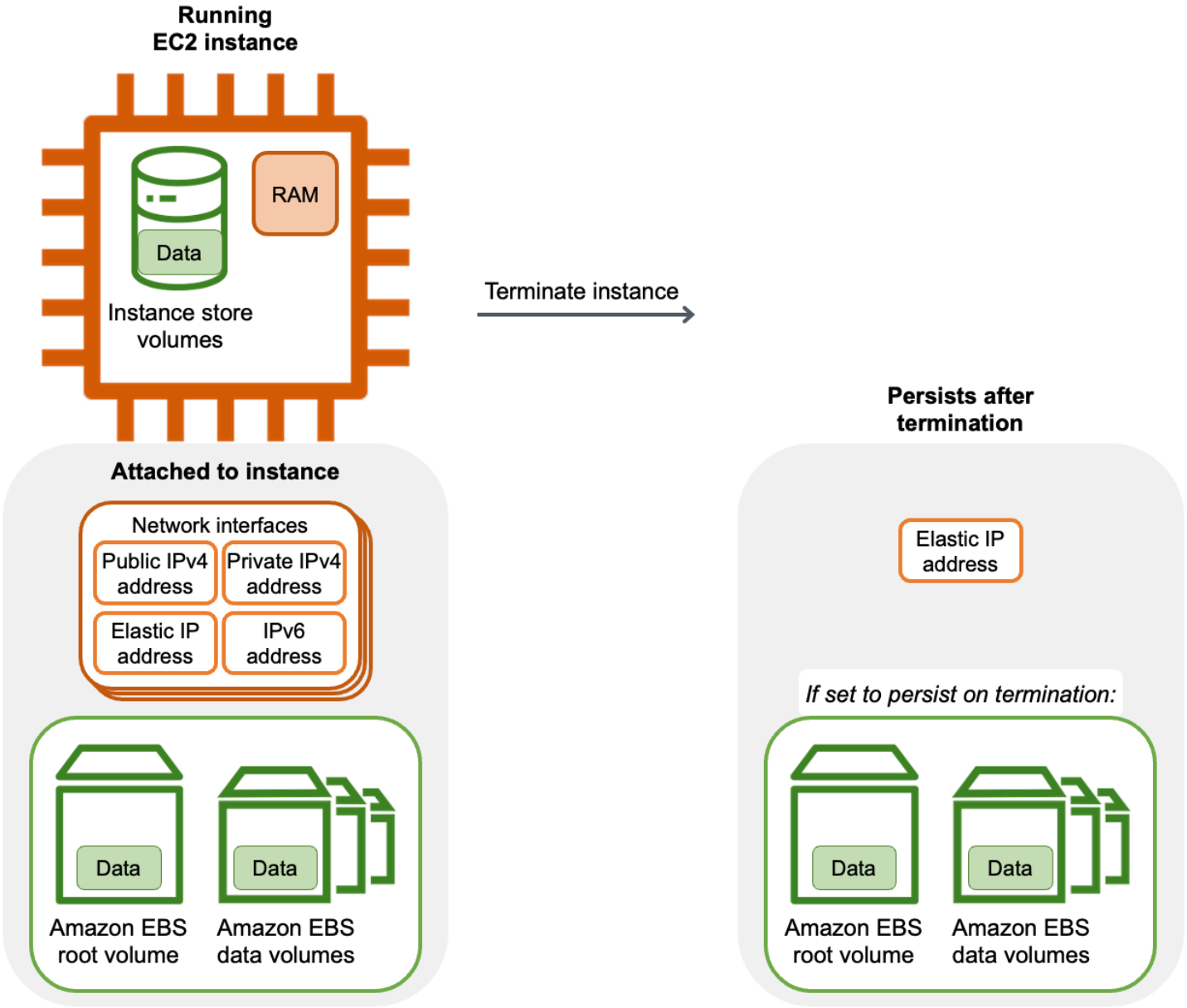
Inhalt

- Wie die Kündigung von Instances funktioniert
- Methoden zum Beenden einer Instance
- Eine Instance mit einem ordnungsgemäßen Herunterfahren des Betriebssystems beenden
- Eine Instance beenden und das ordnungsgemäße Herunterfahren des Betriebssystems umgehen
- Beheben von Problemen bei der Beendigung von Instances
- Beendigungsschutz für Instances ändern
- Ändern des durch die Instance initiierten Abschaltverhaltens
- Daten beim Beenden einer Instance aufbewahren

Wie die Kündigung von Instances funktioniert

Wenn Sie eine Instance beenden, werden Änderungen auf der Betriebssystemebene der Instance registriert, einige Ressourcen gehen verloren, andere bleiben bestehen.

Das folgende Diagramm zeigt, was verloren geht und was fortbesteht, wenn eine EC2 Amazon-Instance beendet wird. Wird eine Instance beendet, werden sämtliche Daten auf allen Instance-Speicher-Volumes und die im Instance-RAM gespeicherten Daten gelöscht. Alle mit der Instance verbundenen Elastic-IP-Adressen werden abgetrennt. Bei Root- und Daten-Volumes von Amazon EBS hängt das Ergebnis von der Einstellung Löschen bei Beendigung für das Volume ab.



Überlegungen

- Datenpersistenz
  - Instance-Speicher-Volumes: Alle Daten werden dauerhaft gelöscht, wenn die Instance beendet wird.
  - EBS-Root-Volume:
    - Wenn es beim Start angehängt wird, wird das Volume standardmäßig gelöscht, wenn die Instance beendet wird.

    - Wenn es nach dem Start angehängt wird, wird das Volume standardmäßig beibehalten, wenn die Instance beendet wird.
  - EBS-Daten-Volumes:
    - Wenn es beim Start mit der Konsole angehängt wird: standardmäßig beibehalten, wenn die Instance beendet wird.
    - Wenn es beim Start mit der CLI angehängt wird: standardmäßig gelöscht, wenn die Instance beendet wird.
    - Wenn es nach dem Start mit der Konsole oder CLI angehängt wird: standardmäßig beibehalten, wenn die Instance beendet wird.

    > **Note**
    >
    > Für alle Volumes, die beim Beenden der Instance nicht gelöscht werden, fallen weiterhin Gebühren an. Sie können die Einstellung so ändern, dass ein Volume beim Beenden der Instance gelöscht oder beibehalten wird. Weitere Informationen finden Sie unter Daten beim Beenden einer Instance aufbewahren.

- Schutz vor versehentlicher Beendigung
  - Um zu verhindern, dass Ihre Instance versehentlich beendet wird, können Sie den Beendigungsschutz aktivieren für die Instance.
  - Um zu steuern, ob eine Instance anhält oder beendet wird, wenn das Herunterfahren von der Instance initiiert wird, ändern Sie das Verhalten beim von der Instance initiierten Herunterfahren.
- Skripts zum Herunterfahren – Wenn Sie bei der Beendigung der Instance ein Skript ausführen, wird Ihre Instance möglicherweise fehlerhaft beendet, weil wir keine Möglichkeit haben, sicherzustellen, dass Skripts zum Herunterfahren ausgeführt werden. Amazon EC2 versucht, eine Instance sauber herunterzufahren und alle Skripts zum Herunterfahren des Systems auszuführen. Bestimmte Ereignisse (z. B. Hardwarefehler) können jedoch verhindern, dass diese Skripts zum Herunterfahren des Systems ausgeführt werden.
- Bare-Metal-Instances – x86-Bare-Metal-Instances unterstützen kein kooperatives Herunterfahren.

Was geschieht, wenn Sie eine Instance beenden

Auf Betriebssystemebene registrierte Änderungen

- Die API-Anfrage sendet ein Tastendruck-Ereignis an den Gast.

- Verschiedene Systemservices werden infolge des Tastendruck-Ereignisses gestoppt. Das ordnungsgemäße Herunterfahren des Systems erfolgt durch systemd (Linux) oder den Systemprozess (Windows). Ein ordnungsgemäßes Herunterfahren wird durch das ACPI-Maustastendruck-Ereignis zum Herunterfahren vom Hypervisor ausgelöst.
- Das Herunterfahren des ACPI wird initiiert.
- Die Instance wird heruntergefahren, nachdem das ordnungsgemäße Herunterfahren abgeschlossen ist. Die Zeit zum Herunterfahren des Betriebssystems kann nicht konfiguriert werden. Die Instance bleibt für eine kurze Zeit in der Konsole sichtbar, dann wird der Eintrag automatisch gelöscht.

Verlorene Ressourcen

- Auf den Instance-Speicher-Volumes gespeicherte Daten.
- EBS-Root-Volume, wenn das Attribut `DeleteOnTermination` auf `true` gesetzt ist.
- EBS-Daten-Volumes (beim Start oder danach angehängt), wenn das Attribut `DeleteOnTermination` auf `true` gesetzt ist.

Ressourcen, die fortbestehen

- EBS-Root-Volume, wenn das Attribut `DeleteOnTermination` auf `false` gesetzt ist.
- EBS-Daten-Volumes (beim Start oder danach angehängt), wenn das Attribut `DeleteOnTermination` auf `false` gesetzt ist.

Reaktion der Anwendung auf die Beendigung der Instance testen

Sie können AWS Fault Injection Service damit testen, wie Ihre Anwendung reagiert, wenn Ihre Instance beendet wird. Weitere Informationen finden Sie im AWS Fault Injection Service - Benutzerhandbuch.

Methoden zum Beenden einer Instance

> **Warning**
>
> Das Beenden einer Instance ist dauerhaft und irreversibel.
> Nachdem Sie eine Instance beendet haben, können Sie keine Verbindung mehr zu ihr herstellen und sie kann nicht wiederhergestellt werden. Alle angehängten Amazon-EBS-

Volumes, die so konfiguriert sind, dass sie beim Beenden gelöscht werden, werden ebenfalls dauerhaft gelöscht und können nicht wiederhergestellt werden. Alle auf den Instance-Speicher-Volumes gespeicherten Daten gehen dauerhaft verloren. Weitere Informationen finden Sie unter Wie die Kündigung von Instances funktioniert.
Bevor Sie eine Instance beenden, stellen Sie sicher, dass Sie alle Daten, die Sie nach der Beendigung behalten müssen, im persistenten Speicher gesichert haben.

Es gibt vier Möglichkeiten, eine vom Benutzer initiierte Instance-Beendigung durchzuführen: Standardbeendigung, Beendigung mit Überspringen des Herunterfahrens des Betriebssystems, erzwungene Beendigung und erzwungene Beendigung mit Überspringen des Herunterfahrens des Betriebssystems. Die folgende Tabelle vergleicht die wichtigsten Unterschiede zwischen den Beendigungsmethoden.

Note

Sie können eine Instance nicht beenden, wenn der Beendigungsschutz aktiviert ist. Weitere Informationen finden Sie unter Instance-Beendigungsschutz ändern.

Beendigungsmethode	Hauptzweck	Anwendungsfall	CLI-Befehl
Standardbeendigung	Normales Herunterfahren der Instance mit versuchtem ordnungsgemäßem Herunterfahren des Betriebssystems.	Typische Instance-Beendigung.	`aws ec2 terminate-instances \ --instance-id i-1234567890abcdef0`
Beendigung mit Überspringen des Herunterfahrens	Umgeht das ordnungsgemäße Herunterfahren des Betriebssystems beim Beenden einer Instance.	Wenn die Umgehung des ordnungsgemäßen Herunterfahrens des Betriebssystems erforderlich ist.	`aws ec2 terminate-instances \ --instance-id i-1234567890abcdef0 \`

Beendigungsmethode	Hauptzweck	Anwendungsfall	CLI-Befehl
des Betriebssystems			`--skip-os-shutdown`
Erzwungene Beendigung	Behandelt eingefrorene Instances. Versucht zuerst eine Standardbeendigung. Wenn die Instance nicht beendet werden kann, wird die Beendigung der Instance erzwungen.	Wenn die Instance im Status `shutting-down` feststeckt.	`aws ec2 terminate-instances \ --instance-id i-1234567890abcdef0 \ --force`
Erzwungene Beendigung mit Überspringen des Herunterfahrens des Betriebssystems	Erzwingt die Beendigung einer Instance und umgeht das ordnungsgemäße Herunterfahren des Betriebssystems.	Wenn eine erzwungene Beendigung und die Umgehung des ordnungsgemäßen Herunterfahrens des Betriebssystems erforderlich ist.	`aws ec2 terminate-instances \ --instance-id i-1234567890abcdef0 \ --force \ --skip-os-shutdown`

Anweisungen zur Verwendung der einzelnen Methoden finden Sie im Folgenden:

- Eine Instance mit einem ordnungsgemäßen Herunterfahren des Betriebssystems beenden
- Eine Instance beenden und das ordnungsgemäße Herunterfahren des Betriebssystems umgehen
- Beendigung einer Instance erzwingen

Eine Instance mit einem ordnungsgemäßen Herunterfahren des Betriebssystems beenden

Sie können eine Instance mit der standardmäßigen Beendigungsmethode beenden, die auch den Versuch eines ordnungsgemäßen Herunterfahrens des Betriebssystems beinhaltet. Weitere Informationen finden Sie unter Methoden zum Beenden einer Instance.

Console

So beenden Sie eine Instance mit der standardmäßigen Beendigungsmethode

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance und dann Instance-Status und Instance beenden (löschen) aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Beenden (löschen) aus.
5. Nachdem Sie eine Instance beendet haben, bleibt sie kurze Zeit mit dem Status `terminated` sichtbar.

   Wenn die Beendigung fehlschlägt oder wenn eine beendete Instance länger als ein paar Stunden sichtbar ist, finden Sie weitere Informationen unter Fortdauernde Anzeige einer beendeten Instance.

AWS CLI

So beenden Sie eine Instance mit der standardmäßigen Beendigungsmethode

Verwenden Sie den Befehl terminate-instances.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

PowerShell

So beenden Sie eine Instance mit der standardmäßigen Beendigungsmethode

Verwenden Sie das cmdlet Remove-EC2Instance.

```
Remove-EC2Instance -InstanceId i-1234567890abcdef0
```

Eine Instance beenden und das ordnungsgemäße Herunterfahren des Betriebssystems umgehen

Sie können das ordnungsgemäße Herunterfahren des Betriebssystems beim Beenden einer Instance umgehen. Weitere Informationen finden Sie unter Methoden zum Beenden einer Instance.

Console

So beenden Sie eine Instance und umgehen das ordnungsgemäße Herunterfahren des Betriebssystems

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance und dann Instance-Status und Instance beenden (löschen) aus.
4. Aktivieren Sie unter Herunterfahren des Betriebssystems überspringen das Kontrollkästchen Herunterfahren des Betriebssystems überspringen. Wenn diese Option nicht in der Konsole angezeigt wird, ist sie in der aktuellen Region in der Konsole noch nicht verfügbar. Sie können jedoch mit dem AWS CLI oder SDK auf diese Funktion zugreifen oder eine andere Region in der Konsole ausprobieren.
5. Wählen Sie Beenden (löschen).
6. Nachdem Sie eine Instance beendet haben, bleibt sie kurze Zeit mit dem Status `terminated` sichtbar.

   Wenn die Beendigung fehlschlägt oder wenn eine beendete Instance länger als ein paar Stunden sichtbar ist, finden Sie weitere Informationen unter Fortdauernde Anzeige einer beendeten Instance.

AWS CLI

So beenden Sie eine Instance und umgehen das ordnungsgemäße Herunterfahren des Betriebssystems

Verwenden Sie den Befehl terminate-instances mit `--skip-os-shutdown`.

```
aws ec2 terminate-instances \
    --instance-ids i-1234567890abcdef0 \
    --skip-os-shutdown
```

PowerShell

So beenden Sie eine Instance und umgehen das ordnungsgemäße Herunterfahren des Betriebssystems

Verwenden Sie das Remove-EC2InstanceCmdlet mit.. `-SkipOsShutdown $true`

```
Remove-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -SkipOsShutdown $true
```

Beheben von Problemen bei der Beendigung von Instances

Der Anforderer muss über die Berechtigung verfügen, `ec2:TerminateInstances` aufzurufen. Weitere Informationen finden Sie unter Beispielrichtlinien für die Arbeit mit Instances.

Wenn Sie Ihre Instance beenden und eine andere Instance gestartet wird, haben Sie höchstwahrscheinlich die automatische Skalierung über eine Funktion wie EC2 Fleet oder Amazon EC2 Auto Scaling konfiguriert. Weitere Informationen finden Sie unter Instances automatisch gestartet oder beendet.

> **Note**
>
> Sie können eine Instance nicht beenden, wenn der Beendigungsschutz aktiviert ist. Weitere Informationen finden Sie unter Instance-Beendigungsschutz ändern.

Wenn Ihre Instance länger als gewöhnlich im Status `shutting-down` bleibt, können Sie versuchen, die Beendigung zu erzwingen. Wenn es in diesem `shutting-down` Zustand bleibt, sollte es durch automatisierte Prozesse innerhalb des EC2 Amazon-Service bereinigt (beendet) werden. Weitere Informationen finden Sie unter Verzögertes Beenden einer Instance.

Beendigungsschutz für Instances ändern

Um zu verhindern, dass Ihre Instance versehentlich mithilfe der EC2 Amazon-API beendet wird, unabhängig davon, ob Sie sie `TerminateInstances` direkt aufrufen oder eine andere Schnittstelle wie die EC2 Amazon-Konsole verwenden, aktivieren Sie den Kündigungsschutz für die Instance. Das Attribut `DisableApiTermination` steuert, ob die Instance beendet werden kann. Standardmäßig

ist der Beendigungsschutz für Ihre Instance deaktiviert. Sie können den Wert dieses Attributs beim Starten der Instance festlegen, oder während die Instance in Betrieb oder angehalten ist.

Das Attribut `DisableApiTermination` hindert Sie nicht daran, eine Instance zu beenden, indem Sie das Herunterfahren der Instance einleiten (z. B. mithilfe eines Betriebssystembefehls zum Herunterfahren des Systems), wenn das Attribut `InstanceInitiatedShutdownBehavior` auf `terminate` festgelegt ist. Weitere Informationen finden Sie unter Ändern des durch die Instance initiierten Abschaltverhaltens.

Überlegungen

- Die Aktivierung des Kündigungsschutzes AWS verhindert nicht, dass die Instance beendet wird, wenn ein geplantes Ereignis zum Beenden der Instance stattfindet.
- Die Aktivierung des Kündigungsschutzes verhindert nicht, dass Amazon EC2 Auto Scaling eine Instance beendet, wenn die Instance defekt ist oder wenn Scale-In-Ereignisse auftreten. Sie können steuern, ob eine Amazon EC2 Auto Scaling Scaling-Gruppe eine bestimmte Instance beenden kann, wenn sie mithilfe des Instance Scale-In-Schutzes skaliert. Sie können steuern, ob eine Amazon EC2 Auto Scaling Scaling-Gruppe fehlerhafte Instances beenden kann, indem Sie den ReplaceUnhealthy Skalierungsprozess unterbrechen.
- Sie können für Spot Instances keinen Beendigungsschutz aktivieren.

Console

So aktivieren Sie den Beendigungsschutz für eine Instance beim Start

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf dem Dashboard Launch Instance (Instance starten) aus.
3. Erweitern Sie Advanced Details (Erweiterte Details). Wählen Sie für Beendigungsschutz die Option Aktivieren aus.
4. Wenn Sie mit der Angabe der Details für Ihre Instance fertig sind, wählen Sie Instance starten aus.

So ändern Sie den Beendigungsschutz für eine Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.

4. Wählen Sie Aktionen, Instance-Einstellungen, Beendigungsschutz ändern.
5. Wählen Sie für Beendigungsschutz die Option Aktivieren, bzw. heben Sie sie auf.
6. Wählen Sie Speichern.

AWS CLI

So aktivieren Sie den Beendigungsschutz für eine Instance

Verwenden Sie den Befehl modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --disable-api-termination
```

So deaktivieren Sie den Beendigungsschutz für eine Instance

Verwenden Sie den Befehl modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --no-disable-api-termination
```

PowerShell

So aktivieren Sie den Beendigungsschutz für eine Instance

Verwenden Sie das cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -DisableApiTermination $true
```

So deaktivieren Sie den Beendigungsschutz für eine Instance

Verwenden Sie das cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -DisableApiTermination $false
```

Mehrere Instances mit Beendigungsschutz beenden

Wenn Sie mehrere Instances in mehreren Availability Zones beenden und eine oder mehrere der angegebenen Instances für den Kündigungsschutz aktiviert sind, schlägt die Anforderung mit den folgenden Ergebnissen fehl:

- Die angegebenen Instances, die sich in derselben Availability Zone wie die geschützte Instance befinden, werden nicht beendet.
- Die angegebenen Instances, die sich in verschiedenen Availability Zones befinden, in denen keine anderen angegebenen Instances geschützt sind, werden erfolgreich beendet.

Beispiel

Angenommen, Sie haben die folgenden vier Instances in zwei Availability Zones.

Instance	Availability Zone	Beendigungsschutz
Instance 1	AZ A	`Disabled`
Instance 2		`Disabled`
Instance 3	AZ B	`Enabled`
Instance 4		`Disabled`

Wenn Sie versuchen, alle diese Instances in derselben Anforderung zu beenden, meldet die Anforderung einen Fehler mit den folgenden Ergebnissen:

- Instance 1 und Instance 2 wurden erfolgreich beendet, da keine der angegebenen Instances für den Beendigungsschutz aktiviert ist.
- Instance 3 und Instance 4 wurden nicht beendet, weil Instance 3 für den Beendigungsschutz aktiviert ist.

Ändern des durch die Instance initiierten Abschaltverhaltens

> **Warning**
>
> Das Beenden einer Instance ist dauerhaft und irreversibel.

Nachdem Sie eine Instance beendet haben, können Sie keine Verbindung mehr zu ihr herstellen und sie kann nicht wiederhergestellt werden. Alle angehängten Amazon-EBS-Volumes, die so konfiguriert sind, dass sie beim Beenden gelöscht werden, werden ebenfalls dauerhaft gelöscht und können nicht wiederhergestellt werden. Alle auf den Instance-Speicher-Volumes gespeicherten Daten gehen dauerhaft verloren. Weitere Informationen finden Sie unter Wie die Kündigung von Instances funktioniert.
Bevor Sie eine Instance beenden, stellen Sie sicher, dass Sie alle Daten, die Sie nach der Beendigung behalten müssen, im persistenten Speicher gesichert haben.

Standardmäßig wird die Instance angehalten, wenn Sie ein Herunterfahren von einer Amazon-EBS-gesicherten Instance initiieren (z. B. mit den Befehlen shutdown oder poweroff). Durch das Ändern von Attribut `InstanceInitiatedShutdownBehavior` können Sie dieses Verhalten für die Instance ändern, sodass sie anstatt dessen angehalten wird. Sie können dieses Attribut aktualisieren, während die Instance läuft oder angehalten ist.

Mit dem Befehl halt wird kein Herunterfahren initiiert. Wenn er verwendet wird, wird die Instance nicht beendet; stattdessen wird die CPU in `HLT` platziert und die Instance wird weiterhin ausgeführt.

Note

Das `InstanceInitiatedShutdownBehavior`-Attribut wird nur verwendet, wenn Sie das Betriebssystem der Instance selbst herunterfahren. Sie gilt nicht, wenn Sie eine Instance über die `StopInstances` API oder die EC2 Amazon-Konsole beenden.

Console

Ändern des durch die Instance initiierten Abschaltverhaltens

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.
4. Wählen Sie Aktionen, Instance-Einstellungen, Verhalten beim Herunterfahren ändern.

   Unter Verhalten beim Herunterfahren wird das aktuelle Verhalten angezeigt.
5. Um das Verhalten zu ändern, wählen Sie Anhalten oder Beenden unter Beendigungsverhalten aus.

6. Wählen Sie Speichern.

AWS CLI

Ändern des durch die Instance initiierten Abschaltverhaltens

Verwenden Sie den Befehl modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --instance-initiated-shutdown-behavior terminate
```

PowerShell

Ändern des durch die Instance initiierten Abschaltverhaltens

Verwenden Sie das cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -InstanceInitiatedShutdownBehavior terminate
```

Daten beim Beenden einer Instance aufbewahren

Wenn eine EC2 Amazon-Instance beendet wird, können Sie die Daten auf Ihren Instance-Speicher-Volumes oder Amazon EBS-Volumes beibehalten. In diesem Thema wird erläutert, wie Sie sicherstellen, dass Ihre Daten auch nach der Instance-Beendigung beibehalten werden.

Wie sich die Beendigung einer Instance auf Root- und Daten-Volumes auswirkt

Instance-Speicher-Volumes

Wenn eine Instance beendet wird, werden die Instance-Speicher-Volumes automatisch gelöscht und die Daten gehen verloren. Um diese Daten über die Lebensdauer der Instance hinaus zu erhalten, müssen Sie diese Daten manuell in einen persistenteren Speicher kopieren, z. B. ein Amazon-EBS-Volume, einen Amazon-S3-Bucket oder ein Amazon-EFS-Dateisystem, bevor Sie die Instance beenden. Weitere Informationen finden Sie unter Speicheroptionen für Ihre Amazon-EC2-Instances.

Amazon EBS-Volumes

Wenn eine Instance beendet wird, werden die EBS-Volumes entweder gelöscht oder beibehalten, abhängig vom Wert des Attributs `DeleteOnTermination` für jedes Volume:

- Ja (Konsole) / `true` (CLI) – Das Volume wird gelöscht, wenn die Instance beendet wird.
- Nein (Konsole) / `false` (CLI) – Das Volume wird beibehalten, wenn die Instance beendet wird. Für beibehaltene Volumes fallen weiterhin Gebühren an.

> **Note**
>
> Nach dem Beenden einer Instance können Sie einen Snapshot des beibehaltenen Volume erstellen oder es an eine andere Instance anhängen. Sie müssen das Volume löschen, damit keine weiteren Gebühren anfallen.

Standardverhalten beim Löschen von EBS-Volumes

Der Standardwert `DeleteOnTermination` ist je nach Volumetyp unterschiedlich, je nachdem, ob das Volume beim Start oder danach angehängt wurde, und mit welcher Methode (Konsole oder CLI) das Volume angehängt wurde:

Volume-Typ	Wann angehängt	Methode zum Anhängen	Standardverhalten beim Beenden der Instance
Root-Volume	Beim Start	Konsole oder CLI	Delete
Root-Volume	Nach dem Starten	Konsole oder CLI	Beibehalten
Daten-Volume	Beim Start	Konsole	Beibehalten
Daten-Volume	Beim Start	CLI	Delete
Daten-Volume	Nach dem Starten	Konsole und CLI	Beibehalten

Einstellungen für die Beibehaltung des Volumes überprüfen

Der Standardwert beim Start für ein EBS-Volume wird durch das auf dem AMI festgelegte Attribut `DeleteOnTermination` bestimmt. Sie können den Wert beim Start der Instance ändern und

so die AMI-Einstellung überschreiben. Wir empfehlen, die Standardeinstellung für das Attribut `DeleteOnTermination` zu überprüfen, nachdem Sie eine Instance gestartet haben.

So überprüfen Sie, ob ein Amazon-EBS-Volume beim Beenden der Instance gelöscht wird

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.
4. Wählen Sie die Registerkarte Speicher.
5. Scrollen Sie unter Blockgeräte nach rechts, um die Spalte Bei Beendigung löschen zu überprüfen.
   - Falls Ja wird das Volume gelöscht, wenn die Instance beendet wird.
   - Falls Nein wird das Volume nicht gelöscht, wenn die Instance beendet wird. Für alle nicht gelöschten Volumes fallen weiterhin Gebühren an.

Das Root-Volume so ändern, dass es beim Start bestehen bleibt

Sie können beim Starten einer Instance das Attribut `DeleteOnTermination` eines EBS-Root-Volumes ändern. Sie können auch das folgende Verfahren für ein Daten-Volume verwenden.

Console

So ändern Sie das Root-Volume einer beizubehaltenden Instance beim Start

1. Folgen Sie den Anweisungen zum Starten einer Instance, aber starten Sie die Instance erst, nachdem Sie die folgenden Schritte durchgeführt haben, um das Root-Volume in persistent zu ändern.
2. Wählen Sie im Bereich Speicher konfigurieren die Option Erweitert aus.
3. Erweitern Sie unter EBS-Volumes die Informationen unter dem Root-Volume.
4. Für Beim Beenden löschen wählen Sie Nein aus.
5. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten.

AWS CLI

So ändern Sie das Root-Volume einer beizubehaltenden Instance beim Start

Verwenden Sie den Befehl run-instances, um den Wert von `DeleteOnTermination` in der Blockgerät-Zuweisung zu ändern.

Fügen Sie die Option `--block-device-mappings` hinzu:

```
--block-device-mappings file://mapping.json
```

Geben Sie für `mapping.json` den Gerätenamen an, z. B. `/dev/sda1` oder `/dev/xvda`, und für `DeleteOnTermination` geben Sie `false` an.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

PowerShell

So ändern Sie das Root-Volume einer beizubehaltenden Instance beim Start

Verwenden Sie das New-EC2InstanceCmdlet, um den Wert von `DeleteOnTermination` in der Blockgerätezuordnung zu ändern.

Fügen Sie die Option `-BlockDeviceMapping` hinzu:

```
-BlockDeviceMapping $bdm
```

Geben Sie für `bdm` den Gerätenamen an, z. B. `/dev/sda1` oder `/dev/xvda`, und für `DeleteOnTermination` geben Sie `false` an.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.DeleteOnTermination = false
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "/dev/sda1"
$bdm.Ebs = $ebd
```

Ändern des Root-Volumes einer laufenden Instance, damit es bestehen bleibt

Sie können das Root-Volume einer laufenden Instance ändern, damit es beibehalten wird Sie können auch das folgende Verfahren für ein Daten-Volume verwenden.

AWS CLI

So ändern Sie das beizubehaltenden Root-Volume

Verwenden Sie den Befehl modify-instance-attribute.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0  \
    --block-device-mappings file://mapping.json
```

Geben Sie für `mapping.json` den Gerätenamen an, z. B. `/dev/sda1` oder `/dev/xvda`, und für `--DeleteOnTermination` geben Sie `false` an.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

PowerShell

So ändern Sie das beizubehaltenden Root-Volume

Verwenden Sie das cmdlet Edit-EC2InstanceAttribute.

Fügen Sie die Option `-BlockDeviceMapping` hinzu:

```
-BlockDeviceMapping $bdm
```

Geben Sie für `bdm` den Gerätenamen an, z. B. `/dev/sda1` oder `/dev/xvda`, und für `DeleteOnTermination` geben Sie `false` an.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.DeleteOnTermination = false
```

```
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "/dev/sda1"
$bdm.Ebs = $ebd
```

Ausmusterung einer Instance

Eine Instance wird planmäßig ausgemustert, wenn AWS einen irreparablen Fehler der zugrunde liegenden Hardware feststellt, auf der die Instance gehostet wird. Der Typ des Instance-Root-Volumes bestimmt das Verhalten bei der Außerbetriebnahme der Instance:

- Wenn das Root-Volume der Instance ein Amazon-EBS-Volume ist, wird die Instance angehalten und Sie können sie jederzeit neu starten. Durch das Starten einer gestoppten Instance wird diese auf eine neue Hardware migriert.
- Wenn das Root-Volume der Instance ein Instance-Speicher-Volume ist, wird die Instance beendet und kann nicht weiter verwendet werden.

Weitere Informationen zu den Instance-Ereignistypen finden Sie unter Geplante Ereignisse für EC2 Amazon-Instances.

Inhalt

- Ermitteln von Instances, die zur Ausmusterung vorgesehen sind
- Durchzuführende Maßnahmen für EBS-gestützte Instances, die ausgemustert werden sollen
- Zu ergreifende Maßnahmen für vom Instance-Speicher gestützte Instances, die ausgemustert werden sollen

Ermitteln von Instances, die zur Ausmusterung vorgesehen sind

Wenn Ihre Instance ausgemustert werden soll, erhalten Sie vor dem Ereignis eine E-Mail mit der Instance-ID und dem Ausmusterungsdatum. Sie können auch überprüfen, ob Instances vorhanden sind, die zur Außerbetriebnahme vorgesehen sind.

> **Important**
>
> Wenn für eine Instance die Außerbetriebnahme geplant ist, empfehlen wir Ihnen, so schnell wie möglich zu handeln, da die Instance möglicherweise bereits nicht erreichbar ist. Weitere Informationen finden Sie unter Check if your instance is reachable.

Optionen zum Ermitteln von Instances, die zur Außerbetriebnahme vorgesehen sind

- Die E-Mail für die Kontokontakte überwachen
- Ihre Instances überprüfen

Die E-Mail für die Kontokontakte überwachen

Wenn für eine Instance die Außerbetriebnahme geplant ist, erhalten die Hauptkontaktperson für das Konto und die Betriebs-Kontaktperson vor dem Ereignis eine E-Mail. Diese E-Mail enthält die Instance-ID und das geplante Datum der Außerbetriebnahme. Weitere Informationen finden Sie unter Aktualisieren der Hauptkontaktperson für Ihr AWS-Konto und Aktualisieren der alternativen Kontaktpersonen für Ihr AWS-Konto im Referenzhandbuch für AWS -Kontenverwaltung.

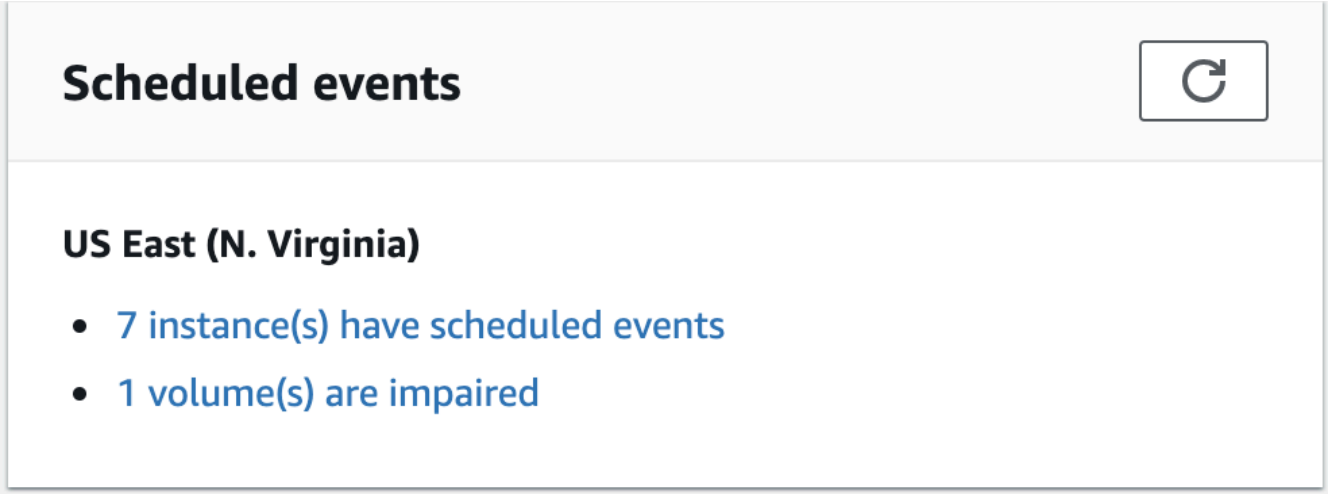
Ihre Instances überprüfen

Wenn Sie ein E-Mail-Konto verwenden, auf das Sie nicht regelmäßig zugreifen, verpassen Sie möglicherweise eine Benachrichtigung zur Außerbetriebnahme einer Instance. Sie können jederzeit überprüfen, ob für eine Ihrer Instances die Außerbetriebnahme geplant ist.

Console

So ermitteln Sie Instances, die zur Außerbetriebnahme vorgesehen sind

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich EC2 Dashboard (EC2-Dashboard) aus. Unter Geplante Ereignisse werden die Ereignisse angezeigt, die Ihren Amazon EC2-Instances und -Volumes zugeordnet sind, sortiert nach Region.



3. Wenn eine Ihrer Instances mit einem geplanten Ereignis aufgeführt wird, klicken Sie auf den Link unter dem Namen der Region, um die Seite Events (Ereignisse) aufzurufen.
4. Auf der Seite Ereignisse werden alle Ressourcen aufgeführt, denen Ereignisse zugeordnet sind. Sie können die Instances, die ausgemustert werden sollen, anzeigen, indem Sie in der ersten Filterliste Instance resources (Instance-Ressourcen) und in der zweiten Filterliste Instance stop or retirement (Stoppen oder Ausmustern einer Instance) auswählen.
5. Wenn in den Filterergebnissen eine Instance angezeigt wird, die ausgemustert werden soll, wählen Sie sie aus und notieren Sie sich das Datum und die Uhrzeit, die im Feld Start time (Startzeit) im Detailbereich angezeigt wird. Das ist das Datum für die Ausmusterung Ihrer Instance.

AWS CLI

So suchen Sie Instances, die zur Außerbetriebnahme vorgesehen sind

Verwenden Sie den Befehl describe-instance-status. Wiederholen Sie den Vorgang in jeder Region, in der Instances ausgeführt werden.

```
aws ec2 describe-instance-status --filters Name=event.code,Values=instance-
retirement
```

PowerShell

So suchen Sie Instances, die zur Außerbetriebnahme vorgesehen sind

Verwenden Sie das cmdlet Get-EC2InstanceStatus. Wiederholen Sie den Vorgang in jeder Region, in der Instances ausgeführt werden.

```
Get-EC2InstanceStatus -Filter @{Name="event.code"; Values="instance-retirement"}
```

Durchzuführende Maßnahmen für EBS-gestützte Instances, die ausgemustert werden sollen

Um die Daten in der zurückgezogenen Instance beizubehalten, können Sie eine der folgenden Aktionen ausführen. Sie sollten diese Aktion unbedingt vor dem Datum für die Ausmusterung Ihrer Instance ausführen, um unerwartete Ausfallzeiten und Datenverlust zu vermeiden.

Wenn Sie bei Linux-Intances nicht sicher sind, ob Ihre Instance durch EBS oder Instance-Speicher unterstützt wird ist, siehe Root-Volumes für Ihre Amazon-EC2-Instances.

Überprüfen, ob Ihre Instance erreichbar ist

Wenn Sie benachrichtigt werden, dass Ihre Instance ausgemustert werden soll, empfiehlt es sich, so schnell wie möglich die folgenden Maßnahmen zu ergreifen:

- Überprüfen Sie, ob Ihre Instance erreichbar ist, indem Sie eine Verbindung zu Ihrer Instance herstellen oder an diese einen Ping senden.
- Wenn Ihre Instance erreichbar ist, sollten Sie planen, Ihre Instance zu einem geeigneten Zeitpunkt vor dem geplanten Ausmusterungsdatum zu stoppen/zu starten, wenn die Auswirkung minimal ist. Weitere Informationen zum Stoppen und Starten Ihrer Instance und darüber, was zu erwarten ist, wenn die Instance gestoppt wird (z. B. die Auswirkungen auf öffentliche, private und Elastic IP-Adressen, die Ihrer Instance zugeordnet sind) finden Sie unter Stoppen und starten Sie EC2 Amazon-Instances. Beachten Sie, dass Daten auf Instance-Speicher-Volumes verloren gehen, wenn Sie die Instance stoppen und starten.
- Wenn Ihre Instance nicht erreichbar ist, sollten Sie sofort Maßnahmen ergreifen und einen Stop/Start durchführen, um Ihre Instance wiederherzustellen.
- Wenn Sie Ihre Instance beenden möchten, planen Sie dies auch so schnell wie möglich, damit keine weiteren Gebühren für die Instance anfallen.

Erstellen eines Backup Ihrer Instance

Erstellen Sie aus Ihrer Instance ein EBS-unterstütztes AMI, damit Sie ein Backup haben. Um die Datenintegrität zu gewährleisten, beenden Sie die Instance, bevor Sie das AMI erstellen. Sie können bis zum Datum für die geplante Ausmusterung warten, an dem die Instance gestoppt wird oder die Instance vorher selbst stoppen. Sie können die Instance jederzeit neu starten. Weitere Informationen finden Sie unter Ein Amazon-EBS-gestütztes AMI erstellen.

Starten einer Ersatz-Instance

Nachdem Sie ein AMI von Ihrer Instance erstellt haben, können Sie das AMI verwenden, um eine Ersatz-Instance zu starten. Wählen Sie in der Amazon EC2-Konsole Ihr neues AMI aus und wählen Sie dann Instance von AMI starten. Konfigurieren Sie die Parameter für Ihre Instance und wählen Sie dann Instance starten. Weitere Informationen zu den jeweiligen Feldern finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten.

Zu ergreifende Maßnahmen für vom Instance-Speicher gestützte Instances, die ausgemustert werden sollen

Um die Daten in der zurückgezogenen Instance beizubehalten, können Sie eine der folgenden Aktionen ausführen. Sie sollten diese Aktion unbedingt vor dem Datum für die Ausmusterung Ihrer Instance ausführen, um unerwartete Ausfallzeiten und Datenverlust zu vermeiden.

> **Warning**
>
> Wenn die Instance ein Instance-Speicher-Root-Volume hat und das Datum der Außerbetriebnahme überschritten wird, wird die Instance beendet und Sie können sie (oder die darin gespeicherten Daten) nicht mehr wiederherstellen. Unabhängig von dem Root-Volume-Typ der Instance gehen die Daten auf Instance-Speicher-Volumes immer verloren, wenn die Instance außer Betrieb genommen wird, auch wenn die Volumes einer Instance mit einem EBS-Root-Volume angefügt sind.

Überprüfen Sie, ob Ihre Instance erreichbar ist

Wenn Sie benachrichtigt werden, dass Ihre Instance ausgemustert werden soll, empfiehlt es sich, so schnell wie möglich die folgenden Maßnahmen zu ergreifen:

- Überprüfen Sie, ob Ihre Instance erreichbar ist, indem Sie eine Verbindung zu Ihrer Instance herstellen oder an diese einen Ping senden.
- Wenn Ihre Instance nicht erreichbar ist, kann wahrscheinlich nur sehr wenig getan werden, um Ihre Instance wiederherzustellen. Weitere Informationen finden Sie unter Problembehandlung bei unerreichbaren Amazon-EC2-Instances. AWS beendet Ihre Instance zum geplanten Ausmusterungsdatum. Daher können Sie bei einer nicht erreichbaren Instance die Instance sofort selbst beenden.

Starten einer Ersatz-Instance

Erstellen Sie mithilfe der AMI-Tools, wie unter Ein Amazon-S3-gestütztes AMI erstellen beschrieben, ein von Amazon S3 gestütztes AMI aus der Instance. Wählen Sie in der Amazon EC2-Konsole Ihr neues AMI aus und wählen Sie dann Instance von AMI starten. Konfigurieren Sie die Parameter für Ihre Instance und wählen Sie dann Instance starten. Weitere Informationen zu den jeweiligen Feldern finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten.

Konvertieren der Instance in eine EBS-gestützte Instance

Übertragen Sie Ihre Daten auf ein EBS-Volume, machen Sie einen Snapshot des Volumes und erstellen Sie dann ein AMI von dem Snapshot. Sie können eine Ersatz-Instance aus Ihrem neuen AMI starten. Weitere Informationen finden Sie unter Konvertieren Sie Ihre Amazon-S3-gestütztes AMI in ein Amazon EBS-gestütztes AMI.

Automatische Instance-Wiederherstellung

> **Important**
>
> In diesem Abschnitt wird beschrieben, wie Sie Wiederherstellungsmechanismen für eine EC2 Instance proaktiv konfigurieren. Diese Wiederherstellungsmechanismen dienen dazu, die Instance-Verfügbarkeit wiederherzustellen, wenn AWS ein zugrunde liegendes Hardware- oder Softwareproblem erkennt, das dazu führt, dass eine Systemstatusprüfung fehlschlägt. Wenn Sie derzeit Probleme beim Zugriff auf Ihre Instance haben, finden Sie weitere Informationen unter Problembehandlung bei EC2 Instanzen.

Wenn AWS festgestellt wird, dass eine Instance aufgrund eines zugrunde liegenden Hardware- oder Softwareproblems nicht verfügbar ist, gibt es zwei Mechanismen, mit denen die Instance-Verfügbarkeit automatisch wiederhergestellt werden kann: die vereinfachte automatische Wiederherstellung und die CloudWatch aktionsbasierte Wiederherstellung von Amazon. Die Wiederherstellung der Instance-Verfügbarkeit wird auch als Instance-Wiederherstellung bezeichnet.

AWS Wird während des Wiederherstellungsprozesses der Instance versuchen, Ihre Instance von dem Host mit dem zugrunde liegenden Hardware- oder Softwareproblem auf einen anderen Host zu verschieben. Eine erfolgreiche Instance-Wiederherstellung wird für die Instance als ungeplanter Neustart angezeigt. Sie können überprüfen, ob eine Instance-Wiederherstellung stattgefunden hat.

Wenn der Wiederherstellungsprozess nicht erfolgreich ist, läuft die Instance möglicherweise weiterhin auf dem Host mit dem zugrunde liegenden Hardware- oder Softwareproblem. In diesem Fall ist ein manuelles Eingreifen erforderlich. Wenn die Instance unerreichbar ist oder die Systemstatusprüfung weiterhin fehlschlägt, wird empfohlen, dass Sie die Instance manuell anhalten und starten. Wenn Sie eine Instance starten, wird sie in der Regel auf einen neuen zugrunde liegenden Host-Computer migriert. Im Gegensatz zur automatischen Instanzwiederherstellung, bei der die Instance ihre öffentliche IPv4 Adresse beibehält, erhält eine neu gestartete Instance jedoch eine neue öffentliche IPv4 Adresse, sofern sie keine Elastic IP-Adresse hat.

Um von den automatischen Wiederherstellungsmechanismen zu profitieren, müssen sie im Voraus auf einer Instance konfiguriert werden, bevor eine Systemstatusprüfung fehlschlägt. Die vereinfachte automatische Wiederherstellung ist beim Start der Instance standardmäßig aktiviert. Sie können optional die CloudWatch aktionsbasierte Wiederherstellung von Amazon nach dem Start konfigurieren. Wenn Sie einen dieser Mechanismen konfiguriert haben, wird Ihre Instance widerstandsfähiger.

Die vereinfachte automatische Wiederherstellung und die CloudWatch aktionsbasierte Wiederherstellung von Amazon sind nur auf unterstützten Instances verfügbar. Weitere Informationen erhalten Sie unter Anforderungen zum Aktivieren der vereinfachten automatischen Wiederherstellung und Anforderungen für die Aktivierung einer CloudWatch aktionsbasierten Wiederherstellung.

Warning

Wenn Sie Ihre AWS Instance aufgrund eines zugrundeliegenden Hardware- oder Softwareproblems wiederherstellen, sollten Sie sich der folgenden Konsequenzen bewusst sein: Daten, die im flüchtigen Speicher (RAM) gespeichert sind, gehen verloren und die Betriebszeit des Betriebssystems beginnt von vorne. Darüber hinaus gehen bei der CloudWatch aktionsbasierten Wiederherstellung auch Daten auf Instance-Speicher-Volumes verloren. Zum Schutz vor Datenverlust empfehlen wir Ihnen, regelmäßig Backups von wertvollen Daten zu erstellen. Weitere Informationen zu den bewährten Methoden für Sicherung und Wiederherstellung für EC2 Instances finden Sie unter Bewährte Methoden für Amazon EC2.

Automatische Mechanismen zur Wiederherstellung von Instances sind für einzelne Instances konzipiert. Hinweise zur Entwicklung eines ausfallsicheren Systems finden Sie unter Ein ausfallsicheres System entwickeln.

Themen

- Schlüsselkonzepte der automatischen Instance-Wiederherstellung
- Unterschiede zwischen vereinfachter automatischer Wiederherstellung und CloudWatch aktionsbasierter Wiederherstellung
- Ein ausfallsicheres System entwickeln
- Überprüfen, ob eine automatische Instance-Wiederherstellung stattgefunden hat
- Konfigurieren Sie die vereinfachte automatische Wiederherstellung auf einer EC2 Amazon-Instance
- Konfigurieren Sie die CloudWatch aktionsbasierte Wiederherstellung für eine EC2 Instanz

Schlüsselkonzepte der automatischen Instance-Wiederherstellung

Die automatische Instance-Wiederherstellung ist eine EC2 Amazon-Funktion, die automatisch die Instance-Verfügbarkeit wiederherstellt, wenn zugrunde liegende Hardware- oder Softwarefehler auftreten, wodurch die Widerstandsfähigkeit und Zuverlässigkeit Ihrer EC2 Instances verbessert wird.

Im Folgenden sind die Schlüsselkonzepte der automatischen Instance-Wiederherstellung angeführt:

Konfigurationsoptionen

Zwei Mechanismen können konfiguriert werden, um die automatische Instance-Wiederherstellung zu unterstützen:

- Vereinfachte automatische Wiederherstellung: Auf unterstützten Instances standardmäßig aktiviert
- CloudWatch aktionsbasierte Wiederherstellung: Erfordert eine manuelle Konfiguration der unterstützten Instances.

System-Statusprüfungen

Systemstatusprüfungen überwachen automatisch die AWS Infrastruktur, auf der Ihre EC2 Instance ausgeführt wird.

- Schlägt eine Systemstatusprüfung fehl, wird eine automatische Instanzwiederherstellung AWS eingeleitet, bei der versucht wird, die betroffene Instanz auf eine andere Hardware zu migrieren.
- Eine fehlgeschlagene Systemstatusprüfung deutet auf ein Problem mit der Hardware oder Software des Hosts und nicht auf ein Problem mit der Instance selbst hin. Durch die automatische Instance-Wiederherstellung kann eine Instance wiederhergestellt werden, die eine Systemstatusprüfung nicht bestanden hat. Die automatische Instance-Wiederherstellung funktioniert jedoch nicht, wenn nur die Instance-Statusprüfung fehlschlägt.
- Informationen zu den Unterschieden zwischen Instance- und Systemstatusprüfungen finden Sie unter Arten von Statusprüfungen.

Beispiele für zugrunde liegende Hardware- oder Softwareprobleme

Zu den Hardware- oder Softwareproblemen, die dazu führen können, dass eine Systemstatusprüfung fehlschlägt, gehören der Verlust der Netzwerkkonnektivität, der Ausfall der Stromversorgung, Softwareprobleme auf dem physischen Host und Hardwareprobleme auf dem physischen Host, die die Erreichbarkeit des Netzwerks beeinträchtigen.

Merkmale wiederhergestellter Instances

Eine wiederhergestellte Instance ist mit der ursprünglichen Instance identisch, mit Ausnahme der Elemente, die verloren gegangen sind.

Erhaltene Elemente:

- Instance-ID
- Bestimmen Ihrer öffentlichen, privaten und Elastic IP-Adressen
- Instance-Metadaten
- Platzierungsgruppe
- EBS-Volumes anfügen
- Availability Zone

Verlorene Elemente:

- Daten, die im flüchtigen Speicher (RAM) gespeichert sind
- Auf Instance-Speicher-Volumes gespeicherte Daten (gilt nur für die CloudWatch aktionsbasierte Wiederherstellung)
- Die Betriebszeit des Betriebssystems wird auf Null zurückgesetzt

Überwachung der Systemstatusprüfungen mit CloudWatch

Die Metrik StatusCheckFailed_System in CloudWatch gibt an, ob eine Systemstatusprüfung bestanden wurde oder fehlgeschlagen ist.

Metrikwerte:

- 0 – Die Systemstatusprüfung wurde bestanden.
- 1 – Die Systemstatusprüfung ist fehlgeschlagen.

Ereignisse in AWS Health Dashboard

AWS Sendet bei automatischen Versuchen zur Instanzwiederherstellung Ereignisse an Sie, die auf dem konfigurierten Wiederherstellungsmechanismus und dessen Ergebnis AWS Health Dashboard basieren:

- Vereinfachte automatische Wiederherstellung
  - Erfolg-Ereignis: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS`
  - Fehler-Ereignis: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE`
- CloudWatch aktionsbasierte Wiederherstellung

- Erfolg-Ereignis: `AWS_EC2_INSTANCE_AUTO_RECOVERY_SUCCESS`
- Fehler-Ereignis: `AWS_EC2_INSTANCE_AUTO_RECOVERY_FAILURE`

Unterschiede zwischen vereinfachter automatischer Wiederherstellung und CloudWatch aktionsbasierter Wiederherstellung

In der folgenden Tabelle werden die wichtigsten Unterschiede zwischen der vereinfachten automatischen Wiederherstellung und der CloudWatch aktionsbasierten Wiederherstellung verglichen.

Vergleichspunkt	Vereinfachte automatische Wiederherstellung	CloudWatch aktionsbasierte Wiederherstellung
Konfiguration	Standardmäßig aktiviert auf unterstützten Instances	Erfordert die manuelle Konfiguration von CloudWatch Alarmen und Aktionen
Flexibilität	Das Wiederherstellungs verhalten wurde behoben, das von verwaltet wird AWS	Individuell anpassbare Aktionen und Bedingungen
Benachrichtigung	Grundlegende Benachric htigungen über AWS Health Dashboard	Anpassbare Benachric htigungen über SNS
Metal-Instance-Größe	Ausgeschlossen	Enthalten
Instance-Speicher-Volumes werden beim Start angehängt.	Wird nicht für Instances unterstützt, die beim Start Instance-Speicher-Volumes anhängen	Wird auf ausgewählten Instance-Typen unterstützt. Beachten Sie, dass Daten auf Instance-Speicher-Volumes während der Instance-Wiederherstellung verloren gehen.
Zeit für die Wiederherstellung	Standard-Wiederherstellungs versuch	Schnellere Wiederherstellungs versuche als vereinfachte

Vergleichspunkt	Vereinfachte automatische Wiederherstellung	CloudWatch aktionsbasierte Wiederherstellung
		automatische Wiederher stellung
Das Hostproblem wird während der Migration behoben	Die Migration wird möglicher weise abgebrochen und die Instance verbleibt auf dem ursprünglichen Host	Die Migration zu einem neuen Host wird fortgesetzt
Cost (Kosten)	Keine zusätzlichen Kosten	Es können Gebühren anfallen CloudWatch

Ein ausfallsicheres System entwickeln

Die vereinfachte automatische Wiederherstellung und die CloudWatch aktionsbasierte Wiederherstellung sind zwar effektiv, um die Verfügbarkeit einzelner Instances aufrechtzuerhalten, AWS empfiehlt jedoch die Implementierung einer Hochverfügbarkeitsarchitektur, die ein Failover des Datenverkehrs auf fehlerfreie Instanzen ermöglicht.

Um dies zu erreichen, sollten Sie AWS Dienste wie Elastic Load Balancing (das den eingehenden Traffic auf mehrere EC2 Instances verteilt) und Amazon EC2 Auto Scaling (das die Anzahl der Instances automatisch an Nachfrage und Zustand anpasst) in Betracht ziehen.

Weitere Informationen zum Aufbau eines belastbaren, fehlertoleranten Systems mit EC2 Instances finden Sie in den folgenden Ressourcen:

- Zurück zu den Grundlagen: Konzipieren für Ausfälle mit EC2 On-the-Canal-Technologie AWS YouTube
- Disaster Recovery (DR) -Architektur im AWSÜberblick, Teil I: Strategien für die Wiederherstellung in der Cloud auf der AWS Architektur-Blogseite
- Benutzerhandbuch für Application Load Balancer
- Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch
- REL11-BP02 Failover auf gesunde Ressourcen im Well-Architected Framework für Zuverlässigkeitssäule AWS

Überprüfen, ob eine automatische Instance-Wiederherstellung stattgefunden hat

Wenn die Instance anscheinend offline war und dann unerwartet neu gestartet wurde, wurde möglicherweise als Reaktion auf einen zugrunde liegenden Hardware- oder Software-Problems eine automatische Instance-Wiederherstellung durchgeführt. Sie können das überprüfen, indem Sie in Ihrem AWS Health Dashboard nach automatischen Instance-Wiederherstellungsereignissen suchen. Sie können auch überprüfen, ob für Ihre Instance ein zugrundeliegendes Hardware- oder Softwareproblem erkannt wurde, indem Sie die CloudWatch Amazon-Metrik StatusCheckFailed_System überprüfen.

Suchen Sie nach Ereignissen in AWS Health Dashboard

Wenn ein automatischer Instanzwiederherstellungsversuch erfolgt, AWS sendet Ereignisse an Ihre AWS Health Dashboard. Das spezifische Ereignis hängt vom konfigurierten Wiederherstellungsmechanismus ab und davon, ob der Versuch erfolgreich war oder fehlgeschlagen ist.

Um nach automatischen Instanzwiederherstellungsereignissen zu suchen AWS Health Dashboard

1. Öffne das AWS Health Dashboard zu https://phd.aws.amazon.com/phd/Hause #/.
2. Suchen Sie nach Ereignissen im Zusammenhang mit der automatischen Instance-Wiederherstellung. Das Vorhandensein dieser Ereignisse kann bestätigen, ob ein Versuch einer automatischen Instance-Wiederherstellung stattgefunden hat und welches Ergebnis er hatte.

   - Vereinfachte automatische Wiederherstellung
     - Erfolg-Ereignis: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS`
     - Fehler-Ereignis: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE`
   - CloudWatch aktionsbasierte Wiederherstellung
     - Erfolg-Ereignis: `AWS_EC2_INSTANCE_AUTO_RECOVERY_SUCCESS`
     - Fehler-Ereignis: `AWS_EC2_INSTANCE_AUTO_RECOVERY_FAILURE`

Überwachen Sie Systemstatusprüfungen mit CloudWatch

Sie können überprüfen, ob für Ihre Instance ein zugrundeliegendes Hardware- oder Softwareproblem erkannt wurde, indem Sie die Metrik StatusCheckFailed_System unter überprüfen. CloudWatch

Der Metrikwert gibt an, ob eine Systemstatusprüfung bestanden wurde (kein Hardware- oder Softwareproblem) oder fehlgeschlagen ist (Hardware- oder Softwareproblem).

So überprüfen Sie, ob ein zugrundeliegendes Hardware- oder Softwareproblem erkannt wurde

1. Die Metrik-Seite der CloudWatch Konsole zu https://console.aws.amazon.com/cloudwatch/Hause öffnen? #metricsV2.
2. Stellen Sie sicher, dass Sie sich in derselben Region wie Ihre EC2 Instance befinden.
3. Fügen Sie die folgende Metrik in das Suchfeld Metriken ein und drücken Sie die Eingabetaste.

   ```
   StatusCheckFailed_System
   ```

4. Wählen Sie EC2 > Metriken pro Instanz.
5. Aktivieren Sie in der Tabelle das Kontrollkästchen neben der Instance, die Sie überprüfen möchten.
6. Ändern Sie den Abfragezeitraum auf den Zeitpunkt, zu dem Sie vermuten, dass das Wiederherstellungsereignis eingetreten ist.
7. Wählen Sie den Tab Graphed metrics und gehen Sie für StatusCheckFailed_System wie folgt vor:

   a. Wählen Sie für Statistik entweder Durchschnitt, Maximum oder Minimum.

   b. Wählen Sie als Zeitraum die Option 1 Minute aus.
8. Überprüfen Sie den Wert für StatusCheckFailed _System.

   - Wert 0: Die Systemstatusprüfung wurde erfolgreich abgeschlossen, was darauf hindeutet, dass kein Hardware- oder Softwareproblem zugrunde liegt.
   - Wert 1: Die Systemstatusüberprüfung ist fehlgeschlagen, was auf ein zugrundeliegendes Hardware- oder Softwareproblem hinweist.

Weitere Informationen finden Sie unter Automatische Instance-Wiederherstellung.

Konfigurieren Sie die vereinfachte automatische Wiederherstellung auf einer EC2 Amazon-Instance

> **Important**
>
> In diesem Abschnitt wird beschrieben, wie Sie Wiederherstellungsmechanismen auf einer EC2 Instance proaktiv konfigurieren. Diese Wiederherstellungsmechanismen dienen dazu, die Instance-Verfügbarkeit wiederherzustellen, wenn AWS ein zugrunde liegendes Hardware- oder Softwareproblem erkennt, das dazu führt, dass eine Systemstatusprüfung fehlschlägt. Wenn Sie derzeit Probleme beim Zugriff auf Ihre Instance haben, finden Sie weitere Informationen unter Problembehandlung bei EC2 Instanzen.

Wenn AWS festgestellt wird, dass eine Instance aufgrund eines zugrunde liegenden Hardware- oder Softwareproblems nicht verfügbar ist, kann die vereinfachte automatische Wiederherstellung die Instanzverfügbarkeit automatisch wiederherstellen, indem die Instance von dem Host mit dem zugrunde liegenden Problem auf einen anderen Host verschoben wird.

Wenn eine vereinfachte automatische Wiederherstellung stattfindet, AWS sendet je nach Ergebnis eines der folgenden Ereignisse an Sie AWS Health Dashboard:

- Erfolg-Ereignis: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS`
- Fehler-Ereignis: `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE`

Sie können Benachrichtigungen konfigurieren, um über diese Ereignisse benachrichtigt zu werden. Weitere Informationen finden Sie unter Erstellen Ihrer ersten Benachrichtigungskonfiguration in AWS-Benutzerbenachrichtigungen im Benutzerhandbuch für AWS-Benutzerbenachrichtigungen . Sie können auch EventBridge Amazon-Regeln verwenden, um vereinfachte automatische Wiederherstellungsereignisse zu überwachen.

Die vereinfachte automatische Wiederherstellung ist standardmäßig auf allen unterstützten Instances beim Start aktiviert. Sie kann jedoch nur ausgeführt werden, wenn sich eine Instance im `running` Status befindet, keine Serviceereignisse in der AWS Health Dashboard aufgeführt sind und für den Instance-Typ Kapazität verfügbar ist. In einigen Situationen, z. B. bei erheblichen Ausfällen, können Kapazitätsengpässe dazu führen, dass Wiederherstellungsversuche fehlschlagen. Weitere Informationen finden Sie unter the section called “Fehlerbehebung bei der vereinfachten automatischen Wiederherstellung”.

Sie können die vereinfachte automatische Wiederherstellung während oder nach dem Start deaktivieren und sie bei Bedarf später wieder aktivieren.

> **Warning**
>
> Wenn Sie AWS Ihre Instance aufgrund eines zugrunde liegenden Hardware- oder Softwareproblems wiederherstellen, sollten Sie sich der folgenden Konsequenzen bewusst sein: Daten, die im flüchtigen Speicher (RAM) gespeichert sind, gehen verloren und die Betriebszeit des Betriebssystems beginnt bei Null. Zum Schutz vor Datenverlust empfehlen wir Ihnen, regelmäßig Backups von wertvollen Daten zu erstellen. Weitere Informationen zu den bewährten Methoden für Sicherung und Wiederherstellung für EC2 Instances finden Sie unter Bewährte Methoden für Amazon EC2.
> Automatische Mechanismen zur Wiederherstellung von Instances sind für einzelne Instances konzipiert. Hinweise zur Entwicklung eines ausfallsicheren Systems finden Sie unter Ein ausfallsicheres System entwickeln.

Inhalt

- Anforderungen zum Aktivieren der vereinfachten automatischen Wiederherstellung
- Vereinfachte automatische Wiederherstellung konfigurieren
- Fehlerbehebung bei der vereinfachten automatischen Wiederherstellung

Anforderungen zum Aktivieren der vereinfachten automatischen Wiederherstellung

Die vereinfachte automatische Wiederherstellung kann auf Instances aktiviert werden, die die folgenden Kriterien erfüllen:

Instance-Typen

- Allzweck: A1, M3, M4, M5, M5a, M5n, M5zn, M6a, M6g, M6i, M6in, M7a, M7g, M7i, M7i-flex, M8a, M8g, M8i, M8i-flex, T1, T2, T3, T3a, T4g
- Computeroptimiert: C3, C4, C5, C5a, C5n, C6a, C6g, C6gn, C6i, C6in, C7a, C7g, C7gn, C7i, C7i-Flex, C8a, C8g, C8GB, C8Gb, C8Gn, C8i, C8i-Flex
- Arbeitsspeicheroptimiert: R3, R4, R5, R5a, R5b, R5n, R6a, R6g, R6i, R6in, R7a, R7g, R7i, R7iz, R8a, R8g, R8gb, R8gn, R8i, R8i-flex, U-3tb1, U-6tb1, U-9tb1, U-12tb1, U-18tb1, U-24tb1, U7i-6tb, U7i-8tb, U7i-12tb, U7in-16tb, U7in-24tb, U7in-32tb, U7inh-32tb, X1, X1e, X2iezn, X8g
- Beschleunigtes Rechnen: G3, G5g, Inf1, P3, VT1

- Hochleistungs-Datenverarbeitung Hpc6a, Hpc7a, Hpc7g

Tenancy

- Freigegeben
- Dedicated Instance

  Weitere Informationen finden Sie unter Amazon-EC2-Dedicated-Instances.

Einschränkungen

Die vereinfachte automatische Wiederherstellung wird nicht für Instances mit den folgenden Merkmalen unterstützt:

- Instance-Größe: `metal`-Instances
- Tenancy: Dedicated Host. Verwenden Sie für Dedicated Hosts stattdessen Dedicated Host Auto Recovery.
- Speicher: Instances mit Instance-Speicher-Volumes
- Netzwerke: Instances, die einen Elastic Fabric Adapter verwenden
- Auto Scaling: Instances, die Teil einer Amazon EC2 Auto Scaling Scaling-Gruppe sind
- Wartung: Instances, für die derzeit ein geplantes Wartungsereignis durchgeführt wird

Vereinfachte automatische Wiederherstellung konfigurieren

Die vereinfachte automatische Wiederherstellung ist standardmäßig aktiviert, wenn Sie eine unterstützte Instance starten. Sie können das automatische Wiederherstellungsverhalten zu `disabled` während oder nach dem Starten der Instance festlegen.

Die `default`-konfiguration ermöglicht nicht die vereinfachte automatische Wiederherstellung für einen nicht unterstützten Instance-Typ.

Console

So deaktivieren Sie die vereinfachte automatische Wiederherstellung beim Launchen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Launch instance (Instance starten) aus.

3. Wählen Sie im Abschnitt Erweiterte Details für Automatische Instance-Wiederherstellung die Option Deaktiviert.
4. Konfigurieren Sie die verbleibenden Instance-Starteinstellungen nach Bedarf und starten Sie dann die Instance.

So deaktivieren Sie die vereinfachte automatische Wiederherstellung nach dem Start

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und dann Actions (Aktionen), Instance Settings (Instance-Einstellungen) und Change auto-recovery behavior (Verhalten der automatischen Wiederherstellung ändern).
4. Wählen Sie Off (Aus) und dann Save (Speichern) aus.

So aktivieren Sie die vereinfachte automatische Wiederherstellung nach dem Start

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und dann Actions (Aktionen), Instance Settings (Instance-Einstellungen) und Change auto-recovery behavior (Verhalten der automatischen Wiederherstellung ändern).
4. Wählen Sie Standard (Ein) und dann Speichern.

AWS CLI

So deaktivieren Sie die vereinfachte automatische Wiederherstellung beim Launchen

Verwenden den Befehl run-instances mit der Option `--maintenance-options`.

```
--maintenance-options AutoRecovery=Disabled
```

So deaktivieren Sie die vereinfachte automatische Wiederherstellung nach dem Start

Verwenden Sie den Befehl modify-instance-maintenance-options.

```
aws ec2 modify-instance-maintenance-options \
```

```
    --instance-id i-1234567890abcdef0 \
    --auto-recovery disabled
```

So aktivieren Sie die vereinfachte automatische Wiederherstellung nach dem Start

Verwenden Sie den Befehl modify-instance-maintenance-options.

```
aws ec2 modify-instance-maintenance-options \
    --instance-id i-1234567890abcdef0 \
    --auto-recovery default
```

PowerShell

So deaktivieren Sie die vereinfachte automatische Wiederherstellung beim Launchen

Verwenden Sie das cmdlet New-EC2Instance.

```
-MaintenanceOptions_AutoRecovery Disabled
```

So deaktivieren Sie die vereinfachte automatische Wiederherstellung nach dem Start

Verwenden Sie das cmdlet Edit-EC2InstanceMaintenanceOption.

```
Edit-EC2InstanceMaintenanceOption `
    -InstanceId i-1234567890abcdef0 `
    -AutoRecovery Disabled
```

So aktivieren Sie die vereinfachte automatische Wiederherstellung nach dem Start

Verwenden Sie das cmdlet Edit-EC2InstanceMaintenanceOption.

```
Edit-EC2InstanceMaintenanceOption `
    -InstanceId i-1234567890abcdef0 `
    -AutoRecovery Enabled
```

Fehlerbehebung bei der vereinfachten automatischen Wiederherstellung

Falls die vereinfachte automatische Wiederherstellung die Instance nicht wiederherstellt, berücksichtigen Sie die folgenden Punkte:

- AWS Service-Events laufen

  Die vereinfachte automatische Wiederherstellung funktioniert nicht bei Serviceereignissen in der AWS Health Dashboard. Sie erhalten möglicherweise keine Benachrichtigungen zu Wiederherstellungsfehlern für solche Ereignisse. Für die neusten Informationen zur Serviceverfügbarkeit lesen Sie die Seite zum Servicezustand-Status.

- Unzureichende Kapazität

  Es ist vorübergehend nicht genügend Ersatzhardware vorhanden, um die Instance zu migrieren.

- Die maximale Anzahl der Wiederherstellungsversuche pro Tag wurde erreicht

  Die Instance hat die maximale zugelassene Anzahl von Wiederherstellungsversuchen pro Tag erreicht. Die Instance kann anschließend außer Betrieb genommen werden, wenn die automatische Wiederherstellung fehlschlägt und als Ursache für das Fehlschlagen der ursprünglichen Systemstatusprüfung ein Leistungsabfall der Hardware ermittelt wurde.

Wenn die Systemstatusprüfung der Instance trotz mehrerer Wiederherstellungsversuche weiterhin fehlschlägt, finden Sie weitere Hinweise unter Problembehandlung bei Instances mit fehlgeschlagenen Statusprüfungen.

Konfigurieren Sie die CloudWatch aktionsbasierte Wiederherstellung für eine EC2 Instanz

> **Important**
>
> In diesem Abschnitt wird beschrieben, wie Sie Wiederherstellungsmechanismen auf einer EC2 Instanz proaktiv konfigurieren. Diese Wiederherstellungsmechanismen dienen dazu, die Instance-Verfügbarkeit wiederherzustellen, wenn AWS ein zugrunde liegendes Hardware- oder Softwareproblem erkennt, das dazu führt, dass eine Systemstatusprüfung fehlschlägt. Wenn Sie derzeit Probleme beim Zugriff auf Ihre Instance haben, finden Sie weitere Informationen unter Problembehandlung bei EC2 Instanzen.

Wenn AWS festgestellt wird, dass eine Instance aufgrund eines zugrunde liegenden Hardware- oder Softwareproblems nicht verfügbar ist, kann die CloudWatch aktionsbasierte Wiederherstellung die Instanzverfügbarkeit automatisch wiederherstellen, indem die Instanz von dem Host mit dem zugrunde liegenden Problem auf einen anderen Host verschoben wird.

Wenn eine CloudWatch aktionsbasierte Wiederherstellung stattfindet, AWS sendet je nach Ergebnis eines der folgenden Ereignisse an Sie AWS Health Dashboard:

- Erfolg-Ereignis: `AWS_EC2_INSTANCE_AUTO_RECOVERY_SUCCESS`
- Fehler-Ereignis: `AWS_EC2_INSTANCE_AUTO_RECOVERY_FAILURE`

Sie können die CloudWatch aktionsbasierte Wiederherstellung konfigurieren, um Wiederherstellungsaktionen zu CloudWatch Amazon-Alarmen hinzuzufügen. CloudWatch Die aktionsbasierte Wiederherstellung funktioniert mit der `StatusCheckFailed_System` Metrik. CloudWatchDie aktionsbasierte to-the-minute Wiederherstellung bietet detaillierte Reaktionszeiten und Amazon Simple Notification Service (Amazon SNS) Benachrichtigungen über Wiederherstellungsaktionen und -ergebnisse. Diese Konfigurationsoptionen ermöglichen im Vergleich zur vereinfachten automatischen Wiederherstellung schnellere Wiederherstellungsversuche mit detaillierterer Kontrolle über die Reaktion auf Fehlschläge bei der Systemstatusprüfung. Weitere Informationen zu den verfügbaren CloudWatch Optionen finden Sie unter Statuschecks für Ihre Instances.

Eine CloudWatch aktionsbasierte Wiederherstellung kann jedoch nur ausgeführt werden, wenn sich eine Instanz im `running` Status befindet, keine Serviceereignisse in der AWS Health Dashboard aufgeführt sind und für den Instanztyp Kapazität verfügbar ist. In einigen Situationen, z. B. bei erheblichen Ausfällen, können Kapazitätsengpässe dazu führen, dass Wiederherstellungsversuche fehlschlagen. Weitere Informationen finden Sie unter the section called “Fehlerbehebung”.

> **Warning**
>
> Wenn Sie Ihre AWS Instance aufgrund eines zugrunde liegenden Hardware- oder Softwareproblems wiederherstellen, sollten Sie sich der folgenden Konsequenzen bewusst sein: Daten, die im flüchtigen Speicher (RAM) und auf Instance-Speicher-Volumes gespeichert sind, gehen verloren, und die Betriebszeit des Betriebssystems beginnt bei Null. Zum Schutz vor Datenverlust empfehlen wir Ihnen, regelmäßig Backups von wertvollen Daten zu erstellen. Weitere Informationen zu den bewährten Methoden für Sicherung und Wiederherstellung für EC2 Instances finden Sie unter Bewährte Methoden für Amazon EC2. Automatische Mechanismen zur Wiederherstellung von Instances sind für einzelne Instances konzipiert. Hinweise zur Entwicklung eines ausfallsicheren Systems finden Sie unter Ein ausfallsicheres System entwickeln.

Inhalt

- Anforderungen für die Aktivierung einer CloudWatch aktionsbasierten Wiederherstellung
- Konfigurieren Sie die CloudWatch aktionsbasierte Wiederherstellung
- Beheben Sie CloudWatch aktionsbasierte Wiederherstellungsfehler

Anforderungen für die Aktivierung einer CloudWatch aktionsbasierten Wiederherstellung

CloudWatch Die aktionsbasierte Wiederherstellung kann für Instanzen aktiviert werden, die die folgenden Kriterien erfüllen:

Instance-Typen

- Allzweck: A1, M3, M4, M5, M5a, M5n, M5zn, M6a, M6g, M6i, M6in, M7a, M7g, M7i, M7i-flex, M8a, M8g, M8i, M8i-flex, T1, T2, T3, T3a, T4g
- Computeroptimiert: C3, C4, C5, C5a, C5n, C6a, C6g, C6gn, C6i, C6in, C7a, C7g, C7gn, C7i, C7i-Flex, C8a, C8g, C8GB, C8Gb, C8Gn, C8i, C8i-Flex
- Arbeitsspeicheroptimiert: R3, R4, R5, R5a, R5b, R5n, R6a, R6g, R6i, R6in, R7a, R7g, R7i, R7iz, R8a, R8g, R8gb, R8gn, R8i, R8i-flex, U-3tb1, U-6tb1, U-9tb1, U-12tb1, U-18tb1, U-24tb1, U7i-6tb, U7i-8tb, U7i-12tb, U7in-16tb, U7in-24tb, U7in-32tb, U7inh-32tb, X1, X1e, X2idn, X2iedn, X2iezn, X8g
- Beschleunigtes Rechnen: G3, G5g, Inf1, P3, VT1
- Hochleistungs-Datenverarbeitung Hpc6a, Hpc7a, Hpc7g
- Metal-Instances: Jeder der oben genannten Instance-Typen mit der Metal-Instance-Größe.
- Wenn Instance-Speicher-Volumes beim Start hinzugefügt werden: Nur die folgenden Instance-Typen werden unterstützt: M3, C3, R3, X1, X1e, X2idn, X2iedn

Tenancy

- Freigegeben
- Dedicated Instance

  Weitere Informationen finden Sie unter Amazon-EC2-Dedicated-Instances.

Einschränkungen

CloudWatch Die aktionsbasierte Wiederherstellung wird für Instances mit den folgenden Eigenschaften nicht unterstützt:

- Tenancy: Dedicated Host. Verwenden Sie für Dedicated Hosts stattdessen Dedicated Host Auto Recovery.
- Netzwerke: Instances, die einen Elastic Fabric Adapter verwenden
- Auto Scaling: Instances, die Teil einer Amazon EC2 Auto Scaling Scaling-Gruppe sind
- Wartung: Instances, für die derzeit ein geplantes Wartungsereignis durchgeführt wird

Einen unterstützten Instance-Typ suchen

Sie können sich die Instance-Typen ansehen, die eine CloudWatch aktionsbasierte Wiederherstellung unterstützen.

Console

Um die Instance-Typen anzuzeigen, die eine CloudWatch aktionsbasierte Wiederherstellung unterstützen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich Instance Types (Instance-Typen) aus.
3. Geben Sie in der Filterleiste Unterstützung für automatische Wiederherstellung = wahr ein. In der Tabelle mit den Instance-Typen werden alle Instance-Typen angezeigt, die eine CloudWatch aktionsbasierte Wiederherstellung unterstützen.
4. (Optional) Fügen Sie Filter hinzu, um den Anwendungsbereich auf bestimmte Instance-Typen von Interesse zu erweitern.

AWS CLI

Um die Instance-Typen anzuzeigen, die eine CloudWatch aktionsbasierte Wiederherstellung unterstützen

Verwenden Sie den Befehl describe-instance-types mit dem Filter `auto-recovery-supported`.

```
aws ec2 describe-instance-types \
    --filters Name=auto-recovery-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

PowerShell

Um die Instanztypen anzuzeigen, die eine CloudWatch aktionsbasierte Wiederherstellung unterstützen

Verwenden Sie das Get-EC2InstanceTypeCmdlet mit dem `auto-recovery-supported` Filter.

```
Get-EC2InstanceType `
    -Filter @{Name="auto-recovery-supported";Values="true"} | `
    Select InstanceType | Sort-Object InstanceType
```

Konfigurieren Sie die CloudWatch aktionsbasierte Wiederherstellung

Um die CloudWatch aktionsbasierte Wiederherstellung für eine EC2 Instanz zu konfigurieren, erstellen Sie einen CloudWatch Alarm, der die `StatusCheckFailed_System` Metrik für die angegebene Instanz überwacht. Stellen Sie den Alarm so ein, dass er ausgelöst wird, wenn der Metrikwert 1 ist, was auf eine fehlgeschlagene Systemstatusprüfung hinweist. Konfigurieren Sie die Alarmaktion so, dass beim Auslösen die Instance automatisch wiederhergestellt wird.

Sie können den Alarm entweder über die EC2 Amazon-Konsole oder die CloudWatch Konsole konfigurieren. Die Anweisungen finden Sie Wiederherstellungsaktionen zu CloudWatch Amazon-Alarmen hinzufügen in diesem Benutzerhandbuch oder Hinzufügen von Wiederherstellungsaktionen zu CloudWatch Amazon-Alarmen im CloudWatch Amazon-Benutzerhandbuch.

Beheben Sie CloudWatch aktionsbasierte Wiederherstellungsfehler

Wenn bei der CloudWatch aktionsbasierten Wiederherstellung Ihre Instanz nicht wiederhergestellt werden kann, sollten Sie die folgenden Probleme berücksichtigen:

- AWS Serviceereignisse werden ausgeführt

  CloudWatch Die aktionsbasierte Wiederherstellung funktioniert nicht bei Serviceereignissen in der AWS Health Dashboard. Sie erhalten möglicherweise keine Benachrichtigungen zu Wiederherstellungsfehlern für solche Ereignisse. Für die neusten Informationen zur Serviceverfügbarkeit lesen Sie die Seite zum Servicezustand-Status.
- Unzureichende Kapazität

  Es ist vorübergehend nicht genügend Ersatzhardware vorhanden, um die Instance zu migrieren.
- Die maximale Anzahl der Wiederherstellungsversuche pro Tag wurde erreicht

Die Instance hat die maximale zugelassene Anzahl von Wiederherstellungsversuchen pro Tag erreicht. Die Instance kann anschließend außer Betrieb genommen werden, wenn die automatische Wiederherstellung fehlschlägt und als Ursache für das Fehlschlagen der ursprünglichen Systemstatusprüfung ein Leistungsabfall der Hardware ermittelt wurde.

Wenn die Systemstatusprüfung der Instance trotz mehrerer Wiederherstellungsversuche weiterhin fehlschlägt, finden Sie weitere Hinweise unter Problembehandlung bei Instances mit fehlgeschlagenen Statusprüfungen.

Verwenden Sie Instanz-Metadaten, um Ihre EC2 Instanz zu verwalten

Instance-Metadaten sind Daten über eine Instance, mit denen Sie die ausgeführte Instance konfigurieren und verwalten können. Instance-Metadaten enthalten Folgendes:

Eigenschaften der Instance-Metadaten

Instance-Metadaten sind in Kategorien unterteilt (z. B. Host-Name, Ereignisse und Sicherheitsgruppen).

Dynamische Daten

Dynamische Daten sind Metadaten, die beim Start der Instance generiert werden, wie z. B. ein Instance-Identitätsdokument. Weitere Informationen finden Sie unter Kategorien von dynamischen Daten.

Benutzerdaten

Sie können Instance-Metadaten auch verwenden, um auf Benutzerdaten zuzugreifen, die Sie beim Start Ihrer Instance angegeben haben. Sie können beispielsweise Parameter für die Konfiguration Ihrer Instance angeben oder ein einfaches Skript einbinden. Sie können auch generische Konfigurationsdateien erstellen AMIs und Benutzerdaten verwenden, um die beim Start bereitgestellten Konfigurationsdateien zu ändern. Wenn Sie beispielsweise Webserver für verschiedene kleine Unternehmen betreiben, können sie alle dasselbe generische AMI verwenden und ihren Inhalt aus dem Amazon-S3-Bucket abrufen, den Sie beim Start in den Benutzerdaten angeben. Um jederzeit einen neuen Kunden hinzuzufügen, erstellen Sie einen Bucket für den Kunden, fügen Sie dessen Inhalt hinzu und starten Ihr AMI mit dem eindeutigen Bucket-Namen, der Ihrem Code in den Benutzerdaten zur Verfügung steht. Wenn Sie mehrere

Instances mit demselben `RunInstances`-Aufruf starten, sind die Benutzerdaten für alle Instances in dieser Reservierung verfügbar. Jede Instance, die Teil derselben Reservierung ist, hat eine eindeutige `ami-launch-index`-Nummer, sodass Sie Code schreiben können, der die Aktivitäten der Instances steuert. Beispielsweise kann sich der erste Host selbst als ursprünglichen Knoten in einem Cluster auswählen. Ein detailliertes AMI-Startbeispiel finden Sie unter Identifizieren Sie jede Instance, die in einer einzelnen Anfrage gestartet wurde.

Important

Sie können nur innerhalb der Instance selbst auf Instance-Metadaten und Benutzerdaten zugreifen. Die Daten sind nicht durch Authentifizierungs- oder kryptografische Verfahren geschützt. Jeder, der direkten Zugriff auf die Instance hat, und möglicherweise auch jede Software, die auf der Instance läuft, kann deren Metadaten einsehen. Daher sollten Sie sensible Daten wie Passwörter oder langlebige Verschlüsselungscodes nicht als Benutzerdaten speichern.

Inhalt

- Instance-Metadatenkategorien
- Kategorien von dynamischen Daten
- Auf Instanz-Metadaten für eine EC2 Instanz zugreifen
- Konfigurieren der Optionen des Instance-Metadaten-Services
- Befehle ausführen, wenn Sie eine EC2 Instance mit Benutzerdateneingabe starten
- Identifizieren Sie jede Instance, die in einer einzelnen Anfrage gestartet wurde

Instance-Metadatenkategorien

Instance-Metadaten-Eigenschaften werden in Kategorien unterteilt. Um Instance-Metadaten abzurufen, geben Sie die Kategorie in der Anfrage an, und die Metadaten werden in der Antwort zurückgegeben.

Wenn neue Kategorien veröffentlicht werden, wird ein neuer Instance-Metadaten-Build mit einer neuen Versionsnummer erstellt. In der folgenden Tabelle wird in der Spalte Version, als die Kategorie veröffentlicht wurde die Build-Version angegeben, als die Instance-Metadatenkategorie freigegeben wurde. Um zu vermeiden, dass Sie Ihren Code jedes Mal aktualisieren müssen, wenn Amazon

einen neuen Instance-Metadaten-Build EC2 veröffentlicht, verwenden Sie `latest` anstelle der Versionsnummer in Ihren Metadatenanfragen. Weitere Informationen finden Sie unter Abrufen der verfügbaren Versionen der Instance-Metadaten.

Wenn Amazon eine neue Instance-Metadatenkategorie EC2 veröffentlicht, sind die Instance-Metadaten für die neue Kategorie möglicherweise nicht für bestehende Instances verfügbar. Bei Instances, die auf dem Nitro-System erstellt wurden, können Sie Instance-Metadaten nur für die Kategorien abrufen, die beim Start verfügbar waren. Bei Instances mit dem Xen-Hypervisor können Sie die Instance stoppen und dann starten, um die für die Instance verfügbaren Kategorien zu aktualisieren.

In der folgenden Tabelle werden die Kategorien von Instance-Metadaten aufgeführt. Einige der Kategorienamen enthalten Platzhalter für Daten, die für Ihre Instance eindeutig sind.. *mac*Stellt beispielsweise die MAC-Adresse für die Netzwerkschnittstelle dar. Sie müssen die Platzhalter durch tatsächliche Werte ersetzen, wenn Sie die Instance-Metadaten abrufen.

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`ami-id`	Die für den Start der Instance verwendete AMI-ID	1,0
`ami-launch-index`	Wenn Sie mehrere Instances mit demselben `RunInstances` -Aufruf starten, gibt dieser Wert die Startreihenfolge für jede Instance an. Der Wert für die zuerst gestartete Instance ist 0. Wenn Sie Instances mit Auto Scaling oder EC2 Fleet starten, ist dieser Wert immer 0.	1,0
`ami-manifest-path`	Der Pfad zu der AMI-Manif estdatei in Amazon S3. Wenn Sie für den Start der Instance ein Amazon EBS-Backed AMI	1,0

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
	verwendet haben, wird als Ergebnis ausgegebe `unknown`.	
`ancestor-ami-ids`	Das AMI IDs aller Instances, die zur Erstellung dieses AMI neu gebündelt wurden. Dieser Wert ist nur vorhanden, wenn die AMI-Manifestdatei einen `ancestor-amis` -Schlüssel enthalten hat.	2007-10-10
`autoscaling/target-lifecycle-state`	Wert, der den Zielstatus des Amazon EC2 Auto Scaling Scaling-Lebenszyklus angibt, zu dem eine Amazon EC2 Auto Scaling Scaling-Instance wechselt. Wird verwendet, wenn die Instance nach dem 10. März 2022 in einen der Ziel-Lebenszyklusstatus wechselt. Mögliche Werte: `Detached` | `InService` | `Standby` | `Terminated` | `Warmed:Hibernated` | `Warmed:Running` | `Warmed:Stopped` | `Warmed:Terminated` . Weitere Informationen finden Sie unter Abrufen des Ziellebenszyklusstatus mithilfe von Instance-Metadaten im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.	15.07.2021

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`block-device-mapping/ami`	Das virtuelle Gerät, das das Dateisystem enthält. root/boot	2007-12-15
`block-device-mapping/ebsN`	Die virtuellen Geräte, die mit einem Amazon EBS-Volume verknüpft sind. Amazon EBS-Volumes sind nur in Metadaten enthalten, wenn sie beim Starten der Instance – oder als die Instance zuletzt gestartet wurde – vorhanden waren. N zeigt dabei den Index für das Amazon EBS-Volume an (z. B. `ebs1` oder `ebs2`).	2007-12-15
`block-device-mapping/ephemeral N`	Die virtuellen Geräte für alle Speichervolumes, die keine NVMe Instanzen sind. N gibt den Index jedes Volumes an. Die Anzahl der Instance-Speicher-Volumes in der Blockgerät-Zuweisung entspricht möglicherweise nicht der tatsächlichen Anzahl der Instance-Speicher-Volumes für die Instance. Der Instance-Typ bestimmt die Anzahl der Instance-Speicher-Volumes, die für eine Instance verfügbar sind. Wenn die Anzahl der Instance-Speicher-Volumes in einer Blockgerät-Zuweisung die für eine Instance verfügbare Anzahl übersteigt, werden die überzähli gen Instance-Speicher-Volumes ignoriert.	2007-12-15

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`block-device-mapping/root`	Die virtuellen Laufwerke oder Partitionen, die den Root-Lauf werken oder Partitionen auf dem virtuellen Laufwerk zugeordnet sind, wobei das Root-Dateisystem (/ oder C:) der angegebenen Instance zugeordnet ist.	2007-12-15
`block-device-mapping/swap`	Die virtuellen Geräte, die mit `swap` verknüpft sind. Nicht immer vorhanden.	2007-12-15
`events/maintenance/history`	Enthält eine JSON-Zeichenfolge mit Informationen zu den Ereigniss en, wenn es abgeschlossene oder abgebrochene Wartungsereignisse für die Instance gibt.	2018-08-17
`events/maintenance/scheduled`	Enthält eine JSON-Zeichenfolge mit Informationen zu den Ereigniss en, wenn es aktive Wartungse reignisse für die Instance gibt. Weitere Informationen finden Sie unter Geplante Ereignisse anzeigen, die sich auf Ihre EC2 Amazon-Instances auswirken.	2018-08-17

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`events/recommendations/rebalance`	Der ungefähre Zeitpunkt in UTC, zu dem die Benachrichtigung über die Empfehlung zur Neuverteilung der EC2 Instance für die Instance ausgegeben wird. Das Folgende ist ein Beispiel für die Metadaten für diese Kategorie: `{"noticeTime": "2020-11-05T08:22:00Z"}` . Diese Kategorie ist erst verfügbar, nachdem die Benachrichtigung gesendet wurde. Weitere Informationen finden Sie unter EC2 Empfehlungen zur Neugewichtung von Instanzen.	2020-10-27
`hostname`	Wenn die EC2 Instanz IP-basierte Benennung (IPBN) verwendet, ist dies der private IPv4 DNS-Hostname der Instanz. Wenn die EC2 Instanz ressourcenbasierte Benennung (RBN) verwendet, ist dies die RBN. Wenn mehrere Netzwerkschnittstellen vorhanden sind, bezieht sich dieser Wert auf das Gerät eth0 (das Gerät mit der Gerätenummer 0). Weitere Informationen zu IPBN und RBN finden Sie unter Hostnamen und Domains der EC2-Instance.	1,0

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`iam/info`	Wenn der Instanz eine IAM-Rolle zugeordnet ist, enthält Informationen darüber, wann das Instanzprofil zuletzt aktualisiert wurde, einschließlich des LastUpdated Datums der Instanz, und. InstanceProfileArn InstanceProfileId Andernfalls nicht vorhanden.	2012-01-12
`iam/security-credentials/role-name`	Wenn der Instance eine IAM-Rolle zugeordnet *`role-name`* ist, ist dies der Name der Rolle und *`role-name`* enthält die temporären Sicherheitsanmeldedaten, die der Rolle zugeordnet sind (weitere Informationen finden Sie unterAbrufen von Sicherheitsanmeldeinformationen aus Instance-Metadaten). Andernfalls nicht vorhanden.	2012-01-12
`identity-credentials/ec2/info`	Informationen zu den Anmeldeinformationen in `identity-credentials/ec2/security-credentials/ec2-instance` .	2018-05-23

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`identity-credentials/ec2/security-credentials/ec2-instance`	Anmeldeinformationen für die Instanzidentitätsrolle, die es der On-Instance-Software ermöglichen, sich selbst AWS zu identifizieren, um Funktionen wie EC2 Instance Connect und AWS Systems Manager Standard-Host-Management-Konfiguration zu unterstützen. An diese Anmeldeinformationen sind keine Richtlinien angehängt, sodass sie über die Identifizierung der Instanz für die AWS Funktion hinaus keine zusätzlichen AWS API-Berechtigungen haben. Weitere Informationen finden Sie unter Instanzidentitätsrollen für EC2 Amazon-Instances.	2018-05-23
`instance-action`	Weist die Instance an, zur Vorbereitung einer Bündelung einen Neustart durchzuführen. Zulässige Werte: `none` | `shutdown` | `bundle-pending` .	2008-09-01
`instance-id`	Die ID dieser Instance	1,0
`instance-life-cycle`	Die Kaufoption dieser Instance. Weitere Informationen finden Sie unter EC2 Abrechnungs- und Kaufoptionen von Amazon.	01.10.2019

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`instance-type`	Der Typ der Instance. Weitere Informationen finden Sie unter EC2 Amazon-Instance-Typen.	2007-08-29
`ipv6`	Die IPv6 Adresse der Instanz. In Fällen, in denen mehrere Netzwerkschnittstellen vorhanden sind, bezieht sich dies auf die Netzwerkschnittstelle des eth0-Geräts (das Gerät, für das die Gerätenummer 0 ist) und die erste zugewiesene IPv6 Adresse. Wenn auf der Netzwerkschnittstelle [0] keine IPv6 Adresse vorhanden ist, ist dieses Element nicht gesetzt und führt zu einer HTTP 404-Antwort.	2021-01-03
`kernel-id`	Die ID des mit dieser Instance gestarteten Kernels (falls zutreffend)	2008-02-01

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`local-hostname`	Wenn mehrere Netzwerkschnittstellen vorhanden sind, bezieht sich dieser Wert auf das Gerät eth0 (das Gerät mit der Gerätenummer 0). Wenn die EC2 Instanz IP-basierte Benennung (IPBN) verwendet, ist dies der private IPv4 DNS-Hostname der Instanz. Wenn die EC2 Instanz ressourcenbasierte Benennung (RBN) verwendet, ist dies die RBN. Weitere Informationen zu IPBN, RBN und zur Benennung von Instanzen finden Sie unter. EC2 Hostnamen und Domains der EC2-Instance	2007-01-19
`local-ipv4`	Die private IPv4 Adresse der Instanz. Wenn mehrere Netzwerkschnittstellen vorhanden sind, bezieht sich dieser Wert auf das Gerät eth0 (das Gerät mit der Gerätenummer 0). Wenn es sich um eine IPv6 reine Instanz handelt, ist dieses Element nicht festgelegt und führt zu einer HTTP 404-Antwort.	1,0

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`mac`	Die Media Access Control-Adresse (MAC) der Instance. Wenn mehrere Netzwerkschnittstellen vorhanden sind, bezieht sich dieser Wert auf das Gerät eth0 (das Gerät mit der Gerätenummer 0).	01.01.2011
`metrics/vhostmd`	Nicht mehr verfügbar.	2011-05-01
`network/interfaces/macs/mac/device-number`	Die eindeutige Gerätenummer, die mit dieser Schnittstelle verknüpft ist. Die Gerätenummer entspricht dem Gerätenamen; `device-number` 2 steht z. B. für das Gerät eth2. Diese Kategorie entspricht den `device-index` Feldern `DeviceIndex` und, die von der EC2 Amazon-API verwendet werden, und den EC2 Befehlen für AWS CLI.	01.01.2011
`network/interfaces/macs/mac/interface-id`	Die ID der Netzwerkschnittstelle.	01.01.2011
`network/interfaces/macs/mac/ipv4-associations/public-ip`	Die privaten IPv4 Adressen, die jeder öffentlichen IP-Adresse zugeordnet und dieser Schnittstelle zugewiesen sind.	01.01.2011
`network/interfaces/macs/mac/ipv6s`	Die der Schnittstelle zugewiesenen IPv6 Adressen.	2016-06-30

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`network/interfaces/macs/mac/ipv6-prefix`	Das der Netzwerkschnittstelle zugewiesene IPv6 Präfix.	
`network/interfaces/macs/mac/local-hostname`	Der private IPv4 DNS-Hostname der Instanz. Wenn mehrere Netzwerkschnittstellen vorhanden sind, bezieht sich dieser Wert auf das Gerät eth0 (das Gerät mit der Gerätenummer 0). Wenn es sich um eine IPv6 reine Instanz handelt, ist dies der ressourcenbasierte Name. Weitere Informationen zu IPBN und RBN finden Sie unter Hostnamen und Domains der EC2-Instance.	2007-01-19
`network/interfaces/macs/mac/local-ipv4s`	Die privaten IPv4 Adressen, die der Schnittstelle zugeordnet sind. Wenn es sich um eine IPv6 reine Netzwerkschnittstelle handelt, ist dieses Element nicht festgelegt und führt zu einer HTTP 404-Antwort.	01.01.2011
`network/interfaces/macs/mac/mac`	Die MAC-Adresse der Instance	01.01.2011
`network/interfaces/macs/`*`mac`*`/network-card`	Der Index der Netzwerkkarte. Einige Instance-Typen unterstützen mehrere Netzwerkkarten.	01.11.2020

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`network/interfaces/macs/mac/owner-id`	Die ID des Eigentümers der Netzwerkschnittstelle. In Umgebungen mit mehreren Schnittstellen kann eine Schnittstelle von einem Drittanbieter wie ELB hinzugefügt werden. Der Datenverkehr auf einer Schnittstelle wird immer dem Eigentümer der Schnittstelle in Rechnung gestellt.	01.01.2011
`network/interfaces/macs/mac/public-hostname`	Das öffentliche DNS der Schnittstelle (). IPv4 Diese Kategorie wird nur ausgegeben, wenn das Attribut `enableDnsHostnames` auf `true` gesetzt ist. Weitere Infomationen finden Sie unter DNS-Attribute für Ihre VPC im Amazon VPC-Benutzerhandbuch. Wenn die Instanz nur eine öffentliche IPv6 Adresse und keine öffentliche IPv4 Adresse hat, ist dieses Element nicht gesetzt und führt zu einer HTTP 404-Antwort.	01.01.2011
`network/interfaces/macs/mac/public-ipv4s`	Die öffentliche IP-Adresse oder die Elastic IP-Adressen, die dem Adapter zugeordnete sind. Es kann mehrere IPv4 Adressen auf einer Instanz geben.	01.01.2011

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`network/interfaces/macs/mac/security-groups`	Sicherheitsgruppen, zu denen die Netzwerkschnittstelle gehört.	01.01.2011
`network/interfaces/macs/mac/security-group-ids`	Die IDs Sicherheitsgruppen, zu denen die Netzwerkschnittstelle gehört.	01.01.2011
`network/interfaces/macs/mac/subnet-id`	Die ID für das Subnetz, in der sich die Schnittstelle befindet.	01.01.2011
`network/interfaces/macs/mac/subnet-ipv4-cidr-block`	Der IPv4 CIDR-Block des Subnetzes, in dem sich die Schnittstelle befindet.	01.01.2011
`network/interfaces/macs/mac/subnet-ipv6-cidr-blocks`	Der IPv6 CIDR-Block des Subnetzes, in dem sich die Schnittstelle befindet.	2016-06-30
`network/interfaces/macs/mac/vpc-id`	Die ID für die VPC, in der sich die Schnittstelle befindet.	01.01.2011
`network/interfaces/macs/mac/vpc-ipv4-cidr-block`	Der primäre IPv4 CIDR-Block der VPC.	01.01.2011
`network/interfaces/macs/mac/vpc-ipv4-cidr-blocks`	Die IPv4 CIDR-Blöcke für die VPC.	2016-06-30
`network/interfaces/macs/mac/vpc-ipv6-cidr-blocks`	Der IPv6 CIDR-Block der VPC, in dem sich die Schnittstelle befindet.	2016-06-30

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`placement/availability-zone`	Die Availability Zone, in der die Instance gestartet wurde	2008-02-01
`placement/availability-zone-id`	Die statische Availability Zone-ID, in der die Instance gestartet wird. Die Availability Zone-ID ist für alle Konten konsistent. Sie kann sich jedoch von der Availability Zone unterscheiden, die je nach Konto variieren kann.	01.10.2019
`placement/group-name`	Der Name der Platzierungsgruppe, in der die Instance gestartet wird.	24.08.2020
`placement/host-id`	Die ID des Hosts, auf dem die Instance gestartet wird. Gilt nur für Dedicated Hosts.	24.08.2020
`placement/partition-number`	Die Nummer der Partition, in der die Instance gestartet wird.	24.08.2020
`placement/region`	Die AWS Region, in der die Instance gestartet wird.	24.08.2020
`product-codes`	AWS Marketplace Produktcodes, die der Instance zugeordnet sind, falls vorhanden.	2007-03-01

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`public-hostname`	Das öffentliche DNS der Instanz (IPv4). Diese Kategorie wird nur ausgegeben, wenn das Attribut `enableDnsHostnames` auf `true` gesetzt ist. Weitere Infomationen finden Sie unter DNS-Attribute für Ihre VPC im Amazon VPC-Benutzerhandbuch. Wenn die Instanz nur eine öffentliche IPv6 Adresse und keine öffentliche IPv4 Adresse hat, ist dieses Element nicht gesetzt und führt zu einer HTTP 404-Antwort.	2007-01-19
`public-ipv4`	Die öffentliche IPv4 Adresse. Wenn eine Elastic IP-Adresse mit der Instance verknüpft ist, ist der zurückgegebene Wert die Elastic IP-Adresse.	2007-01-19
`public-keys/0/openssh-key`	Der öffentliche Schlüssel. Nur verfügbar, wenn bei der Instance-Startzeit angegeben.	1,0
`ramdisk-id`	Die ID des RAM-Datenträgers, der beim Start angegeben wurde (falls zutreffend)	2007-10-10
`reservation-id`	Die ID der Reservierung	1,0

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`security-groups`	Die Namen der Sicherheitsgruppen für die Instance. Nach dem Start können Sie die Sicherheitsgruppen von Instances ändern. Solche Änderungen spiegeln sich hier und innetwork /interfaces/macs/*mac*/security-groups wider.	1,0
`services/domain`	Die Domain für AWS Ressourcen für die Region.	2014-02-25
`services/partition`	Die Partition, in der sich die Ressource befindet. Für AWS Standardregionen lautet die Partition`aws`. Wenn Sie Ressourcen in anderen Partition en haben, lautet die Partition `aws-`*`partitionname`* . Die Aufteilung der Ressourcen in der Region China (Peking) lautet beispielsweise `aws-cn`.	2015-10-20

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`spot/instance-action`	Die Aktion (in den Ruhezustand versetzen, anhalten oder beenden) sowie den ungefähren Zeitpunkt in UTC, an dem die Aktion ausgeführt wird. Dieses Element ist nur vorhanden, wenn die Spot-Instance für das Versetzen in den Ruhezustand, das Anhalten oder das Beenden markiert wurde. Weitere Informationen finden Sie unter instance-action.	15.11.2016
`spot/termination-time`	Die ungefähre Zeit in UTC, zu der das Betriebssystem für Ihre Spot-Instance das Signal zum Beenden empfängt. Dieser Artikel ist nur dann vorhanden und enthält einen Zeitwert (z. B. 2015-01-05T18:02:00 Z), wenn die Spot-Instance von Amazon zur Kündigung markiert wurde. EC2 Das Element für den Beendigungszeitpunkt enthält keinen Wert, wenn Sie die Spot-Instance selbst beenden. Weitere Informationen finden Sie unter termination-time.	2014-11-05
`system`	Der zugrunde liegende Virtualisierungstyp (Hypervisor) der Instance.	24.09.2022

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`tags/instance`	Die Instance-Tags, die der Instance zugeordnet sind. Nur verfügbar, wenn Sie explizit Zugriff auf Tags in Instance-Metadaten zulassen. Weitere Informationen finden Sie unter Zugriff auf Tags in Instance-Metadaten ermöglichen .	23.03.2021

Kategorien von dynamischen Daten

In der folgenden Tabelle werden die Kategorien von dynamischen Daten aufgeführt.

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`fws/instance-monitoring`	Wert, der angibt, ob der Kunde eine detaillierte einminütige Überwachung aktiviert hat. CloudWatch Zulässige Werte: `enabled | disabled`	2009-04-04
`instance-identity/document`	JSON-Wert mit Instance-Attributen, z. B. Instance-ID, private IP-Adresse, usw. Siehe Instance-Identitätsdokumente für Amazon-EC2-Instances.	2009-04-04
`instance-identity/pkcs7`	Wird verwendet, um die Authentizität und den Inhalt des Dokuments mithilfe der Signatur zu überprüfen. Siehe Instance-Identitätsdokumente für Amazon-EC2-Instances.	2009-04-04

Kategorie	Description	Version, als die Kategorie veröffentlicht wurde
`instance-identity/signature`	Die Daten können von Dritten verwendet werden, um den Ursprung und die Authentizität zu überprüfen. Siehe Instance-Identitätsdokumente für Amazon-EC2-Instances.	2009-04-04

Auf Instanz-Metadaten für eine EC2 Instanz zugreifen

Sie können auf EC2 Instanz-Metadaten innerhalb der Instanz selbst oder über die EC2 Konsole SDKs, API oder die zugreifen AWS CLI. Informationen zum Abrufen der aktuellen Instance-Metadateneinstellungen für eine Instance über die Konsole oder Befehlszeile finden Sie unter Abfragen von Instance-Metadatenoptionen für vorhandene Instances.

Sie können Benutzerdaten für Instances mit einem EBS-Stamm-Volume ändern. Die Instances muss angehalten werden. Eine Anleitung für die Konsole finden Sie unter Instance-Benutzerdaten aktualisieren. Ein Linux-Beispiel, das die verwendet AWS CLI, finden Sie unter modify-instance-attribute. Ein Windows-Beispiel, das die Tools für Windows verwendet PowerShell, finden Sie unterthe section called “Benutzerdaten und die Tools für Windows PowerShell”.

> **Note**
>
> Beachten Sie, dass für HTTP-Anfragen für den Abruf von Instance-Metadaten und Benutzerdaten keine Gebühren berechnet werden.

Überlegungen zum Instance-Zugriff auf Instance-Metadaten

Um Probleme beim Abrufen von Instance-Metadaten zu vermeiden, sollten Sie Folgendes beachten.

Befehlsformat

Das Befehlsformat ist unterschiedlich, je nachdem, ob Sie Instance Metadata Service Version 1 (IMDSv1) oder Instance Metadata Service Version 2 (IMDSv2) verwenden. Standardmäßig

können Sie beide Instance-Metadaten-Services verwenden. Um die Verwendung von IMDSv2 zu erzwingen, lesen Sie Instance-Metadaten-Services für den Zugriff auf Instance-Metadaten verwenden.

Falls IMDSv2 erforderlich, IMDSv1 funktioniert nicht

Wenn Sie es verwenden IMDSv1 und keine Antwort erhalten, IMDSv2 ist dies wahrscheinlich erforderlich. Um zu überprüfen, ob dies erforderlich IMDSv2 ist, wählen Sie die Instanz aus, um ihre Details anzuzeigen. Der IMDSv2Wert gibt entweder Erforderlich (Sie müssen verwenden IMDSv2) oder Optional (Sie können entweder IMDSv2 oder verwendenIMDSv1) an.

(IMDSv2) Wird verwendet/latest/api/token, um das Token abzurufen

Das Ausgeben von PUT-Anfragen an einen beliebigen versionsspezifischen Pfad, beispielsweise `/2021-03-23/api/token`, führt dazu, dass der Metadatenservice „403-Verboten“-Fehler zurückgibt. Dieses Verhalten ist beabsichtigt.

Metadaten-Version

Um zu vermeiden, dass Sie Ihren Code jedes Mal aktualisieren müssen, wenn Amazon einen neuen Instance-Metadaten-Build EC2 veröffentlicht, empfehlen wir, den Pfad und nicht die Versionsnummer zu verwenden`latest`.

IPv6 Unterstützung

Um Instanz-Metadaten mithilfe einer IPv6 Adresse abzurufen, stellen Sie sicher, dass Sie die IPv6 Adresse des IMDS `[fd00:ec2::254]` anstelle der IPv4 Adresse `169.254.169.254` aktivieren und verwenden. Bei der Instance muss es sich um eine Nitro-basierte Instance handeln, die in einem Subnetz gestartet wurde, das Folgendes unterstützt. IPv6

(Windows) Erstellen Sie eine benutzerdefinierte Version AMIs mit Windows Sysprep

Um sicherzustellen, dass IMDS funktioniert, wenn Sie eine Instance von einem benutzerdefinierten Windows-AMI starten, muss das AMI ein standardisiertes Image sein, welches mit Windows Sysprep erstellt wurde. Andernfalls funktioniert der IMDS nicht. Weitere Informationen finden Sie unter Ein Amazon-EC2-AMI mit Windows Sysprep erstellen.

Erwägen Sie in einer Container-Umgebung eine Neukonfiguration oder Erhöhung des Hop-Limits auf 2.

Die AWS SDKs Verwendung IMDSv2 ruft standardmäßig auf. Wenn der IMDSv2 Anruf keine Antwort erhält, AWS SDKs wiederholen einige den Anruf und verwendenIMDSv1, falls er immer noch nicht erfolgreich ist. Dies kann zu einer Verzögerung führen, insbesondere in einer Container-Umgebung. Wenn AWS SDKs das Hop-Limit in einer Container-Umgebung bei 1

liegt, erhält der Anruf bei Bedarf möglicherweise überhaupt keine Antwort, da das Aufrufen des Containers als zusätzlicher Netzwerk-Hop betrachtet wird. IMDSv2

Um diese Probleme in einer Container-Umgebung zu vermeiden, sollten Sie die Konfiguration so ändern, dass Einstellungen (wie z. B. AWS-Region) direkt an den Container übergeben werden, oder erwägen Sie, das Hop-Limit auf 2 zu erhöhen. Informationen zu den Auswirkungen des Hop-Limits finden Sie unter Erweiterte Schutzmaßnahmen gegen offene Firewalls, Reverse-Proxys und SSRF-Schwachstellen mit Verbesserungen am Instanz-Metadatendienst. EC2 Weitere Informationen zum Ändern des Hop-Limits finden Sie unter Ändern des PUT-Antwort-Hop-Limits.

Begrenzen von Paketen pro Sekunde (PPS)

Für Services, die Link-Local-Adressen verwenden, gilt eine Obergrenze von 1 024 Paketen pro Sekunde (PPS). Dieses Limit umfasst die Summe von Route-53-Resolver-DNS-Abfragen, Instance Metadata Service (IMDS)-Anfragen, Amazon Time Service Network Time Protocol (NTP)-Anfragen und Windows-Licensing-Service-Anfragen (für Microsoft Windows-basierte Instances).

Zusätzliche Überlegungen zum Zugriff auf Benutzerdaten

- Benutzerdaten werden als Opaque-Daten behandelt: Was Sie eingeben, wird auch ausgegeben. Die Interpretation der Benutzerdaten und die Instance ist Aufgabe der Instance.
- Benutzerdaten müssen mit Base64 codiert werden. Je nachdem, welches Tool oder SDK Sie verwenden, wird die Base64-Kodierung möglicherweise für Sie durchgeführt. Zum Beispiel:
  - Die EC2 Amazon-Konsole kann die Base64-Kodierung für Sie durchführen oder Base64-kodierte Eingaben akzeptieren.
  - AWS CLI Version 2 führt standardmäßig die Base64-Kodierung von Binärparametern für Sie durch. AWS CLI Version 1 führt die Base64-Kodierung des Parameters für Sie durch. `--user-data`
  - Die AWS SDK für Python (Boto3) führt die Base64-Kodierung des Parameters für Sie durch. `UserData`
- Benutzerdaten sind auf 16 KB an Rohdaten, bevor diese base64-codiert werden, begrenzt. Die Länge einer Zeichenfolge n nach base64-Codierung ist ceil(n/3)*4.
- Benutzerdaten müssen base64-decodiert werden, wenn Sie sie abrufen. Wenn Sie die Daten über Instance-Metadaten oder die Konsole abrufen, werden sie automatisch für Sie dekodiert.
- Wenn Sie eine Instance anhalten, ihre Benutzerdaten ändern und die Instance wieder starten, werden die aktualisierten Benutzerdaten nicht automatisch ausgeführt, wenn Sie die Instance

starten. Bei Windows-Instances können Sie die Einstellungen so konfigurieren, dass aktualisierte Benutzerdatenskripte einmalig beim Starten der Instance oder bei jedem Neustart oder Start der Instance ausgeführt werden.

- Benutzerdaten sind ein Instance-Attribut. Wenn Sie ein AMI auf der Grundlage einer Instance erstellen, sind die Instance-Benutzerdaten nicht im AMI enthalten.

Greifen Sie von einer Instanz aus auf Instanz-Metadaten zu EC2

Da Ihre Instance-Metadaten in Ihrer laufenden Instance verfügbar sind, müssen Sie weder die EC2 Amazon-Konsole noch die verwenden AWS CLI. Dies kann sehr hilfreich sein, wenn Sie ein Skript schreiben möchten, das in der Instance ausgeführt werden soll. So können Sie z. B. über die Instance-Metadaten auf die lokale IP-Adresse Ihrer Instance zugreifen, um die Verbindung zu einer externen Anwendung zu verwalten.

Alle folgenden Daten werden als Instance-Metadaten betrachtet, der Zugriff erfolgt jedoch auf unterschiedliche Weise. Wählen Sie die Registerkarte aus, die den Typ der Instance-Metadaten darstellt, auf die Sie zugreifen möchten, um weitere Informationen zu erhalten.

Metadata

Instance-Metadaten-Eigenschaften werden in Kategorien unterteilt. Eine Beschreibung der einzelnen Instance-Metadatenkategorien finden Sie unter Instance-Metadatenkategorien.

Um von einer laufenden Instance aus auf die Eigenschaften der Instance-Metadaten zuzugreifen, rufen Sie die Daten aus dem Folgenden ab IPv4 oder IPv6 URIs. Die IP-Adressen sind Link-lokale Adressen und nur von der Instance aus gültig. Weitere Informationen finden Sie unter Link-lokale Adressen.

IPv4

```
http://169.254.169.254/latest/meta-data/
```

IPv6

```
http://[fd00:ec2::254]/latest/meta-data/
```

Dynamic data

Verwenden Sie eine der folgenden Methoden, um dynamische Daten aus einer laufenden Instanz abzurufenURIs.

IPv4

```
http://169.254.169.254/latest/dynamic/
```

IPv6

```
http://[fd00:ec2::254]/latest/dynamic/
```

Beispiele: Zugriff mit cURL

Die folgenden Beispiele verwenden cURL, um die High-Level-Instance-Identitätskategorien abzurufen.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/
instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

Beispiele: Zugriff mit PowerShell

In den folgenden Beispielen werden PowerShell die Identitätskategorien für Instanzen auf hoher Ebene abgerufen.

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

Weitere Informationen zu dynamischen Daten und Beispiele dafür, wie sie abgerufen werden können, finden Sie unter Instance-Identitätsdokumente für Amazon-EC2-Instances.

User data

Verwenden Sie eine der folgenden Methoden, um Benutzerdaten aus einer Instanz abzurufen URIs. Um Benutzerdaten mithilfe der IPv6 Adresse abzurufen, müssen Sie sie aktivieren, und die Instance muss eine Nitro-basierte Instance in einem Subnetz sein, das dies unterstützt. IPv6

IPv4

```
http://169.254.169.254/latest/user-data
```

IPv6

```
http://[fd00:ec2::254]/latest/user-data
```

Eine Anfrage für Benutzerdaten geben die Daten unverändert zurück (Content-Type `application/octet-stream`). Wenn die Instance keine Benutzerdaten hat, gibt die Anfrage `404 - Not Found` zurück.

Beispiele: Zugriff mit cURL zum Abrufen von kommagetrenntem Text

Die folgenden Beispiele verwenden cURL, um Benutzerdaten abzurufen, die als kommagetrennter Text angegeben wurden.

IMDSv2

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
curl http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Beispiele: Access with zum Abrufen von PowerShell kommagetrenntem Text

In den folgenden Beispielen werden Benutzerdaten abgerufen PowerShell , die als kommagetrennter Text angegeben wurden.

IMDSv2

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
-Method PUT -Uri http://169.254.169.254/latest/api/token} -Method GET -uri http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Beispiele: Zugriff mit cURL zum Abrufen eines Skripts

Die folgenden Beispiele verwenden cURL, um Benutzerdaten abzurufen, die als Skript angegeben wurden.

IMDSv2

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

IMDSv1

```
curl http://169.254.169.254/latest/user-data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Beispiele: Access with, PowerShell um ein Skript abzurufen

In den folgenden Beispielen PowerShell werden Benutzerdaten abgerufen, die als Skript angegeben wurden.

IMDSv2

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

IMDSv1

```
Invoke-RestMethod -uri http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Abfragen von Instance-Metadatenoptionen für vorhandene Instances

Sie können die Instance-Metadatenoptionen für vorhandene Instances abfragen.

Console

So fragen Sie die Instance-Metadatenoptionen für eine vorhandene Instance ab

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie Ihre Instance aus und überprüfen Sie die folgenden Felder:
   - IMDSv2— Der Wert ist entweder erforderlich oder optional.
   - Tags in Instance-Metadaten zulassen – Der Wert ist entweder Aktiviert oder Deaktiviert.
4. Wenn Sie die Instance ausgewählt haben, wählen Sie Aktionen, Instance-Einstellungen und Instance-Metadatenoptionen ändern.

   Im Dialogfeld wird angezeigt, ob der Instance-Metadatenservice für die ausgewählte Instance aktiviert oder deaktiviert ist.

AWS CLI

So fragen Sie die Instance-Metadatenoptionen für eine vorhandene Instance ab

Verwenden Sie den Befehl describe-instances.

```
aws ec2 describe-instances \
    --instance-id i-1234567898abcdef0 \
    --query 'Reservations[].Instances[].MetadataOptions'
```

PowerShell

Um die Instanz-Metadatenoptionen für eine bestehende Instanz mithilfe der Tools für abzufragen PowerShell

Verwenden Sie das Get-EC2InstanceCmdlet.

```
(Get-EC2Instance `
    -InstanceId i-1234567898abcdef0).Instances.MetadataOptions
```

Antworten und Fehlermeldungen

Alle Instance-Metadaten werden als Text zurückgegeben (HTTP-Inhaltstyp `text/plain`).

Eine Anfrage für eine spezifische Metadatenressource gibt den entsprechenden Wert oder einen HTTP-Fehlercode `404 - Not Found` zurück, wenn die Ressource nicht verfügbar ist.

Eine Anfrage für eine allgemeine Metadatenressource (der URI endet auf „/”) gibt eine Liste der verfügbaren Ressourcen oder einen HTTP-Fehlercode `404 - Not Found` zurück, wenn keine entsprechenden Ressourcen vorhanden sind. Die Listenelemente stehen jeweils in einer eigenen Zeile, d. h. sie sind durch Zeilenvorschübe (ASCII 10) getrennt.

Wenn eine IMDSv1 Anfrage keine Antwort erhält, IMDSv2 ist dies wahrscheinlich erforderlich.

Bei Anfragen, die über gestellt wurden IMDSv2, können die folgenden HTTP-Fehlercodes zurückgegeben werden:

- `400 - Missing or Invalid Parameters` – Die PUT-Anfrage ist nicht gültig.
- `401 - Unauthorized` – Die GET-Anfrage verwendet ein ungültiges Token. Die empfohlene Aktion ist das Erzeugen eines neuen Token.
- `403 - Forbidden` – Die Anfrage ist nicht zulässig oder der IMDS ist deaktiviert.
- `404 - Not Found` – Die Ressource ist nicht verfügbar oder es gibt keine solche Ressource.
- `503` – Die Anforderung konnte nicht abgeschlossen werden. Wiederholen Sie die Anforderung.

Wenn das IMDS einen Fehler zurückgibt, druckt curl die Fehlermeldung in der Ausgabe und gibt einen Erfolgsstatuscode zurück. Die Fehlermeldung wird in der TOKEN-Variablen gespeichert, was dazu führt, dass curl-Befehle, die das Token verwenden, fehlschlagen. Wenn Sie curl mit der -f

Option aufrufen, wird im Falle eines HTTP-Serverfehlers ein Fehlerstatuscode zurückgegeben. Wenn Sie die Fehlerbehandlung aktivieren, kann die Shell den Fehler auffangen und das Skript beenden.

Drosselung abfragen

Wir drosseln die Abfragen an den IMDS pro Instance und begrenzen die Anzahl gleichzeitiger Verbindungen von einer Instance zum IMDS.

Wenn Sie das IMDS zum Abrufen von AWS Sicherheitsanmeldedaten verwenden, vermeiden Sie es, bei jeder Transaktion oder gleichzeitig von einer großen Anzahl von Threads oder Prozessen aus nach Anmeldeinformationen zu fragen, da dies zu einer Drosselung führen kann. Wir empfehlen stattdessen, die Anmeldeinformationen im Cache zu speichern, bis sie sich ihrer Ablaufzeit nähern. Weitere Informationen über die IAM-Rolle und die der Rolle zugeordneten Sicherheitsanmeldeinformationen finden Sie unter Abrufen von Sicherheitsanmeldeinformationen aus Instance-Metadaten.

Wenn es beim Zugriff auf den IMDS zu einer Drosselung kommt, versuchen Sie Ihre Abfrage mit einer exponentiellen Backoff-Strategie erneut.

Instance-Metadaten-Services für den Zugriff auf Instance-Metadaten verwenden

Sie können mit einer der folgenden Methoden auf Instance-Metadaten aus einer laufenden Instance zugreifen:

- Instanz-Metadatendienst Version 2 (IMDSv2) — eine sitzungsorientierte Methode

  Beispiele finden Sie unter Beispiele für IMDSv2.
- Instanz-Metadatendienst Version 1 (IMDSv1) — eine Methode request/response

  Beispiele finden Sie unter Beispiele für IMDSv1.

Standardmäßig können Sie entweder IMDSv1 oder oder IMDSv2 beide verwenden.

Sie können den Instanz-Metadatendienst (IMDS) auf jeder Instanz so konfigurieren, dass er nur IMDSv2 Aufrufe akzeptiert, was dazu führt, dass IMDSv1 Aufrufe fehlschlagen. Informationen darüber, wie Sie Ihre Instance für die Verwendung konfigurieren IMDSv2, finden Sie unterKonfigurieren der Optionen des Instance-Metadaten-Services.

Die GET Header PUT oder sind einzigartig für IMDSv2. Wenn diese Header in der Anfrage enthalten sind, dann ist die Anfrage für vorgesehen. IMDSv2 Wenn keine Header vorhanden sind, wird davon ausgegangen, dass die Anfrage dafür bestimmt ist. IMDSv1

Einen ausführlichen Überblick über dieses Thema IMDSv2 finden Sie unter Erweiterter Schutz vor offenen Firewalls, Reverse-Proxys und SSRF-Sicherheitslücken mit Verbesserungen am Instanz-Metadatendienst. EC2

Themen

- Funktionsweise von Instance-Metadatenservice Version 2
- Verwenden eines unterstützten AWS -SDK
- Beispiele für IMDSv2
- Beispiele für IMDSv1

Funktionsweise von Instance-Metadatenservice Version 2

IMDSv2 verwendet sitzungsorientierte Anfragen. Bei sitzungsorientierten Anforderungen erstellen Sie ein Sitzungs-Token, das die Sitzungsdauer definiert, die mindestens eine Sekunde und maximal sechs Stunden betragen kann. Während der angegebenen Dauer können Sie dasselbe Sitzungs-Token für nachfolgende Anfragen verwenden. Nach Ablauf der angegebenen Dauer müssen Sie ein neues Sitzungs-Token erstellen, das Sie für zukünftige Anfragen verwenden können.

> **Note**
>
> Die Beispiele in diesem Abschnitt verwenden die IPv4 Adresse des Instance Metadata Service (IMDS):. `169.254.169.254` Wenn Sie Instanz-Metadaten für EC2 Instances über die IPv6 Adresse abrufen, stellen Sie sicher, dass Sie stattdessen die IPv6 Adresse aktivieren und verwenden:. `[fd00:ec2::254]` Die IPv6 Adresse des IMDS ist mit Befehlen kompatibel IMDSv2 . Die IPv6 Adresse ist nur auf Nitro-basierten Instances in einem Subnetz zugänglich, das von IPv6 -unterstützt wird (Dual-Stack oder nur). IPv6

In den folgenden Beispielen wird ein Shell-Skript verwendet, IMDSv2 um die Metadatenelemente der Instanz auf oberster Ebene abzurufen. Jedes Beispiel:

- Erstellt ein Sitzungs-Token mit einer Dauer von sechs Stunden (21 600 Sekunden) unter Verwendung der PUT-Anfrage.

- Speichern den Sitzungs-Token-Header in einer Variablen namens `TOKEN` (Linux-Instances) oder `token` (Windows-Instances)
- aFordert die Top-Level-Metadatenelemente über das Token an.

Linux-Beispiel

Sie können zwei separate Befehle ausführen oder kombinieren.

Separate Befehle

Generieren Sie zuerst ein Token mit dem folgenden Befehl.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`
```

Verwenden Sie dann das Token, um mit dem folgenden Befehl Metadatenelemente der obersten Ebene zu generieren.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
```

Kombinierte Befehle

Sie können das Token speichern und die Befehle kombinieren. Das folgende Beispiel kombiniert die beiden obigen Befehle und speichert den Sitzungs-Token-Header in einer Variablen namens TOKEN.

> **Note**
>
> Wenn beim Erstellen des Tokens anstelle eines gültigen Tokens ein Fehler auftritt, wird in der Variablen eine Fehlermeldung gespeichert, und der Befehl funktioniert nicht.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
 && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
```

Nachdem Sie ein Token erstellt haben, können Sie es bis zum Ablauf wiederverwenden. Im folgenden Beispielbefehl, der die ID des AMIs abruft, mit dem die Instance gestartet wurde, wird das im vorherigen Beispiel in `$TOKEN` gespeicherte Token wiederverwendet.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/ami-id
```

Windows-Beispiel

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -
Uri http://169.254.169.254/latest/meta-data/
```

Nachdem Sie ein Token erstellt haben, können Sie es bis zum Ablauf wiederverwenden. Im folgenden Beispielbefehl, der die ID des AMIs abruft, mit dem die Instance gestartet wurde, wird das im vorherigen Beispiel in `$token` gespeicherte Token wiederverwendet.

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
 -Method GET -uri http://169.254.169.254/latest/meta-data/ami-id
```

Wenn Sie IMDSv2 Instanz-Metadaten anfordern, muss die Anfrage Folgendes enthalten:

1. Verwenden Sie eine PUT-Anfrage, um eine Sitzung mit dem Instance-Metadaten-Service zu starten. Die PUT-Anfrage gibt ein Token zurück, das in nachfolgenden GET-Anfragen an den Instance-Metadaten-Service enthalten sein muss. Das Token wird für den Zugriff auf Metadaten mit IMDSv2 benötigt.
2. Nehmen Sie das Token GET in alle Anfragen an den IMDS auf. Wenn die Token-Verwendung auf `required` festgelegt ist, erhalten Anfragen ohne gültiges Token oder mit abgelaufenem Token einen `401 - Unauthorized`-HTTP-Fehlercode.
   - Das Token ist ein Instance-bezogener Schlüssel. Das Token ist auf anderen EC2 Instances nicht gültig und wird abgelehnt, wenn Sie versuchen, es außerhalb der Instanz zu verwenden, auf der es generiert wurde.
   - Die PUT-Anfrage muss einen Header enthalten, der die Time To Live (TTL) für das Token in Sekunden bis zu maximal sechs Stunden (21 600 Sekunden) angibt. Das Token stellt eine logische Sitzung dar. Die TTL gibt die Gültigkeitsdauer des Token und damit die Dauer der Sitzung an.
   - Nachdem ein Token abgelaufen ist, müssen Sie eine neue Sitzung mit einem anderen PUT erstellen, um auf die Instance-Metadaten zuzugreifen.

- Sie können auswählen, ob Sie ein Token wiederverwenden oder bei jeder Anforderung einen neues Token erstellen möchten. Für eine kleine Anzahl von Anfragen kann es einfacher sein, bei jedem Zugriff auf den IMDS ein Token zu generieren und sofort zu verwenden. Aus Effizienzgründen können Sie jedoch eine längere Dauer für das Token festlegen und es wiederverwenden, anstatt jedes Mal eine PUT-Anfrage stellen zu müssen, wenn Sie Instance-Metadaten anfordern müssen. Es gibt kein praktisches Limit für die Anzahl gleichzeitiger Token, von denen jedes für eine eigene Sitzung steht. IMDSv2 ist jedoch immer noch durch normale IMDS-Verbindungs- und Drosselungsgrenzen eingeschränkt. Weitere Informationen finden Sie unter Drosselung abfragen.

In IMDSv2 Instance-Metadatenanfragen sind HTTP GET- und HEAD-Methoden zulässig. PUT-Anfragen werden abgelehnt, wenn sie einen X-Forwarded-For-Header enthalten.

Standardmäßig hat die Antwort auf PUT-Anfragen auf IP-Protokollebene ein Antworthop-Limit (Time To Live) von 1. Wenn Sie ein größeres Hop-Limit benötigen, können Sie es mit dem Befehl anpassen. modify-instance-metadata-options AWS CLI Beispielsweise benötigen Sie möglicherweise eine größeres Hop-Limit für die Abwärtskompatibilität mit Container-Services, die auf der Instance ausgeführt werden. Weitere Informationen finden Sie unter Modifizieren von Instance-Metadatenoptionen für vorhandene Instances.

Verwenden eines unterstützten AWS -SDK

Zur Verwendung IMDSv2 müssen Ihre EC2 Instances eine AWS SDK-Version verwenden, die die Verwendung unterstützt IMDSv2. Die neuesten Versionen aller AWS SDKs unterstützen die Verwendung von IMDSv2.

> **Important**
>
> Wir empfehlen Ihnen, über die SDK-Versionen auf dem Laufenden zu bleiben, um über die neuesten Features, Sicherheitsupdates und zugrunde liegenden Abhängigkeiten informiert zu sein. Die fortgesetzte Verwendung einer nicht unterstützten SDK-Version wird nicht empfohlen und erfolgt nach Ihrem Ermessen. Weitere Informationen finden Sie in den Wartungsrichtlinien für AWS SDKs und Tools im AWS SDKs Referenzhandbuch für Tools.

Im Folgenden sind die Mindestversionen aufgeführt, die die Verwendung von unterstützen IMDSv2:

- AWS CLI – 1.16.289

- AWS Tools for Windows PowerShell – 4.0.1.0
- AWS SDK für .NET – 3.3.634.1
- AWS SDK für C++ – 1.7.229
- AWS SDK für Go – 1.25.38
- AWS SDK for Go v2 — 0.19.0
- AWS SDK für Java – 1.11.678
- AWS SDK for Java 2.x – 2.10.21
- AWS SDK für JavaScript in Node.js — 2.722.0
- AWS SDK für Kotlin – 1,1.4
- AWS SDK für PHP – 3.147.7
- AWS SDK für Python (Botocore) — 1.13.25
- AWS SDK für Python (Boto3) – 1.12.6
- AWS SDK für Ruby – 3.79.0

Beispiele für IMDSv2

Führen Sie die folgenden Beispiele auf Ihrer EC2 Amazon-Instance aus, um die Instance-Metadaten für abzurufen IMDSv2.

Auf Windows-Instanzen können Sie Windows verwenden PowerShell oder cURL oder wget installieren. Wenn Sie ein Drittanbieter-Tool in einer Windows-Instance installieren, sollten Sie die zugehörige Dokumentation unbedingt sorgfältig lesen; die Methode für die Aufrufe und die Ausgabe können von dieser Dokumentation abweichen.

Beispiele

- Abrufen der verfügbaren Versionen der Instance-Metadaten
- Anfordern der Top-Level-Metadatenelemente
- Die Werte für Metadatenelemente abrufen
- Abrufen der Liste der verfügbaren öffentlichen Schlüssel
- Anzeigen der Formate, in denen der öffentliche Schlüssel 0 verfügbar ist
- Anfordern des öffentlichen Schlüssels 0 (im OpenSSH-Schlüsselformat)
- Anfordern der Subnetz-ID für eine Instance
- Abrufen von Instance-Tags für eine Instance

Abrufen der verfügbaren Versionen der Instance-Metadaten

In diesem Beispiel werden die verfügbaren Versionen der Instance-Metadaten abgerufen. Jede Version bezieht sich auf einen Instance-Metadaten-Build, wenn neue Instance-Metadatenkategorien veröffentlicht wurden. Die Build-Versionen der Instance-Metadaten korrelieren nicht mit den EC2 Amazon-API-Versionen. Es stehen frühere Versionen zur Verfügung, für den Fall dass Skripte angewendet werden, die auf den Strukturen und Daten dieser früheren Versionen aufbauen.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
```

```
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

Anfordern der Top-Level-Metadatenelemente

In diesem Beispiel werden die Metadaten-Elemente der obersten Ebene abgerufen. Weitere Informationen zu den einzelnen Punkten in der Antwort finden Sie unter Instance-Metadatenkategorien.

Beachten Sie, dass Tags nur dann in dieser Ausgabe enthalten sind, wenn Sie den Zugriff zugelassen haben. Weitere Informationen finden Sie unter the section called “Zugriff auf Tags in Instance-Metadaten ermöglichen ”.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-life-cycle
```

```
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
```

```
reservation-id
security-groups
services/
tags/
```

Die Werte für Metadatenelemente abrufen

Die folgenden Beispiele zeigen die Werte einiger der Top-Level-Metadatenelemente, die im vorherigen Beispiel abgerufen wurden. Diese Anfragen verwenden das gespeicherte Token, das mit dem Befehl im vorherigen Beispiel erstellt wurde. Das Token darf nicht abgelaufen sein.

cURL

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/reservation-id
r-0efghijk987654321
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

PowerShell

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Abrufen der Liste der verfügbaren öffentlichen Schlüssel

In diesem Beispiel wird die Liste der verfügbaren öffentlichen Schlüssel abgerufen.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/
0=my-public-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

Anzeigen der Formate, in denen der öffentliche Schlüssel 0 verfügbar ist

In diesem Beispiel werden die Formate abgerufen, in denen der öffentliche Schlüssel 0 verfügbar ist.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/
```

```
openssh-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
openssh-key
```

Anfordern des öffentlichen Schlüssels 0 (im OpenSSH-Schlüsselformat)

In diesem Beispiel wird der öffentliche Schlüssel 0 abgerufen (im Format für OpenSSH-Schlüssel).

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Anfordern der Subnetz-ID für eine Instance

In diesem Beispiel wird eine Subnetz-ID für eine Instance vergeben.

cURL

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

PowerShell

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -
Method GET -Uri http://169.254.169.254/latest/meta-data/network/interfaces/
macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Abrufen von Instance-Tags für eine Instance

Wenn der Zugriff auf Instance-Tags in den Instance-Metadaten aktiviert ist, können Sie die Tags für eine Instance aus den Instance-Metadaten abrufen. Weitere Informationen finden Sie unter Abrufen von Tags aus Instance-Metadaten.

Beispiele für IMDSv1

Führen Sie die folgenden Beispiele auf Ihrer EC2 Amazon-Instance aus, um die Instance-Metadaten für abzurufen IMDSv1.

Auf Windows-Instanzen können Sie Windows verwenden PowerShell oder cURL oder wget installieren. Wenn Sie ein Drittanbieter-Tool in einer Windows-Instance installieren, sollten Sie die zugehörige Dokumentation unbedingt sorgfältig lesen; die Methode für die Aufrufe und die Ausgabe können von dieser Dokumentation abweichen.

Beispiele

- Abrufen der verfügbaren Versionen der Instance-Metadaten
- Anfordern der Top-Level-Metadatenelemente
- Die Werte für Metadatenelemente abrufen
- Abrufen der Liste der verfügbaren öffentlichen Schlüssel
- Anzeigen der Formate, in denen der öffentliche Schlüssel 0 verfügbar ist
- Anfordern des öffentlichen Schlüssels 0 (im OpenSSH-Schlüsselformat)
- Anfordern der Subnetz-ID für eine Instance
- Abrufen von Instance-Tags für eine Instance

Abrufen der verfügbaren Versionen der Instance-Metadaten

In diesem Beispiel werden die verfügbaren Versionen der Instance-Metadaten abgerufen. Jede Version bezieht sich auf einen Instance-Metadaten-Build, wenn neue Instance-Metadatenkategorien veröffentlicht wurden. Die Build-Versionen der Instance-Metadaten korrelieren nicht mit den EC2 Amazon-API-Versionen. Es stehen frühere Versionen zur Verfügung, für den Fall dass Skripte angewendet werden, die auf den Strukturen und Daten dieser früheren Versionen aufbauen.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/
```

```
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

Anfordern der Top-Level-Metadatenelemente

In diesem Beispiel werden die Metadaten-Elemente der obersten Ebene abgerufen. Weitere Informationen zu den einzelnen Punkten in der Antwort finden Sie unter Instance-Metadatenkategorien.

Beachten Sie, dass Tags nur dann in dieser Ausgabe enthalten sind, wenn Sie den Zugriff zugelassen haben. Weitere Informationen finden Sie unter the section called “Zugriff auf Tags in Instance-Metadaten ermöglichen ”.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
```

```
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
tags/
```

Die Werte für Metadatenelemente abrufen

Die folgenden Beispiele zeigen die Werte einiger der Top-Level-Metadatenelemente, die im vorherigen Beispiel abgerufen wurden.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Abrufen der Liste der verfügbaren öffentlichen Schlüssel

In diesem Beispiel wird die Liste der verfügbaren öffentlichen Schlüssel abgerufen.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-keys/ 0=my-public-key
```

Anzeigen der Formate, in denen der öffentliche Schlüssel 0 verfügbar ist

In diesem Beispiel werden die Formate abgerufen, in denen der öffentliche Schlüssel 0 verfügbar ist.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/
```

```
openssh-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/0/openssh-key
openssh-key
```

Anfordern des öffentlichen Schlüssels 0 (im OpenSSH-Schlüsselformat)

In diesem Beispiel wird der öffentliche Schlüssel 0 abgerufen (im Format für OpenSSH-Schlüssel).

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
```

```
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Anfordern der Subnetz-ID für eine Instance

In diesem Beispiel wird eine Subnetz-ID für eine Instance vergeben.

cURL

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/
macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

PowerShell

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/network/
interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Abrufen von Instance-Tags für eine Instance

Wenn der Zugriff auf Instance-Tags in den Instance-Metadaten aktiviert ist, können Sie die Tags für eine Instance aus den Instance-Metadaten abrufen. Weitere Informationen finden Sie unter Abrufen von Tags aus Instance-Metadaten.

Übergang zur Verwendung von Instance-Metadatenservice Version 2

Wenn Sie Ihre Instances so konfigurieren möchten, dass sie nur Aufrufe von Instance Metadata Service Version 2 (IMDSv2) akzeptieren, empfehlen wir Ihnen, die folgenden Tools und den folgenden Übergangspfad zu verwenden.

Themen

- Tools für den Übergang zu IMDSv2
- Empfohlener Pfad zur Anforderung IMDSv2

Tools für den Übergang zu IMDSv2

Mit den folgenden Tools können Sie den Übergang Ihrer Software von zu identifizieren, zu überwachen und IMDSv1 zu IMDSv2 verwalten. Anweisungen zur Verwendung dieser Tools finden Sie unterEmpfohlener Pfad zur Anforderung IMDSv2.

AWS Software

Die neuesten Versionen von AWS CLI und AWS SDKs unterstützen IMDSv2. Um zu verwendenIMDSv2, aktualisieren Sie Ihre EC2 Instances, sodass sie die neuesten Versionen verwenden. Die AWS SDK-Mindestversionen, die dies unterstützen IMDSv2, finden Sie unterVerwenden eines unterstützten AWS -SDK.

Alle Amazon Linux 2- und Amazon Linux 2023-Softwarepakete IMDSv2 werden unterstützt. Amazon Linux 2023 ist IMDSv1 standardmäßig deaktiviert.

IMDS-Paket-Analysator

IMDS Packet Analyzer ist ein Open-Source-Tool, das IMDSv1 Aufrufe während der Startphase und der Laufzeitvorgänge Ihrer Instance identifiziert und protokolliert. Durch die Analyse dieser Protokolle können Sie genau identifizieren, welche Software Ihre Instances IMDSv1 aufruft, und bestimmen, welche Software aktualisiert werden muss, damit sie IMDSv2 nur auf Ihren Instances unterstützt wird. Sie können IMDS-Paket-Analysator von der Befehlszeile aus ausführen oder als Service installieren. Weitere Informationen finden Sie AWS ImdsPacketAnalyzerunter GitHub.

CloudWatch

CloudWatch bietet die folgenden zwei Metriken für die Überwachung Ihrer Instances:

`MetadataNoToken`— IMDSv2 verwendet tokengestützte Sitzungen, tut dies aber IMDSv1 nicht. Die `MetadataNoToken` Metrik verfolgt die Anzahl der Aufrufe des Instance Metadata Service (IMDS), die verwendet werden. IMDSv1 Indem Sie diese Metrik bis zum Wert Null nachverfolgen, können Sie feststellen, ob und wann Ihre Software auf IMDSv2 aktualisiert wurde.

`MetadataNoTokenRejected`— Nach der Deaktivierung IMDSv1 können Sie anhand der `MetadataNoTokenRejected` Metrik verfolgen, wie oft ein IMDSv1 Anruf versucht und abgelehnt wurde. Indem Sie diese Metrik verfolgen, können Sie feststellen, ob Ihre Software aktualisiert werden muss, um sie verwenden IMDSv2 zu können.

Weitere Informationen finden Sie unter Instance-Metriken.

Starten APIs

Neue Instanzen: Verwenden Sie die RunInstancesAPI, um neue Instances zu starten, für die die Verwendung von IMDSv2 erforderlich ist. Weitere Informationen finden Sie unter Konfigurieren von Instance-Metadatenoptionen für neue Instances.

Bestehende Instanzen: Verwenden Sie die ModifyInstanceMetadataOptionsAPI, um die Verwendung von IMDSv2 auf vorhandenen Instanzen vorzuschreiben. Weitere Informationen finden Sie unter Modifizieren von Instance-Metadatenoptionen für vorhandene Instances.

Neue Instances, die von Amazon EC2 Auto Scaling Scaling-Gruppen gestartet wurden: Um die Verwendung von IMDSv2 für alle neuen Instances zu verlangen, die von Amazon EC2 Auto Scaling Scaling-Gruppen gestartet wurden, können Ihre Amazon EC2 Auto Scaling Scaling-Gruppen entweder eine Startvorlage oder eine Startkonfiguration verwenden. Wenn Sie eine Startvorlage erstellen oder eine Startkonfiguration erstellen, müssen Sie die `MetadataOptions`-Parameter so konfigurieren, dass die Verwendung von IMDSv2 erforderlich ist. Die Amazon EC2 Auto Scaling Scaling-Gruppe startet neue Instances mit der neuen Startvorlage oder Startkonfiguration, bestehende Instances sind jedoch nicht betroffen.

Bestehende Instances in einer Amazon EC2 Auto Scaling Scaling-Gruppe: Verwenden Sie die ModifyInstanceMetadataOptionsAPI, um die Verwendung von IMDSv2 auf vorhandenen Instances vorzuschreiben, oder beenden Sie die Instances, und die Amazon EC2 Auto Scaling Scaling-Gruppe startet neue Ersatz-Instances mit den Einstellungen der Instance-Metadaten-Optionen, die in der neuen Startvorlage oder Startkonfiguration definiert sind.

AMIs

AMIs konfiguriert mit dem `ImdsSupport` Parameter, der auf gesetzt ist, `v2.0` startet IMDSv2 standardmäßig Instances, die dies erfordern. Amazon Linux 2023 ist konfiguriert mit`ImdsSupport = v2.0`.

Neu AMIs: Verwenden Sie den CLI-Befehl register-image, um den `ImdsSupport` Parameter auf zu setzen, `v2.0` wenn Sie ein neues AMI erstellen.

Existierend AMIs: Verwenden Sie den modify-image-attributeCLI-Befehl, um den `ImdsSupport` Parameter auf festzulegen, `v2.0` wenn Sie ein vorhandenes AMI ändern.

Weitere Informationen finden Sie unter Konfigurieren des AMI.

IAM-Richtlinien und SCPs

Sie können eine IAM-Richtlinie oder eine AWS Organizations Service Control Policy (SCP) verwenden, um Benutzer wie folgt zu kontrollieren:

- Eine Instance kann nicht mithilfe der RunInstancesAPI gestartet werden, es sei denn, die Instance ist für die Verwendung konfiguriert. IMDSv2
- Eine laufende Instanz kann nicht mithilfe der ModifyInstanceMetadataOptionsAPI geändert werden, um sie erneut zu aktivierenIMDSv1.

Die IAM-Richtlinie oder die SCP muss die folgenden IAM-Bedingungsschlüssel enthalten:

- `ec2:MetadataHttpEndpoint`
- `ec2:MetadataHttpPutResponseHopLimit`
- `ec2:MetadataHttpTokens`

Wenn ein Parameter im API- oder CLI-Aufruf nicht mit dem Status übereinstimmt, der in der Richtlinie angegeben ist, die den Bedingungsschlüssel enthält, schlägt der API- oder CLI-Aufruf mit einer `UnauthorizedOperation` Antwort fehl.

Darüber hinaus können Sie eine zusätzliche Schutzebene wählen, um die Änderung von IMDSv1 zu durchzusetzen IMDSv2. Auf der Ebene der Zugriffsverwaltung können Sie in Bezug auf die über die EC2 Rolle APIs aufgerufenen Anmeldeinformationen einen Bedingungsschlüssel entweder in IAM-Richtlinien oder in Richtlinien zur AWS Organizations Dienststeuerung verwenden (SCPs). Insbesondere wenn Sie den Bedingungsschlüssel `ec2:RoleDelivery` mit einem Wert von `2.0` in Ihren IAM-Richtlinien verwenden, IMDSv1 erhalten API-Aufrufe mit EC2 Rollenanmeldedaten von eine `UnauthorizedOperation` Antwort. Das Gleiche kann mit der von einer SCP erzwungenen Bedingung weiter gefasst werden. Dadurch wird sichergestellt, dass die über übermittelten Anmeldeinformationen IMDSv1 nicht tatsächlich zum Aufrufen verwendet werden können APIs , da bei API-Aufrufen, die nicht der angegebenen Bedingung entsprechen, eine `UnauthorizedOperation` Fehlermeldung ausgegeben wird.

Beispiele für IAM-Richtlinien finden Sie unter Arbeiten mit Instance-Metadaten. Weitere Informationen zu SCPs finden Sie im AWS Organizations Benutzerhandbuch unter Richtlinien zur Servicesteuerung.

Deklarative Richtlinien

Verwenden Sie deklarative Richtlinien (eine Funktion von AWS Organizations), um die IMDS-Standardversion zentral festzulegen und unternehmensweit durchzusetzenIMDSv2 . Eine

Beispielrichtlinie finden Sie auf der Registerkarte Standardwerte für Instanz-Metadaten im Abschnitt Unterstützte deklarative Richtlinien im Benutzerhandbuch.AWS Organizations

Empfohlener Pfad zur Anforderung IMDSv2

Unter Verwendung der oben genannten Tools empfehlen wir den folgenden Pfad für den Übergang zuIMDSv2:

- Schritt 1: Identifizieren Sie Instanzen mit IMDSv2 =optional und überprüfen Sie die Nutzung IMDSv1
- Schritt 2: Aktualisieren Sie die Software auf IMDSv2
- Schritt 3: Keine Instanzen erforderlich IMDSv2
- Schritt 4: Stellen Sie IMDSv2 =required als Standard ein
- Schritt 5: Erzwingen Sie, dass für Instances Folgendes erforderlich ist IMDSv2

Schritt 1: Identifizieren Sie Instanzen mit IMDSv2 =optional und überprüfen Sie die Nutzung IMDSv1

Um Ihren IMDSv2 Migrationsumfang einzuschätzen, identifizieren Sie Instanzen, die so konfiguriert sind, dass sie entweder IMDSv1 oder zulassen IMDSv2, und prüfen Sie IMDSv1 Aufrufe.

1. Identifizieren Sie Instanzen, die so konfiguriert sind, dass sie entweder IMDSv1 oder IMDSv2:

   Amazon EC2 console

   1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
   2. Wählen Sie im Navigationsbereich Instances aus.
   3. Um nur die Instances zu sehen, die so konfiguriert sind, dass sie IMDSv1 oder zulassen IMDSv2, fügen Sie den Filter IMDSv2 = optional hinzu.
   4. Um zu sehen, ob dies optional oder für alle Instanzen erforderlich IMDSv2 ist, öffnen Sie alternativ das Einstellungsfenster (Zahnradsymbol) IMDSv2, schalten Sie die Option ein und wählen Sie Bestätigen. Dadurch wird die IMDSv2Spalte zur Instanzen-Tabelle hinzugefügt.

   AWS CLI

   Verwenden Sie den Befehl describe-instances und filtern `metadata-options.http-tokens = optional` Sie wie folgt nach:

```
aws ec2 describe-instances --filters "Name=metadata-options.http-
tokens,Values=optional" --query "Reservations[*].Instances[*].[InstanceId]" --
output text
```

2. IMDSv1 Audit-Aufrufe für jede Instanz:

   Verwenden Sie die CloudWatch Metrik`MetadataNoToken`. Diese Metrik zeigt die Anzahl der IMDSv1 Aufrufe an das IMDS auf Ihren Instances. Weitere Informationen finden Sie unter Instanz-Metriken.

3. Identifizieren Sie die Software auf Ihren Instances, die IMDSv1 Anrufe tätigt:

   Verwenden Sie den Open-Source-IMDS Packet Analyzer, um IMDSv1 Aufrufe während der Startphase und der Laufzeitvorgänge Ihrer Instance zu identifizieren und zu protokollieren. Verwenden Sie diese Informationen, um die Software zu identifizieren, die aktualisiert werden muss, damit Ihre Instances IMDSv2 nur einsatzbereit sind. Sie können IMDS-Paket-Analysator von der Befehlszeile aus ausführen oder als Service installieren.

Schritt 2: Aktualisieren Sie die Software auf IMDSv2

Aktualisieren Sie alle SDKs, und Software CLIs, die Rollenanmeldedaten auf Ihren Instances verwendet, auf IMDSv2 -kompatible Versionen. Weitere Informationen zur Aktualisierung der CLI finden Sie unter Installieren oder Aktualisieren auf die neueste Version der AWS CLI im Benutzerhandbuch für AWS Command Line Interface .

Schritt 3: Keine Instanzen erforderlich IMDSv2

Nachdem Sie anhand der `MetadataNoToken` Metrik bestätigt haben, dass keine IMDSv1 Aufrufe mehr erforderlich sind, konfigurieren Sie Ihre vorhandenen Instances so, dass sie erforderlich sind IMDSv2. Konfigurieren Sie außerdem alle neuen Instanzen so, dass sie erforderlich sind IMDSv2. Mit anderen Worten, deaktivieren Sie es IMDSv1 auf allen vorhandenen und neuen Instanzen.

1. Konfigurieren Sie bestehende Instanzen so, dass sie Folgendes erfordernIMDSv2:

   Amazon EC2 console

   1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
   2. Wählen Sie im Navigationsbereich Instances aus.
   3. Wählen Sie Ihre Instance aus.

4. Wählen Sie Aktionen, Instance-Einstellungen und Instance-Metadata-Optionen ändern.
5. Wählen Sie für IMDSv2Erforderlich aus.
6. Wählen Sie Speichern.

AWS CLI

Verwenden Sie den modify-instance-metadata-optionsCLI-Befehl, um anzugeben, IMDSv2 dass nur verwendet werden soll.

> **Note**
>
> Sie können diese Einstellung bei laufenden Instances ändern. Die Änderung wird sofort wirksam, ohne dass ein Neustart der Instanz erforderlich ist.

Weitere Informationen finden Sie unter Erfordern die Verwendung von IMDSv2.

2. Achten Sie nach der Deaktivierung IMDSv1 auf Probleme:
   1. Verfolgen Sie anhand der `MetadataNoTokenRejected` CloudWatch Metrik, wie oft ein IMDSv1 Anruf versucht und abgelehnt wurde.
   2. Wenn die `MetadataNoTokenRejected` Metrik IMDSv1 Aufrufe einer Instanz aufzeichnet, bei der Softwareprobleme auftreten, bedeutet dies, dass die Software aktualisiert werden muss, damit sie verwendet IMDSv2 werden kann.
3. Konfigurieren Sie neue Instanzen so, dass sie Folgendes erfordernIMDSv2:

   Amazon EC2 console

   1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
   2. Folgen Sie den Schritten, um eine Instance zu starten.
   3. Erweitern Sie Erweiterte Details und wählen Sie als Metadaten-Version nur V2 aus (Token erforderlich).
   4. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus.

      Weitere Informationen finden Sie unter Konfigurieren der Instance beim Start.

AWS CLI

AWS CLI: Verwenden Sie den Befehl run-instances und geben Sie an, dass dies erforderlich IMDSv2 ist.

Schritt 4: Stellen Sie IMDSv2 =required als Standard ein

Sie können IMDSv2 =required als Standardkonfiguration entweder auf Konto- oder Organisationsebene festlegen. Dadurch wird sichergestellt, dass alle neu gestarteten Instances automatisch so konfiguriert werden, dass sie Folgendes benötigen IMDSv2.

1. Legen Sie den Standard auf Kontoebene fest:

   Amazon EC2 console

   1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
   2. Wählen Sie im EC2 Dashboard unter Kontoattribute die Option Datenschutz und Sicherheit aus.
   3. Wählen Sie unter IMDS-Standardeinstellungen die Option Verwalten aus.
   4. Wählen Sie für Instance-Metadaten-Service die Option Aktiviert aus.
   5. Wählen Sie für die Metadatenversion nur V2 aus (Token erforderlich).
   6. Wählen Sie Aktualisieren aus.

   AWS CLI

   Verwenden Sie den modify-instance-metadata-defaultsCLI-Befehl und geben Sie `--http-tokens required` und an`--http-put-response-hop-limit 2`.

   Weitere Informationen finden Sie unter IMDSv2 Als Standard für das Konto festlegen.

2. Alternativ können Sie mithilfe einer deklarativen Richtlinie den Standard auf Organisationsebene festlegen:

   Verwenden Sie eine deklarative Richtlinie, um den Organisationsstandard für auf erforderlich festzulegen. IMDSv2 Eine Beispielrichtlinie finden Sie auf der Registerkarte Standardwerte

für Instanz-Metadaten im Abschnitt Unterstützte deklarative Richtlinien im AWS Organizations Benutzerhandbuch.

Schritt 5: Erzwingen Sie, dass für Instances Folgendes erforderlich ist IMDSv2

Verwenden Sie die folgenden IAM- oder SCP-Bedingungsschlüssel, um die Verwendung zu erzwingen IMDSv2 :

- `ec2:MetadataHttpTokens`
- `ec2:MetadataHttpPutResponseHopLimit`
- `ec2:MetadataHttpEndpoint`

Diese Bedingungsschlüssel steuern die Verwendung von RunInstancesModifyInstanceMetadataOptions APIs und den entsprechenden. CLIs Wenn eine Richtlinie erstellt wird und ein Parameter im API-Aufruf nicht mit dem in der Richtlinie über den Bedingungsschlüssel angegebenen Status übereinstimmt, schlägt der API- oder CLI-Aufruf mit einer `UnauthorizedOperation`-Antwort fehl.

Beispiele für IAM-Richtlinien finden Sie unter Arbeiten mit Instance-Metadaten.

Zugriff auf den Instance-Metadaten-Service einschränken

Sie können die Verwendung lokaler Firewall-Regeln in Betracht ziehen, um den Zugriff auf den Instance Metadata Service (IMDS) für einige oder alle Prozesse zu deaktivieren.

Bei Nitro-basierten Instances kann das IMDS von Ihrem eigenen Netzwerk aus erreicht werden, wenn eine Netzwerk-Appliance innerhalb Ihrer VPC, beispielsweise ein virtueller Router, Pakete an die IMDS-Adresse weiterleitet und die Standard-Quell-/Zielprüfung der Instance deaktiviert ist. Um zu verhindern, dass eine Quelle von außerhalb Ihrer VPC den IMDS erreicht, empfehlen wir Ihnen, die Konfiguration der Netzwerk-Appliance so zu ändern, dass Pakete mit der IPv4 Zieladresse des IMDS `169.254.169.254` und, falls Sie den IPv6 Endpunkt aktiviert haben, der IPv6 Adresse des IMDS verworfen werden. `[fd00:ec2::254]`

IMDS-Zugriff für Linux-Instances einschränken

Verwendung von iptables zur Einschränkung des Zugriffs

Das folgende Beispiel verwendet Linux-iptables und sein `owner`-Modul, um zu verhindern, dass der Apache-Webserver (basierend auf seiner Standardinstallationsbenutzer-ID von `apache`) auf

169.254.169.254 zugreift. Es verwendet eine Ablehnungsregel, um alle Instanz-Metadatenanfragen (unabhängig davon, ob IMDSv1 oder IMDSv2) von Prozessen, die unter diesem Benutzer ausgeführt werden, abzulehnen.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner
 --uid-owner apache --jump REJECT
```

Oder Sie können erwägen, nur bestimmten Benutzern oder Gruppen Zugriff zu gewähren, indem Sie Zulassungsregeln verwenden. Zulassungsregeln können aus Sicherheitssicht einfacher zu verwalten sein, da Sie eine Entscheidung darüber treffen müssen, welche Software Zugriff auf Instance-Metadaten benötigt. Wenn Sie Zulassungsregeln verwenden, ist es weniger wahrscheinlich, dass Sie Software versehentlich den Zugriff auf den Metadaten-Service erlauben (auf den sie nicht zugreifen soll), wenn Sie später die Software oder Konfiguration auf einer Instance ändern. Sie können außerdem Gruppen mit Zulassungsregeln kombinieren, sodass Sie Benutzer zu einer zugelassenen Gruppe hinzufügen und aus dieser entfernen können, ohne die Firewall-Regel ändern zu müssen.

Das folgende Beispiel verhindert den Zugriff auf den IMDS durch alle Prozesse, mit Ausnahme von Prozessen, die im Benutzerkonto `trustworthy-user` ausgeführt werden.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match
 owner ! --uid-owner trustworthy-user --jump REJECT
```

> **Note**
>
> - Um lokale Firewall-Regeln zu verwenden, müssen Sie die vorhergehenden Beispielbefehle an Ihre Bedürfnisse anpassen.
> - Standardmäßig sind iptables-Regeln nicht über Systemneustarts hinweg persistent. Sie können durch die Verwendung von Betriebssystemfeatures, die hier nicht beschrieben werden, persistent gestaltet werden.
> - Das iptables `owner`-Modul überprüft nur dann die Gruppenzugehörigkeit, wenn die Gruppe die Primärgruppe eines bestimmten lokalen Benutzers ist. Andere Gruppen werden nicht abgeglichen.

Verwendung von PF oder IPFW zur Einschränkung des Zugriffs

Wenn Sie FreeBSD oder OpenBSD verwenden, können Sie überlegen, PF oder IPFW zu verwenden. Die folgenden Beispiele beschränken den Zugriff auf den IMDS auf den Root-Benutzer.

PF

```
$ block out inet proto tcp from any to 169.254.169.254
```

```
$ pass out inet proto tcp from any to 169.254.169.254 user root
```

IPFW

```
$ allow tcp from any to 169.254.169.254 uid root
```

```
$ deny tcp from any to 169.254.169.254
```

> **Note**
>
> Die Reihenfolge der PF- und IPFW-Befehle ist von Bedeutung. PF verwendet standardmäßig die letzte übereinstimmende Regel und IPFW die erste übereinstimmende Regel.

IMDS-Zugriff für Windows-Instances einschränken

Verwenden der Windows-Firewall zur Zugriffsbeschränkung

Im folgenden PowerShell Beispiel wird die integrierte Windows-Firewall verwendet, um zu verhindern, dass der Internet Information Server-Webserver (basierend auf seiner standardmäßigen Installationsbenutzer-ID von`NT AUTHORITY\IUSR`) auf 169.254.169.254 zugreift. Es verwendet eine Ablehnungsregel, um alle Instanz-Metadatenanforderungen (unabhängig davon, ob IMDSv1 oderIMDSv2) von Prozessen, die unter diesem Benutzer ausgeführt werden, abzulehnen.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount ("NT
 AUTHORITY\IUSR")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $BlockPrincipalSDDL = "D:(A;;CC;;;$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service from IIS" -Action
 block -Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $BlockPrincipalSDDL
```

Oder Sie können erwägen, nur bestimmten Benutzern oder Gruppen Zugriff zu gewähren, indem Sie Zulassungsregeln verwenden. Zulassungsregeln können aus Sicherheitssicht einfacher zu verwalten

sein, da Sie eine Entscheidung darüber treffen müssen, welche Software Zugriff auf Instance-Metadaten benötigt. Wenn Sie Zulassungsregeln verwenden, ist es weniger wahrscheinlich, dass Sie Software versehentlich den Zugriff auf den Metadaten-Service erlauben (auf den sie nicht zugreifen soll), wenn Sie später die Software oder Konfiguration auf einer Instance ändern. Sie können außerdem Gruppen mit Zulassungsregeln kombinieren, sodass Sie Benutzer zu einer zugelassenen Gruppe hinzufügen und aus dieser entfernen können, ohne die Firewall-Regel ändern zu müssen.

Das folgende Beispiel verhindert den Zugriff auf Instance-Metadaten durch alle Prozesse, die als OS-Gruppe ausgeführt werden, die in der Variable `blockPrincipal` angegeben ist (in diesem Beispiel die Windows-Gruppe `Everyone`), mit Ausnahme der in `exceptionPrincipal` angegebenen Prozesse (in diesem Beispiel eine Gruppe namens `trustworthy-users`). Sie müssen für Prinzipale den Zugriff verweigern und ablehnen, da die Windows-Firewall im Gegensatz zur `! --uid-owner trustworthy-user`-Regel in Linux-iptables keinen Mechanismus zur Verfügung stellt, um nur einen bestimmten Prinzipal (Benutzer oder Gruppe) zuzulassen, indem alle anderen abgelehnt werden.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("Everyone")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $exceptionPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("trustworthy-users")
PS C:\> $ExceptionPrincipalSID =
 $exceptionPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $PrincipalSDDL = "O:LSD:(D;;CC;;;$ExceptionPrincipalSID)(A;;CC;;;
$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service for
 $($blockPrincipal.Value), exception: $($exceptionPrincipal.Value)" -Action block -
Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $PrincipalSDDL
```

> **Note**
>
> Um lokale Firewall-Regeln zu verwenden, müssen Sie die vorhergehenden Beispielbefehle an Ihre Bedürfnisse anpassen.

Verwenden von netsh-Regeln zur Zugriffsbeschränkung

Sie können erwägen, die gesamte Software mit `netsh`-Regeln zu blockieren. Diese sind jedoch viel weniger flexibel.

```
C:\> netsh advfirewall firewall add rule name="Block metadata service altogether"
 dir=out protocol=TCP remoteip=169.254.169.254 action=block
```

> **Note**
>
> - Um lokale Firewall-Regeln zu verwenden, müssen Sie die vorhergehenden Beispielbefehle an Ihre Bedürfnisse anpassen.
> - `netsh`-Regeln müssen von einer Eingabeaufforderung mit erhöhten Rechten aus festgelegt werden und können nicht so konfiguriert werden, dass sie bestimmte Prinzipale verweigern oder zulassen.

Konfigurieren der Optionen des Instance-Metadaten-Services

Der Instanz-Metadatendienst (IMDS) wird lokal auf jeder EC2 Instanz ausgeführt. Die Optionen für Instanz-Metadaten beziehen sich auf eine Reihe von Konfigurationen, die den Zugriff und das Verhalten des IMDS auf einer EC2 Instanz steuern.

Sie können die folgenden Optionen für Instance-Metadaten für jede Instance konfigurieren:

Instance Metadata Service (IMDS): `enabled` | `disabled`

Sie können den IMDS auf einer Instance aktivieren oder deaktivieren. Wenn diese Option deaktiviert ist, können Sie oder ein anderer Code nicht auf die Instance-Metadaten auf der Instance zugreifen.

Das IMDS hat zwei Endpunkte auf einer Instanz: IPv4 (`169.254.169.254`) und IPv6 (). `[fd00:ec2::254]` Wenn Sie das IMDS aktivieren, wird der IPv4 Endpunkt automatisch aktiviert. Wenn Sie den IPv6 Endpunkt aktivieren möchten, müssen Sie dies explizit tun.

IPv6 IMDS-Endpunkt: | `enabled` `disabled`

Sie können den IPv6 IMDS-Endpunkt auf einer Instanz explizit aktivieren. Wenn der IPv6 Endpunkt aktiviert ist, bleibt der IPv4 Endpunkt aktiviert. Der IPv6 Endpunkt wird nur auf Nitro-basierten Instances in Subnetzen unterstützt, die IPv6 von -unterstützt werden (Dual Stack oder IPv6 nur).

Metadaten-Version: `IMDSv1 or IMDSv2 (token optional)` | `IMDSv2 only (token required)`

Bei der Anforderung von Instanz-Metadaten ist für IMDSv2 Aufrufe ein Token erforderlich. IMDSv1Für Aufrufe ist kein Token erforderlich. Sie können eine Instanz so konfigurieren, dass sie entweder IMDSv1 oder IMDSv2 -Aufrufe zulässt (wobei ein Token optional ist) oder dass sie nur IMDSv2 Aufrufe zulässt (wenn ein Token erforderlich ist).

Metadaten-Antwort-Hop-Limits: 1–64

Das Hop-Limit ist die Anzahl der Netzwerk-Hops, die PUT-Antwort ausführen darf. Sie können das Hop-Limit auf ein Minimum von 1 und ein Maximum von 64 festlegen. In einer Container-Umgebung kann ein Hop-Limit von 1 zu Problemen führen. Informationen zur Behebung dieser Probleme finden Sie in den Informationen zu Containerumgebungen unter Überlegungen zum Instance-Zugriff auf Instance-Metadaten.

Zugriffs auf Tags in Instance-Metadaten: `enabled` | `disabled`

Sie können den Zugriff auf die Tags der Instance in den Metadaten der Instance aktivieren oder deaktivieren. Weitere Informationen finden Sie unter Zeigen Sie Tags für Ihre EC2 Instances mithilfe von Instanz-Metadaten an.

Informationen zum Anzeigen der aktuellen Konfiguration einer Instance finden Sie unter Abfragen von Instance-Metadatenoptionen für vorhandene Instances.

Konfigurieren der Instance-Metadaten-Optionen

Die Optionen für Instance-Metadaten können wie folgt auf verschiedenen Ebenen konfiguriert werden:

- Konto – Sie können Standardwerte für die Instance-Metadatenoptionen auf Kontoebene für jede AWS-Region festlegen. Wenn eine Instance gestartet wird, werden die Optionen für die Instance-Metadaten automatisch auf die Werte auf Kontoebene festgelegt. Sie können diese Werte beim Start ändern. Standardwerte auf Kontoebene wirken sich nicht auf bestehende Instances aus.
- AMI – Wenn Sie ein neues AMI registrieren oder ein vorhandenes AMI ändern, können Sie den Parameter `imds-support` auf `v2.0` setzen. Wenn eine Instance mit diesem AMI gestartet wird, wird die Version der Instance-Metadaten automatisch auf IMDSv2 und das Hop-Limit auf 2 gesetzt.
- Instance – Sie können alle Optionen für Instance-Metadaten einer Instance beim Start ändern und dabei die Standardeinstellungen überschreiben. Sie können auch nach dem Start auf einer

ausgeführten oder angehaltenen Instance die Instance-Metadaten-Optionen ändern. Beachten Sie, dass Änderungen möglicherweise durch eine IAM- oder SCP-Richtlinie eingeschränkt werden.

Weitere Informationen erhalten Sie unter Konfigurieren von Instance-Metadatenoptionen für neue Instances und Modifizieren von Instance-Metadatenoptionen für vorhandene Instances.

Rangfolge der Optionen für Instance-Metadaten

Der Wert für jede Instance-Metadatenoption wird beim Start der Instance in einer hierarchischen Rangfolge festgelegt. Die Hierarchie mit der höchsten Priorität an oberster Stelle sieht wie folgt aus:

- Priorität 1: Instance-Konfiguration beim Start – Werte können entweder in der Startvorlage oder in der Instance-Konfiguration angegeben werden. Alle hier angegebenen Werte haben Vorrang vor Werten, die auf Kontoebene oder im AMI angegeben wurden.
- Priorität 2: Kontoeinstellungen — Wenn beim Start der Instance kein Wert angegeben wird, wird er durch die Einstellungen auf Kontoebene bestimmt (die für jede Instanz festgelegt sind). AWS-Region Einstellungen auf Kontoebene enthalten entweder einen Wert für jede Metadatenoption oder geben an, dass überhaupt keine Präferenz ausgewählt wird.
- Priorität 3: AMI-Konfiguration – Wenn beim Start der Instance oder auf Kontoebene kein Wert angegeben wird, wird er durch die AMI-Konfiguration bestimmt. Dies gilt nur für `HttpTokens` und `HttpPutResponseHopLimit`.

Jede Metadatenoption wird separat bewertet. Die Instance kann mit einer Mischung aus direkter Instance-Konfiguration, Standardeinstellungen auf Kontoebene und der Konfiguration aus dem AMI konfiguriert werden.

Sie können den Wert jeder Metadatenoption nach dem Start einer laufenden oder angehaltenen Instance ändern, sofern die Änderungen nicht durch eine IAM- oder SCP-Richtlinie eingeschränkt sind.

Ermitteln der Werte für Metadatenoptionen – Beispiel 1

In diesem Beispiel wird eine EC2 Instance in einer Region gestartet, in der der Wert auf `1` Kontoebene festgelegt `HttpPutResponseHopLimit` ist. Das angegebene AMI hat `ImdsSupport` auf `v2.0` eingestellt. Beim Start werden keine Metadatenoptionen direkt auf der Instance angegeben. Die Instance wird mit den folgenden Metadatenoptionen gestartet:

```
"MetadataOptions": {
```

```
    ...
    "HttpTokens": "required",
    "HttpPutResponseHopLimit": 1,
    ...
```

Diese Werte wurden wie folgt bestimmt:

- Beim Start wurden keine Metadatenoptionen angegeben: Beim Start der Instance wurden weder in den Instance-Startparametern noch in der Startvorlage spezifische Werte für die Metadatenoptionen angegeben.
- Kontoeinstellungen haben als Nächstes Vorrang: Wenn beim Start keine spezifischen Werte angegeben wurden, haben die Einstellungen auf Kontoebene innerhalb der Region Vorrang. Das bedeutet, dass die auf Kontoebene konfigurierten Standardwerte angewendet werden. In diesem Fall wurde der `HttpPutResponseHopLimit` auf `1` gesetzt.
- AMI-Einstellungen haben letzten Vorrang: Wenn beim Start oder auf Kontoebene kein bestimmter Wert angegeben wurde für `HttpTokens` (die Instance-Metadatenversion), wird die AMI-Einstellung angewendet. In diesem Fall wurde anhand der AMI-Einstellung `ImdsSupport: v2.0` festgelegt, dass `HttpTokens` auf `required` eingestellt war. Beachten Sie, dass die AMI-Einstellung `ImdsSupport: v2.0` zwar für die Einstellung `HttpPutResponseHopLimit: 2` vorgesehen ist, sie jedoch durch die Einstellung `HttpPutResponseHopLimit: 1` auf Kontoebene, die höhere Priorität hat, außer Kraft gesetzt wurde.

Ermitteln der Werte für Metadatenoptionen – Beispiel 2

In diesem Beispiel wird die EC2 Instance mit den gleichen Einstellungen wie im vorherigen Beispiel 1 gestartet, allerdings mit der `HttpTokens` Einstellung `optional` direkt auf der Instance beim Start. Die Instance wird mit den folgenden Metadatenoptionen gestartet:

```
"MetadataOptions": {
    ...
    "HttpTokens": "optional",
    "HttpPutResponseHopLimit": 1,
    ...
```

Der Wert für `HttpPutResponseHopLimit` wird auf die gleiche Weise wie in Beispiel 1 bestimmt. Der Wert für `HttpTokens` wird jedoch wie folgt bestimmt: Metadatenoptionen, die beim Start auf der Instance konfiguriert wurden, haben Vorrang. Obwohl das AMI mit `ImdsSupport: v2.0` konfiguriert

war (mit anderen Worten `HttpTokens` ist auf`required` gesetzt), hatte der Wert, der beim Start auf der Instance angegeben wurde (`HttpTokens` gesetzt auf `optional`), Vorrang.

Version der Instance-Metadaten festlegen

Wenn eine Instance gestartet wird, ist der Wert für die Version der Instance-Metadaten entweder `IMDSv1 or IMDSv2 (token optional)` oder `IMDSv2 only (token required)`.

Beim Start der Instance können Sie den Wert für die Metadatenversion entweder manuell angeben oder den Standardwert verwenden. Wenn Sie den Wert manuell angeben, überschreibt er alle Standardwerte. Wenn Sie den Wert nicht manuell angeben möchten, wird er durch eine Kombination von Standardeinstellungen bestimmt, wie in der folgenden Tabelle beschrieben.

Die Tabelle zeigt, wie die Metadatenversion für eine Instance beim Start (angezeigt durch Resultierende Instance-Konfiguration in Spalte 4) durch die Einstellungen auf den verschiedenen Konfigurationsebenen bestimmt wird. Die Rangfolge erfolgt von links nach rechts, wobei die erste Spalte den höchsten Vorrang hat, und zwar wie folgt:

- Spalte 1: Startparameter – Stellt die Einstellung für die Instance dar, die Sie beim Start manuell angeben.
- Spalte 2: Standard auf Kontoebene – Stellt die Einstellung für das Konto dar.
- Spalte 3: AMI-Standard – Stellt die Einstellung auf dem AMI dar.

Startparameter	Standard auf Kontoebene	Standard-AMI	Resultierende Instance-Konfiguration
Nur V2 (Token erforderlich)	Keine Präferenz	Nur V2	Nur V2
Nur V2 (Token erforderlich)	Nur V2	Nur V2	Nur V2
Nur V2 (Token erforderlich)	V1 oder V2	Nur V2	Nur V2
V1 oder V2 (Token optional)	Keine Präferenz	Nur V2	V1 oder V2

Startparameter	Standard auf Kontoebene	Standard-AMI	Resultierende Instance-Konfiguration
V1 oder V2 (Token optional)	Nur V2	Nur V2	V1 oder V2
V1 oder V2 (Token optional)	V1 oder V2	Nur V2	V1 oder V2
Nicht gesetzt	Keine Präferenz	Nur V2	Nur V2
Nicht gesetzt	Nur V2	Nur V2	Nur V2
Nicht gesetzt	V1 oder V2	Nur V2	V1 oder V2
Nur V2 (Token erforderlich)	Keine Präferenz	Null	Nur V2
Nur V2 (Token erforderlich)	Nur V2	Null	Nur V2
Nur V2 (Token erforderlich)	V1 oder V2	Null	Nur V2
V1 oder V2 (Token optional)	Keine Präferenz	Null	V1 oder V2
V1 oder V2 (Token optional)	Nur V2	Null	V1 oder V2
V1 oder V2 (Token optional)	V1 oder V2	Null	V1 oder V2
Nicht gesetzt	Keine Präferenz	Null	V1 oder V2
Nicht gesetzt	Nur V2	Null	Nur V2
Nicht gesetzt	V1 oder V2	Null	V1 oder V2

Verwenden Sie IAM-Bedingungsschlüssel, um die Optionen für Instance-Metadaten einzuschränken

Sie können auch IAM-Bedingungsschlüssel in einer IAM-Richtlinie oder SCP wie folgt verwenden:

- Zulassen, dass eine Instance nur gestartet wird, wenn sie so konfiguriert ist, dass sie die Verwendung von IMDSv2 erzwingt
- Beschränken der Anzahl der zulässigen Hops
- Deaktivieren des Zugriffs auf Instance-Metadaten

Aufgaben

- Konfigurieren von Instance-Metadatenoptionen für neue Instances
- Modifizieren von Instance-Metadatenoptionen für vorhandene Instances

> **Note**
>
> Sie sollten vorsichtig vorgehen und sorgfältige Tests durchführen, bevor Sie Änderungen vornehmen. Beachten Sie die folgenden Punkte:
>
> - Wenn Sie die Verwendung von erzwingen IMDSv2, wird der Zugriff auf Metadaten IMDSv1 für Anwendungen oder Agenten unterbrochen.
> - Wenn Sie den gesamten Zugriff auf Instance-Metadaten deaktivieren, werden Anwendungen oder Agenten, die auf Instance-Metadaten angewiesen sind, den Zugriff auf die Funktion verlieren.
> - Denn IMDSv2 müssen Sie `/latest/api/token` beim Abrufen des Tokens verwenden.
> - (Nur Windows) Wenn Ihre PowerShell Version älter als 4.0 ist, müssen Sie auf Windows Management Framework 4.0 aktualisieren, um die Verwendung von IMDSv2 zu erfordern.

Konfigurieren von Instance-Metadatenoptionen für neue Instances

Sie können die folgenden Instance-Metadatenoptionen für neue Instances konfigurieren.

Optionen

- Erzwingen der Verwendung von IMDSv2

- Aktivieren Sie das IMDS IPv4 und die Endpoints IPv6
- Deaktivieren des Zugriffs auf Instance-Metadaten
- Zulassen des Zugriffs auf Tags in Instance-Metadaten

> **Note**
>
> Diese Einstellung wird auf Kontoebene konfiguriert, entweder direkt im Konto oder mithilfe einer deklarativen Richtlinie. Sie müssen in jeder AWS-Region konfiguriert werden, in der Sie die Optionen für Instance-Metadaten konfigurieren möchten. Mithilfe einer deklarativen Richtlinie können Sie die Einstellung auf mehrere Regionen gleichzeitig, sowie auf mehrere Konten gleichzeitig anwenden. Wenn eine deklarative Richtlinie verwendet wird, können Sie die Einstellung nicht direkt in einem Konto ändern. In diesem Thema wird beschrieben, wie Sie die Einstellung direkt in einem Konto konfigurieren. Informationen zur Verwendung deklarativer Richtlinien finden Sie unter Deklarative Richtlinien im AWS Organizations - Benutzerhandbuch.

Erzwingen der Verwendung von IMDSv2

Sie können die folgenden Methoden verwenden, um die Verwendung von für IMDSv2 Ihre neuen Instances vorzuschreiben.

Um zu benötigen IMDSv2

- IMDSv2 Als Standard für das Konto festlegen
- Konfigurieren der Instance beim Start
- Konfigurieren des AMI
- Verwenden einer IAM-Richtlinie

IMDSv2 Als Standard für das Konto festlegen

Sie können die Standardversion für den Instanz-Metadaten-Service (IMDS) jeweils AWS-Region auf Kontoebene festlegen. Das heißt, wenn Sie eine neue Instance starten, wird die Instance-Metadatenversion automatisch auf den Standard auf Kontoebene gesetzt. Sie können den Wert jedoch beim Start oder nach dem Start manuell überschreiben. Weitere Informationen darüber, wie sich Einstellungen auf Kontoebene und manuelle Überschreibungen auf eine Instance auswirken, finden Sie unter Rangfolge der Optionen für Instance-Metadaten.

> **Note**
>
> Durch das Festlegen der Standardeinstellung auf Kontoebene werden bestehende Instances nicht zurückgesetzt. Wenn Sie beispielsweise die Standardeinstellung auf Kontoebene auf festlegen, sind alle vorhandenen Instanzen IMDSv2, die auf festgelegt sind, nicht betroffen IMDSv1 . Wenn Sie den Wert für bestehende Instances ändern möchten, müssen Sie den Wert für die Instances selbst manuell ändern.

Sie können den Kontostandard für die Version der Instanz-Metadaten auf festlegen, IMDSv2 sodass alle neuen Instances im Konto mit IMDSv2 erforderlich gestartet werden und deaktiviert IMDSv1 werden. Bei diesem standardmäßigen Konto gelten beim Start einer Instance die folgenden Standardwerte für die Instance:

- Konsole: Die Metadatenversion ist nur auf V2 festgelegt (Token erforderlich) und das Limit für den Metadaten-Response-Hop ist auf 2 festgelegt.
- AWS CLI: `HttpTokens` ist auf `required` gesetzt und `HttpPutResponseHopLimit` ist auf 2 gesetzt.

> **Note**
>
> Bevor Sie den Kontostandard auf festlegen IMDSv2, stellen Sie sicher, dass Ihre Instances nicht von abhängig sind IMDSv1. Weitere Informationen finden Sie unter Empfohlener Pfad zur Anforderung IMDSv2.

Console

Um es IMDSv2 als Standard für das Konto für die angegebene Region festzulegen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich Dashboard aus. EC2
4. Wählen Sie unter Kontoattribute die Option Datenschutz und Sicherheit aus.
5. Wählen Sie neben IMDS-Standardeinstellungen die Option Verwalten aus.

6. Gehen Sie auf der Seite IMDS-Standardwerte verwalten wie folgt vor:

   a. Für den Instance-Metadaten-Services wählen Sie die Option Aktivieren.

   b. Wählen Sie für Metadatenversion die Option Nur V2 (Token erforderlich) aus.

   c. Geben Sie für Metadaten-Antwort-Hop-Limit den Wert 2 an, wenn Ihre Instances Container hosten sollen. Wählen Sie andernfalls Keine Präferenz aus. Wenn keine Präferenz angegeben wird, ist der Wert beim Start standardmäßig 2, wenn das AMI die Einstellung `ImdsSupport: v2.0` hat; andernfalls ist er standardmäßig 1.

   d. Wählen Sie Aktualisieren aus.

AWS CLI

Um es IMDSv2 als Standard für das Konto für die angegebene Region festzulegen

Verwenden Sie den modify-instance-metadata-defaultsBefehl und geben Sie die Region an, in der die Einstellungen auf IMDS-Kontoebene geändert werden sollen. Schließen Sie die Einstellung `--http-tokens` auf `required` ein und legen Sie `--http-put-response-hop-limit` auf 2 fest, wenn Ihre Instances Container hosten werden. Geben Sie andernfalls `-1` an, dass keine Präferenz angegeben werden soll. Wenn `-1` (keine Präferenz) angegeben wird, ist der Wert beim Start standardmäßig 2, wenn das AMI die Einstellung `ImdsSupport: v2.0` hat; andernfalls ist er standardmäßig 1.

```
aws ec2 modify-instance-metadata-defaults \
    --region us-east-1 \
    --http-tokens required \
    --http-put-response-hop-limit 2
```

Es folgt eine Beispielausgabe.

```
{
    "Return": true
}
```

So zeigen Sie die Standard-Kontoeinstellungen für die Instance-Metadatenoptionen für die angegebene Region an

Verwenden Sie den get-instance-metadata-defaultsBefehl und geben Sie die Region an.

```
aws ec2 get-instance-metadata-defaults --region us-east-1
```

Es folgt eine Beispielausgabe.

```
{
    "AccountLevel": {
        "HttpTokens": "required",
        "HttpPutResponseHopLimit": 2
    },
    "ManagedBy": "account"
}
```

Das `ManagedBy`-Feld gibt die Entität an, die die Einstellung konfiguriert hat. `account` zeigt in diesem Beispiel an, dass die Einstellung direkt im Konto konfiguriert wurde. Ein Wert von `declarative-policy` würde bedeuten, dass die Einstellung durch eine deklarative Richtlinie konfiguriert wurde. Weitere Informationen finden Sie unter Deklarative Richtlinien im AWS Organizations -Benutzerhandbuch.

Um es IMDSv2 als Standard für das Konto für alle Regionen festzulegen

Verwenden Sie den modify-instance-metadata-defaultsBefehl, um die Einstellungen auf IMDS-Kontoebene für alle Regionen zu ändern. Schließen Sie die Einstellung `--http-tokens` auf `required` ein und legen Sie `--http-put-response-hop-limit` auf 2 fest, wenn Ihre Instances Container hosten werden. Geben Sie andernfalls `-1` an, dass keine Präferenz angegeben werden soll. Wenn `-1` (keine Präferenz) angegeben wird, ist der Wert beim Start standardmäßig 2, wenn das AMI die Einstellung `ImdsSupport: v2.0` hat; andernfalls ist er standardmäßig 1.

```
echo -e "Region          \t Modified" ; \
echo -e "--------------  \t ---------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 modify-instance-metadata-defaults \
            --region $region \
            --http-tokens required \
```

```
            --http-put-response-hop-limit 2 \
            --output text)
        echo -e "$region        \t $output"
    );
done
```

Es folgt eine Beispielausgabe.

```
Region                  Modified
--------------          ---------
ap-south-1              True
eu-north-1              True
eu-west-3               True
...
```

So zeigen Sie die Standard-Kontoeinstellungen für die Instance-Metadatenoptionen für alle Regionen an

Verwenden Sie den Befehl get-instance-metadata-defaults.

```
echo -e "Region   \t Level          Hops    HttpTokens" ; \
echo -e "-------------- \t ------------   ----    ----------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 get-instance-metadata-defaults \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Es folgt eine Beispielausgabe.

```
Region          Level          Hops    HttpTokens
--------------  ------------   ----    ----------
ap-south-1      ACCOUNTLEVEL   2       required
eu-north-1      ACCOUNTLEVEL   2       required
```

```
eu-west-3        ACCOUNTLEVEL    2       required
...
```

PowerShell

Um es IMDSv2 als Standard für das Konto für die angegebene Region festzulegen

Verwenden Sie den Edit-EC2InstanceMetadataDefaultBefehl und geben Sie die Region an, in der die Einstellungen auf IMDS-Kontoebene geändert werden sollen. Schließen Sie die Einstellung `-HttpToken` auf `required` ein und legen Sie `-HttpPutResponseHopLimit` auf 2 fest, wenn Ihre Instances Container hosten werden. Geben Sie andernfalls `-1` an, dass keine Präferenz angegeben werden soll. Wenn `-1` (keine Präferenz) angegeben wird, ist der Wert beim Start standardmäßig 2, wenn das AMI die Einstellung `ImdsSupport: v2.0` hat; andernfalls ist er standardmäßig 1.

```
Edit-EC2InstanceMetadataDefault `
    -Region us-east-1 `
    -HttpToken required `
    -HttpPutResponseHopLimit 2
```

Es folgt eine Beispielausgabe.

```
True
```

So zeigen Sie die Standard-Kontoeinstellungen für die Instance-Metadatenoptionen für die angegebene Region an

Verwenden Sie den Get-EC2InstanceMetadataDefaultBefehl und geben Sie die Region an.

```
Get-EC2InstanceMetadataDefault -Region us-east-1 | Format-List
```

Es folgt eine Beispielausgabe.

```
HttpEndpoint            :
HttpPutResponseHopLimit : 2
HttpTokens              : required
InstanceMetadataTags    :
```

Um es IMDSv2 als Standard für das Konto für alle Regionen festzulegen

Verwenden Sie das Edit-EC2InstanceMetadataDefaultCmdlet, um die Einstellungen auf IMDS-Kontoebene für alle Regionen zu ändern. Schließen Sie die Einstellung `-HttpToken` auf `required` ein und legen Sie `-HttpPutResponseHopLimit` auf 2 fest, wenn Ihre Instances Container hosten werden. Geben Sie andernfalls `-1` an, dass keine Präferenz angegeben werden soll. Wenn `-1` (keine Präferenz) angegeben wird, ist der Wert beim Start standardmäßig 2, wenn das AMI die Einstellung `ImdsSupport: v2.0` hat; andernfalls ist er standardmäßig 1.

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region   = $_
        Modified = (Edit-EC2InstanceMetadataDefault `
                -Region $_ `
                -HttpToken required `
                -HttpPutResponseHopLimit 2)
    }
} | `
Format-Table Region, Modified -AutoSize
```

Erwartete Ausgabe

```
Region         Modified
------         --------
ap-south-1         True
eu-north-1         True
eu-west-3          True
...
```

So zeigen Sie die Standard-Kontoeinstellungen für die Instance-Metadatenoptionen für alle Regionen an

Verwenden Sie das Cmdlet. Get-EC2InstanceMetadataDefault

```
(Get-EC2Region).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region = $_
        HttpPutResponseHopLimit = (Get-EC2InstanceMetadataDefault -Region
 $_).HttpPutResponseHopLimit
        HttpTokens              = (Get-EC2InstanceMetadataDefault -Region
 $_).HttpTokens
```

```
    }
} | `
Format-Table -AutoSize
```

Beispielausgabe

```
Region         HttpPutResponseHopLimit HttpTokens
------         ----------------------- ----------
ap-south-1                           2 required
eu-north-1                           2 required
eu-west-3                            2 required
...
```

Konfigurieren der Instance beim Start

Wenn Sie eine Instance starten, können Sie die Instance so konfigurieren, dass die Verwendung von erforderlich ist, IMDSv2 indem Sie die folgenden Felder konfigurieren:

- EC2 Amazon-Konsole: Stellen Sie die Metadaten-Version nur auf V2 ein (Token erforderlich).
- AWS CLI: Stellen Sie `HttpTokens` auf `required` ein.

Wenn Sie angeben, dass dies erforderlich IMDSv2 ist, müssen Sie auch den IMDS-Endpunkt (Instance Metadata Service) aktivieren, indem Sie die Option Metadaten-Zugriff auf Aktiviert (Konsole) oder `HttpEndpoint` auf `enabled` (AWS CLI) setzen.

In einer Container-Umgebung empfehlen wir, IMDSv2 das Hop-Limit auf zu 2 setzen, sofern dies erforderlich ist. Weitere Informationen finden Sie unter Überlegungen zum Instance-Zugriff auf Instance-Metadaten.

Console

Um die Verwendung von IMDSv2 auf einer neuen Instance zu verlangen

- Wenn Sie eine neue Instance in der EC2 Amazon-Konsole starten, erweitern Sie Erweiterte Details und gehen Sie wie folgt vor:
  - Für Metadaten zugänglich wählen Sie Aktiviert.
  - Wählen Sie für Metadatenversion die Option Nur V2 (Token erforderlich) aus.
  - (Container-Umgebung) Wählen Sie für Metadata-Antwort-Hop-Limit den Wert 2 aus.

Weitere Informationen finden Sie unter Erweiterte Details.

AWS CLI

Um die Verwendung von IMDSv2 auf einer neuen Instance zu verlangen

Im folgenden Beispiel für run-instances wird eine `c6i.large`-Instance gestartet, bei der `--metadata-options` auf `HttpTokens=required` gesetzt ist. Wenn Sie einen Wert für `HttpTokens` angeben, müssen Sie auch `HttpEndpoint` auf `enabled` einstellen. Da der Secure Token-Header auf `required` für Anfragen zum Abrufen von Metadaten eingestellt ist, muss die Instanz IMDSv2 bei der Anforderung von Instanz-Metadaten verwendet werden.

In einer Containerumgebung empfehlen wir, IMDSv2 das Hop-Limit auf 2 with `HttpPutResponseHopLimit=2` zu setzen, sofern dies erforderlich ist.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
 ...
    --metadata-options
 "HttpEndpoint=enabled,HttpTokens=required,HttpPutResponseHopLimit=2"
```

PowerShell

Um die Verwendung von IMDSv2 auf einer neuen Instance zu verlangen

Das folgende New-EC2InstanceCmdlet-Beispiel startet eine `c6i.large` Instanz mit `MetadataOptions_HttpEndpoint` set to `enabled` und dem `MetadataOptions_HttpTokens` Parameter to. `required` Wenn Sie einen Wert für `HttpTokens` angeben, müssen Sie auch `HttpEndpoint` auf `enabled` einstellen. Da der Secure Token-Header auf `required` für Anfragen zum Abrufen von Metadaten festgelegt ist, muss die Instanz IMDSv2 bei der Anforderung von Instanz-Metadaten verwendet werden.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpTokens required
```

CloudFormation

Informationen zur Angabe der Metadatenoptionen für eine Instanz, die verwendet CloudFormation wird, finden Sie in der entsprechenden AWS::EC2::LaunchTemplate MetadataOptionsEigenschaft im AWS CloudFormation Benutzerhandbuch.

Konfigurieren des AMI

Wenn Sie ein neues AMI registrieren oder ein vorhandenes AMI ändern, können Sie den Parameter `imds-support` auf `v2.0` setzen. Bei Instances, die über dieses AMI gestartet werden, ist Metadatenversion auf Nur V2 (Token erforderlich) (Konsole) eingestellt, oder `HttpTokens` ist auf `required` eingestellt (AWS CLI). Bei diesen Einstellungen setzt die Instanz voraus, dass diese bei der Anforderung von Instanz-Metadaten verwendet IMDSv2 wird.

Hinweis: Wenn Sie `imds-support` auf `v2.0` einstellen, wird bei Instances, die über dieses AMI gestartet werden, auch Metadata response hop limit (Limit für Metadaten-Antwort-Hop) (Konsole) oder `http-put-response-hop-limit` (AWS CLI) auf 2 eingestellt.

Important

Verwenden Sie diesen Parameter nur, wenn Ihre AMI-Software ihn unterstütztIMDSv2. Nachdem Sie den Wert auf `v2.0` gesetzt haben, können Sie das nicht mehr rückgängig machen. Die einzige Möglichkeit, Ihr AMI „zurückzusetzen“, besteht darin, ein neues AMI aus dem zugrunde liegenden Snapshot zu erstellen.

Um ein neues AMI zu konfigurieren für IMDSv2

Verwenden Sie eine der folgenden Methoden, um ein neues AMI für zu konfigurierenIMDSv2.

AWS CLI

Das folgende register-image-Beispiel registriert ein AMI mit dem angegebenen Snapshot eines EBS-Stamm-Volumes als `/dev/xvda` des Geräts. Geben Sie `v2.0` den `imds-support` Parameter so an, dass Instances, die über dieses AMI gestartet werden, diesen benötigen, IMDSv2 wenn Instance-Metadaten angefordert werden.

```
aws ec2 register-image \
    --name my-image \
```

```
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/
xvda,Ebs={SnapshotId=snap-0123456789example} \
    --architecture x86_64 \
    --imds-support v2.0
```

PowerShell

Das folgende Register-EC2ImageCmdlet-Beispiel registriert ein AMI unter Verwendung des angegebenen Snapshots eines EBS-Root-Volumes als Gerät. `/dev/xvda` Geben Sie `v2.0` den `ImdsSupport` Parameter so an, dass Instances, die über dieses AMI gestartet werden, diesen benötigen, IMDSv2 wenn Instance-Metadaten angefordert werden.

```
Register-EC2Image `
    -Name 'my-image' `
    -RootDeviceName /dev/xvda `
    -BlockDeviceMapping  (
    New-Object `
        -TypeName Amazon.EC2.Model.BlockDeviceMapping `
        -Property @{
        DeviceName = '/dev/xvda';
        EBS        = (New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property
 @{
                SnapshotId = 'snap-0123456789example'
                VolumeType = 'gp3'
                } )
        }  ) `
    -Architecture X86_64 `
    -ImdsSupport v2.0
```

So konfigurieren Sie ein vorhandenes AMI für IMDSv2

Verwenden Sie eine der folgenden Methoden, um ein vorhandenes AMI für zu konfigurierenIMDSv2.

AWS CLI

Im folgenden modify-image-attributeBeispiel wird ein vorhandenes AMI IMDSv2 nur für geändert. Geben Sie `v2.0` den `imds-support` Parameter so an, dass Instances, die über dieses AMI gestartet werden, diesen benötigen, IMDSv2 wenn Instance-Metadaten angefordert werden.

```
aws ec2 modify-image-attribute \
```

```
    --image-id ami-0abcdef1234567890 \
    --imds-support v2.0
```

PowerShell

Das folgende Edit-EC2ImageAttributeCmdlet-Beispiel ändert ein vorhandenes AMI nur für. IMDSv2 Geben Sie `v2.0` den `imds-support` Parameter so an, dass Instances, die über dieses AMI gestartet werden, diesen benötigen, IMDSv2 wenn Instance-Metadaten angefordert werden.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -ImdsSupport 'v2.0'
```

Verwenden einer IAM-Richtlinie

Sie können eine IAM-Richtlinie erstellen, die verhindert, dass Benutzer neue Instances starten, es sei denn, sie benötigen IMDSv2 die neue Instance.

Um die Verwendung von IMDSv2 auf allen neuen Instances mithilfe einer IAM-Richtlinie durchzusetzen

Um sicherzustellen, dass Benutzer nur Instances starten können, die IMDSv2 bei der Anforderung von Instance-Metadaten verwendet werden müssen, können Sie angeben, dass die erforderliche Bedingung erfüllt sein IMDSv2 muss, bevor eine Instance gestartet werden kann. Die IAM-Beispielrichtlinie finden Sie unter Arbeiten mit Instance-Metadaten.

Aktivieren Sie das IMDS IPv4 und die Endpoints IPv6

Das IMDS hat zwei Endpunkte auf einer Instanz: IPv4 (`169.254.169.254`) und (). IPv6 `[fd00:ec2::254]` Wenn Sie das IMDS aktivieren, wird der IPv4 Endpunkt automatisch aktiviert. Der IPv6 Endpunkt bleibt auch dann deaktiviert, wenn Sie eine Instance in einem Subnetz starten, das IPv6 nur für das Subnetz zuständig ist. Um den IPv6 Endpunkt zu aktivieren, müssen Sie dies explizit tun. Wenn Sie den IPv6 Endpunkt aktivieren, bleibt der IPv4 Endpunkt aktiviert.

Sie können den IPv6 Endpunkt beim Start der Instance oder danach aktivieren.

Anforderungen für die Aktivierung des IPv6 Endpunkts

- Der ausgewählte Instance-Typ ist eine Nitro-basierte Instance.

- Das ausgewählte Subnetz unterstützt IPv6, wobei es sich bei dem Subnetz entweder um ein Dual-Stack-Netzwerk oder IPv6 um ein reines Subnetz handelt.

Verwenden Sie eine der folgenden Methoden, um eine Instance mit aktiviertem IPv6 IMDS-Endpunkt zu starten.

Console

Um den IPv6 IMDS-Endpunkt beim Start der Instance zu aktivieren

- Starten Sie die Instance in der EC2 Amazon-Konsole mit den folgenden Angaben unter Erweiterte Details:
  - Wählen Sie für IPv6 Metadaten-Endpunkt die Option Aktiviert aus.

Weitere Informationen finden Sie unter Erweiterte Details.

AWS CLI

Um den IPv6 IMDS-Endpunkt beim Start der Instanz zu aktivieren

Im folgenden Run-Instance-Beispiel wird eine `c6i.large` Instance gestartet, bei der der IPv6 Endpunkt für das IMDS aktiviert ist. Um den IPv6 Endpunkt zu aktivieren, geben Sie für den `--metadata-options` Parameter Folgendes an. `HttpProtocolIpv6=enabled` Wenn Sie einen Wert für `HttpProtocolIpv6` angeben, müssen Sie auch `HttpEndpoint` auf `enabled` einstellen.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=enabled,HttpProtocolIpv6=enabled"
```

PowerShell

Um den IPv6 IMDS-Endpunkt beim Start der Instanz zu aktivieren

Im folgenden New-EC2InstanceCmdlet-Beispiel wird eine `c6i.large` Instanz gestartet, bei der der IPv6 Endpunkt für das IMDS aktiviert ist. Um den IPv6 Endpunkt zu aktivieren, geben Sie as an. `MetadataOptions_HttpProtocolIpv6 enabled` Wenn Sie

einen Wert für `MetadataOptions_HttpProtocolIpv6` angeben, müssen Sie auch `MetadataOptions_HttpEndpoint` auf `enabled` einstellen.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpProtocolIpv6 enabled
```

Deaktivieren des Zugriffs auf Instance-Metadaten

Sie können den Zugriff auf die Instance-Metadaten deaktivieren, indem Sie den IMDS deaktivieren, wenn Sie eine Instance starten. Sie können den Zugriff später wieder aktivieren, indem Sie den IMDS erneut aktivieren. Weitere Informationen finden Sie unter Aktivieren des Zugriffs auf Instance-Metadaten.

Important

Sie können wählen, ob Sie den IMDS beim Start oder nach dem Start deaktivieren möchten. Wenn Sie den IMDS beim Start deaktivieren, funktioniert Folgendes möglicherweise nicht:

- Möglicherweise haben Sie keinen SSH-Zugriff auf Ihre Instance. Auf den`public-keys/0/openssh-key`, den öffentlichen SSH-Schlüssel Ihrer Instance, kann nicht zugegriffen werden, da der Schlüssel normalerweise über EC2 Instanz-Metadaten bereitgestellt und abgerufen wird.
- EC2 Benutzerdaten sind nicht verfügbar und werden beim Start der Instanz nicht ausgeführt. EC2 Benutzerdaten werden auf dem IMDS gehostet. Wenn Sie den IMDS deaktivieren, deaktivieren Sie effektiv den Zugriff auf Benutzerdaten.

Sie können den IMDS nach dem Start wieder aktivieren, um auf diese Funktion zuzugreifen.

Console

So deaktivieren Sie den Zugriff auf Instance-Metadaten beim Start

- Starten Sie die Instance in der EC2 Amazon-Konsole mit den folgenden Angaben unter Erweiterte Details:

- Für Metadaten zugänglich wählen Sie Deaktiviert.

Weitere Informationen finden Sie unter Erweiterte Details.

AWS CLI

So deaktivieren Sie den Zugriff auf Instance-Metadaten beim Start

Starten Sie die Instance, wobei `--metadata-options` auf `HttpEndpoint=disabled` eingestellt ist.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=disabled"
```

PowerShell

So deaktivieren Sie den Zugriff auf Instance-Metadaten beim Start

Das folgende New-EC2InstanceCmdlet-Beispiel startet eine Instance mit der `MetadataOptions_HttpEndpoint` Einstellung auf. `disabled`

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint disabled
```

CloudFormation

Informationen zum Angeben der Metadatenoptionen für eine Instanz, die Sie verwenden CloudFormation, finden Sie in der AWS::EC2::LaunchTemplate MetadataOptionsentsprechenden Eigenschaft im CloudFormation Benutzerhandbuch.

Zulassen des Zugriffs auf Tags in Instance-Metadaten

Standardmäßig gibt es keinen Zugriff auf Instance-Tags in den Instance-Metadaten. Sie müssen den Zugriff für jede Instance explizit zulassen. Wenn der Zugriff erlaubt ist, müssen die Instance-Tag-Schlüssel bestimmten Zeichenbeschränkungen entsprechen, andernfalls schlägt der Instance-

Start fehl. Weitere Informationen finden Sie unter Zugriff auf Tags in Instance-Metadaten ermöglichen .

Modifizieren von Instance-Metadatenoptionen für vorhandene Instances

Sie können die Instance-Metadatenoptionen für vorhandene Instances ändern.

Sie können auch eine IAM-Richtlinie erstellen, die verhindert, dass Benutzer die Instance-Metadatenoptionen für vorhandene Instances ändern. Um zu kontrollieren, welche Benutzer die Optionen für Instance-Metadaten ändern können, geben Sie eine Richtlinie an, die verhindert, dass alle Benutzer außer Benutzern mit einer bestimmten Rolle die ModifyInstanceMetadataOptionsAPI verwenden. Die IAM-Beispielrichtlinie finden Sie unter Arbeiten mit Instance-Metadaten.

> **Note**
>
> Wenn zur Konfiguration der Instance-Metadatenoptionen eine deklarative Richtlinie verwendet wurde, können Sie diese nicht direkt im Konto ändern. Weitere Informationen finden Sie unter Deklarative Richtlinien im AWS Organizations -Benutzerhandbuch.

Erfordern die Verwendung von IMDSv2

Verwenden Sie eine der folgenden Methoden, um die Optionen für Instanzmetadaten auf einer vorhandenen Instanz so zu ändern, dass diese Option bei der Anforderung von Instanz-Metadaten erforderlich IMDSv2 ist. Wann IMDSv2 ist erforderlich, IMDSv1 kann nicht verwendet werden.

> **Note**
>
> Bevor Sie verlangen, dass dies verwendet IMDSv2 wird, stellen Sie sicher, dass die Instanz keine IMDSv1 Aufrufe tätigt. Die `MetadataNoToken` CloudWatch Metrik verfolgt IMDSv1 Anrufe. Wenn für eine Instance keine IMDSv1 Nutzung `MetadataNoToken` aufgezeichnet wird, ist die Instance bereit, sie zu nutzen IMDSv2.

Console

Um die Verwendung von IMDSv2 auf einer vorhandenen Instanz vorzuschreiben

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.

3. Wählen Sie Ihre Instance aus.
4. Wählen Sie Aktionen, Instance-Einstellungen und Instance-Metadata-Optionen ändern.
5. Führen Sie im Dialogfeld Instance-Metadatenoptionen ändern Folgendes aus:
    a. Für den Instance-Metadatenservice wählen Sie die Option Aktivieren.
    b. Wählen Sie für IMDSv2die Option Erforderlich aus.
    c. Wählen Sie Speichern.

AWS CLI

Um die Verwendung von IMDSv2 auf einer vorhandenen Instanz zu verlangen

Verwenden Sie den modify-instance-metadata-optionsCLI-Befehl und setzen Sie den `http-tokens` Parameter auf`required`. Wenn Sie einen Wert für `http-tokens` angeben, müssen Sie auch `http-endpoint` auf `enabled` einstellen.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-tokens required \
    --http-endpoint enabled
```

PowerShell

Um die Verwendung von IMDSv2 auf einer vorhandenen Instanz zu verlangen

Verwenden Sie das Edit-EC2InstanceMetadataOptionCmdlet und setzen Sie den `HttpTokens` Parameter auf. `required` Wenn Sie einen Wert für `HttpTokens` angeben, müssen Sie auch `HttpEndpoint` auf `enabled` einstellen.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpTokens required `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Stellen Sie die Verwendung von wieder her IMDSv1

Wenn IMDSv2 erforderlich, IMDSv1 funktioniert nicht, wenn Instanz-Metadaten angefordert werden. Wann IMDSv2 ist optional, dann IMDSv1 funktionieren IMDSv2 sowohl als auch. Machen Sie

die Wiederherstellung daher IMDSv2 optional IMDSv1, indem Sie eine der folgenden Methoden verwenden.

Console

Um die Verwendung von IMDSv1 auf einer Instanz wiederherzustellen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie Ihre Instance aus.
4. Wählen Sie Aktionen, Instance-Einstellungen und Instance-Metadata-Optionen ändern.
5. Führen Sie im Dialogfeld Instance-Metadatenoptionen ändern Folgendes aus:
   a. Vergewissern Sie sich, dass für den Instance-Metadatenservice die Option Aktivieren ausgewählt ist.
   b. Wählen Sie für IMDSv2„Optional“.
   c. Wählen Sie Speichern.

AWS CLI

Um die Verwendung von IMDSv1 auf einer Instanz wiederherzustellen

Sie können den modify-instance-metadata-optionsCLI-Befehl mit `http-tokens` set to verwenden, `optional` um die Verwendung von IMDSv1 bei der Anforderung von Instance-Metadaten wiederherzustellen.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-tokens optional \
    --http-endpoint enabled
```

PowerShell

Um die Verwendung von IMDSv1 auf einer Instanz wiederherzustellen

Sie können das Edit-EC2InstanceMetadataOptionCmdlet mit der `HttpTokens` Einstellung auf verwenden, `optional` um die Verwendung von IMDSv1 bei der Anforderung von Instanzmetadaten wiederherzustellen.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpTokens optional `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Ändern des PUT-Antwort-Hop-Limits

Für bestehende Instances können Sie die Einstellungen für das PUT-Antwort-Hop-Limit ändern.

Derzeit AWS SDKs unterstützen nur die AWS CLI und die Änderung des PUT-Antwort-Hop-Limits.

AWS CLI

So ändern Sie das PUT-Antwort-Hop-Limit

Verwenden Sie den modify-instance-metadata-optionsCLI-Befehl und setzen Sie den `http-put-response-hop-limit` Parameter auf die erforderliche Anzahl von Hops. Im folgenden Beispiel wird das Hop-Limit auf 3 gesetzt. Beachten Sie, dass Sie beim Angeben eines Werts für `http-put-response-hop-limit` auch `http-endpoint` auf `enabled` setzen müssen.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-put-response-hop-limit 3 \
    --http-endpoint enabled
```

PowerShell

So ändern Sie das PUT-Antwort-Hop-Limit

Verwenden Sie das Edit-EC2InstanceMetadataOptionCmdlet und setzen Sie den `HttpPutResponseHopLimit` Parameter auf die erforderliche Anzahl von Hops. Im folgenden Beispiel wird das Hop-Limit auf 3 gesetzt. Beachten Sie, dass Sie beim Angeben eines Werts für `HttpPutResponseHopLimit` auch `HttpEndpoint` auf `enabled` setzen müssen.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpPutResponseHopLimit 3 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Aktivieren Sie das IMDS und die Endpoints IPv4 IPv6

Das IMDS hat zwei Endpunkte auf einer Instanz: IPv4 (`169.254.169.254`) und (). IPv6 `[fd00:ec2::254]` Wenn Sie das IMDS aktivieren, wird der IPv4 Endpunkt automatisch aktiviert. Der IPv6 Endpunkt bleibt auch dann deaktiviert, wenn Sie eine Instance in einem Subnetz starten, das IPv6 nur für das Subnetz zuständig ist. Um den IPv6 Endpunkt zu aktivieren, müssen Sie dies explizit tun. Wenn Sie den IPv6 Endpunkt aktivieren, bleibt der IPv4 Endpunkt aktiviert.

Sie können den IPv6 Endpunkt beim Start der Instance oder danach aktivieren.

Anforderungen für die Aktivierung des IPv6 Endpunkts

- Der ausgewählte Instance-Typ ist eine Nitro-basierte Instance.
- Das ausgewählte Subnetz unterstützt IPv6, wobei es sich bei dem Subnetz entweder um ein Dual-Stack-Netzwerk oder IPv6 um ein reines Subnetz handelt.

Derzeit AWS SDKs unterstützen nur die AWS CLI und die Aktivierung des IPv6 IMDS-Endpunkts nach dem Start der Instance.

AWS CLI

Um den IPv6 IMDS-Endpunkt für Ihre Instance zu aktivieren

Verwenden Sie den modify-instance-metadata-optionsCLI-Befehl und setzen Sie den `http-protocol-ipv6` Parameter auf`enabled`. Beachten Sie, dass Sie beim Angeben eines Werts für `http-protocol-ipv6` auch `http-endpoint` auf `enabled` setzen müssen.

```
aws ec2 modify-instance-metadata-options \
 --instance-id i-1234567890abcdef0 \
 --http-protocol-ipv6 enabled \
 --http-endpoint enabled
```

PowerShell

Um den IPv6 IMDS-Endpunkt für Ihre Instance zu aktivieren

Verwenden Sie das Edit-EC2InstanceMetadataOptionCmdlet und setzen Sie den `HttpProtocolIpv6` Parameter auf. `enabled` Beachten Sie, dass Sie beim Angeben eines Werts für `HttpProtocolIpv6` auch `HttpEndpoint` auf `enabled` setzen müssen.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpProtocolIpv6 enabled `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Aktivieren des Zugriffs auf Instance-Metadaten

Sie können den Zugriff auf Instance-Metadaten aktivieren, indem Sie den HTTP-Endpunkt des IMDS auf Ihrer Instance aktivieren, unabhängig davon, welche Version des IMDS Sie verwenden. Sie können diese Änderung jederzeit rückgängig machen, indem Sie den HTTP-Endpunkt deaktivieren.

Verwenden Sie eine der folgenden Methoden, um den Zugriff auf Instance-Metadaten für eine Instance zu aktivieren.

Console

So aktivieren Sie den Zugriff auf Instance-Metadaten

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie Ihre Instance aus.
4. Wählen Sie Aktionen, Instance-Einstellungen und Instance-Metadata-Optionen ändern.
5. Führen Sie im Dialogfeld Instance-Metadatenoptionen ändern Folgendes aus:
   a. Für den Instance-Metadatenservice wählen Sie die Option Aktivieren.
   b. Wählen Sie Speichern.

AWS CLI

So aktivieren Sie den Zugriff auf Instance-Metadaten

Verwenden Sie den modify-instance-metadata-optionsCLI-Befehl und setzen Sie den `http-endpoint` Parameter auf`enabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-endpoint enabled
```

PowerShell

So aktivieren Sie den Zugriff auf Instance-Metadaten

Verwenden Sie das Edit-EC2InstanceMetadataOptionCmdlet und setzen Sie den `HttpEndpoint` Parameter auf. `enabled`

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Deaktivieren des Zugriffs auf Instance-Metadaten

Sie können den Zugriff auf Instance-Metadaten deaktivieren, indem Sie den HTTP-Endpunkt des IMDS auf Ihrer Instance deaktivieren, unabhängig davon, welche Version des IMDS Sie verwenden. Sie können diese Änderung jederzeit rückgängig machen, indem Sie den HTTP-Endpunkt aktivieren.

Verwenden Sie eine der folgenden Methoden, um den Zugriff auf Instance-Metadaten für eine Instance zu deaktivieren.

Console

So deaktivieren Sie den Zugriff auf Instance-Metadaten

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie Ihre Instance aus.
4. Wählen Sie Aktionen, Instance-Einstellungen und Instance-Metadata-Optionen ändern.
5. Führen Sie im Dialogfeld Instance-Metadatenoptionen ändern Folgendes aus:
   a. Für den Instance-Metadatenservice entfernen Sie die Option Aktivieren.
   b. Wählen Sie Speichern.

AWS CLI

So deaktivieren Sie den Zugriff auf Instance-Metadaten

Verwenden Sie den modify-instance-metadata-optionsCLI-Befehl und setzen Sie den `http-endpoint` Parameter auf`disabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --http-endpoint disabled
```

PowerShell

So deaktivieren Sie den Zugriff auf Instance-Metadaten

Verwenden Sie das Edit-EC2InstanceMetadataOptionCmdlet und setzen Sie den `HttpEndpoint` Parameter auf. `disabled`

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -HttpEndpoint disabled).InstanceMetadataOptions
```

Zulassen des Zugriffs auf Tags in Instance-Metadaten

Sie können den Zugriff auf Tags in den Instance-Metadaten einer laufenden oder angehaltenen Instance erlauben. Sie müssen den Zugriff für jede Instance explizit zulassen. Wenn der Zugriff erlaubt ist, müssen die Instance-Tag-Schlüssel bestimmten Zeichenbeschränkungen entsprechen, andernfalls schlägt der Instance-Start fehl. Weitere Informationen finden Sie unter Zugriff auf Tags in Instance-Metadaten ermöglichen .

Befehle ausführen, wenn Sie eine EC2 Instance mit Benutzerdateneingabe starten

Wenn Sie eine EC2 Amazon-Instance starten, können Sie Benutzerdaten an die Instance übergeben, die zur Ausführung automatisierter Konfigurationsaufgaben oder zur Ausführung von Skripten nach dem Start der Instance verwendet wird.

Wenn Sie an komplexeren Automatisierungsszenarien interessiert sind, sollten Sie dies in Betracht ziehen CloudFormation. Weitere Informationen finden Sie unter Bereitstellen von Anwendungen auf Amazon EC2 mit CloudFormation im AWS CloudFormation Benutzerhandbuch.

Auf Linux-Instances können Sie zwei Arten von Benutzerdaten an Amazon übergeben EC2: Shell-Skripte und Cloud-Init-Direktiven. Sie können diese Daten auch als Klartext an den Launch Instance Wizard weiterleiten, entweder als Datei (dies ist hilfreich für den Start von Instances mithilfe der Befehlszeilen-Tools) oder als base64-kodierten Text (für API-Aufrufe).

Auf Windows-Instances verarbeiten die Start-Agenten Ihre Benutzerdaten-Skripts.

Überlegungen

- Benutzerdaten werden als Opaque-Daten behandelt: Was Sie eingeben, wird auch ausgegeben. Die Interpretation der Daten ist Aufgabe der Instance.
- Benutzerdaten müssen mit Base64 codiert werden. Die EC2 Amazon-Konsole kann die Base64-Kodierung für Ihre Eingabe durchführen oder Base64-kodierte Eingaben akzeptieren. Wenn Sie die Benutzerdaten über Instance-Metadaten oder die Konsole abrufen, werden sie automatisch für Sie base64-dekodiert.
- Benutzerdaten sind auf 16 KB an Rohdaten, bevor diese base64-codiert werden, begrenzt. Die Länge einer Zeichenfolge n nach base64-Codierung ist ceil(n/3)*4.
- Benutzerdaten sind ein Instance-Attribut. Wenn Sie ein AMI auf der Grundlage einer Instance erstellen, sind die Instance-Benutzerdaten nicht im AMI enthalten.

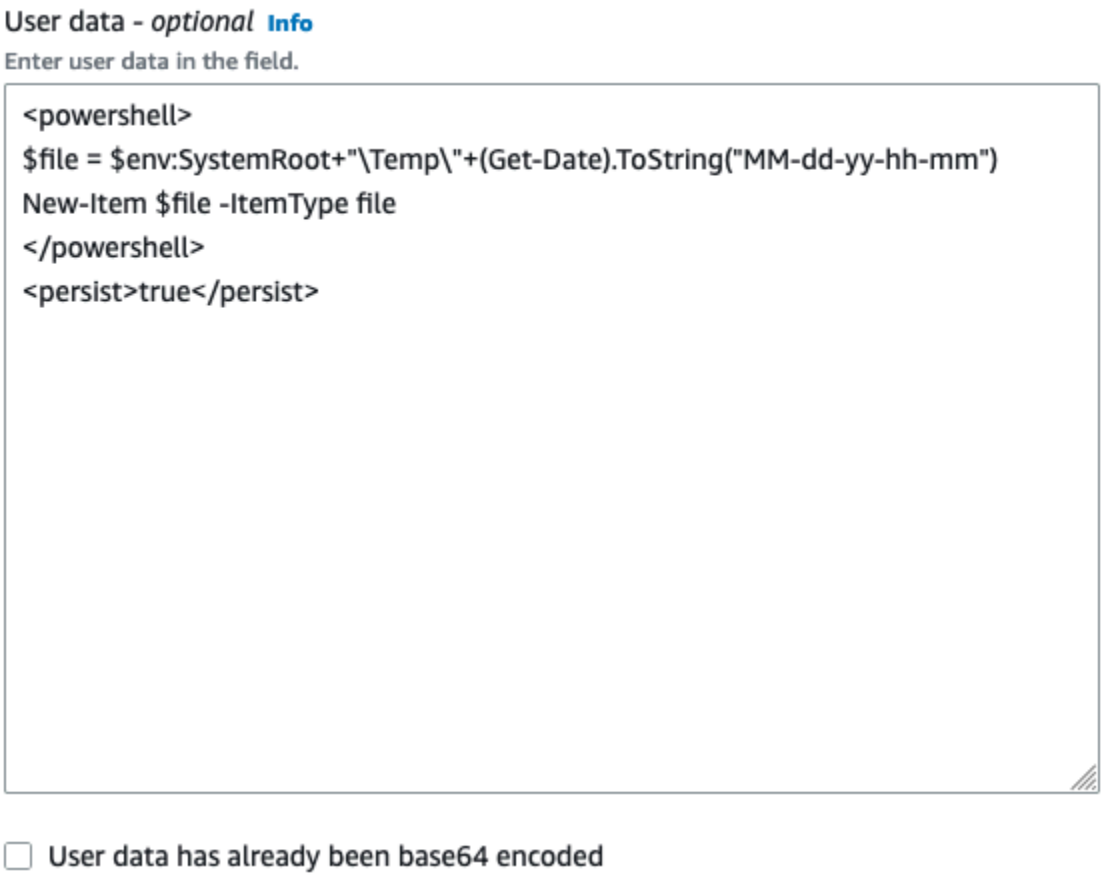
Benutzerdaten in der AWS-Managementkonsole

Sie können Instance-Benutzerdaten angeben, wenn Sie die Instance starten. Wenn das Root-Volume der Instance ein EBS-Volume ist, können Sie die Instance auch anhalten und ihre Benutzerdaten aktualisieren.

Instance-Benutzerdaten beim Start mit dem Launch Wizard angeben

Sie können Benutzerdaten angeben, wenn Sie eine Instance mit dem Launch Wizard in der EC2 Konsole starten. Um Benutzerdaten beim Start anzugeben, folgen Sie dem Verfahren zum Starten einer Instance. Das Feld User data (Benutzerdaten) befindet sich im Abschnitt Erweiterte Details des Launch Instance Wizard. Geben Sie Ihr PowerShell Skript in das Feld Benutzerdaten ein und schließen Sie dann den Vorgang zum Starten der Instance ab.

Im folgenden Screenshot des Feldes Benutzerdaten erstellt das Beispielskript eine Datei im temporären Windows-Ordner und verwendet das aktuelle Datum und die Uhrzeit im Dateinamen. Wenn Sie `<persist>true</persist>` einfügen, wird das Skript bei jedem Neustart oder Start der Instance ausgeführt. Wenn Sie das Kontrollkästchen Benutzerdaten wurden bereits base64-codiert leer lassen, führt die EC2 Amazon-Konsole die Base64-Kodierung für Sie durch.



Weitere Informationen finden Sie unter Instance-Benutzerdaten beim Start mit dem Launch Wizard angeben. Ein Linux-Beispiel, das das verwendet, finden Sie unter AWS CLI. the section called “Benutzerdaten und die AWS CLI” Ein Windows-Beispiel, das die Tools für Windows verwendet PowerShell, finden Sie unterthe section called “Benutzerdaten und die Tools für Windows PowerShell”.

Anzeigen und Aktualisieren der Instance-Benutzerdaten

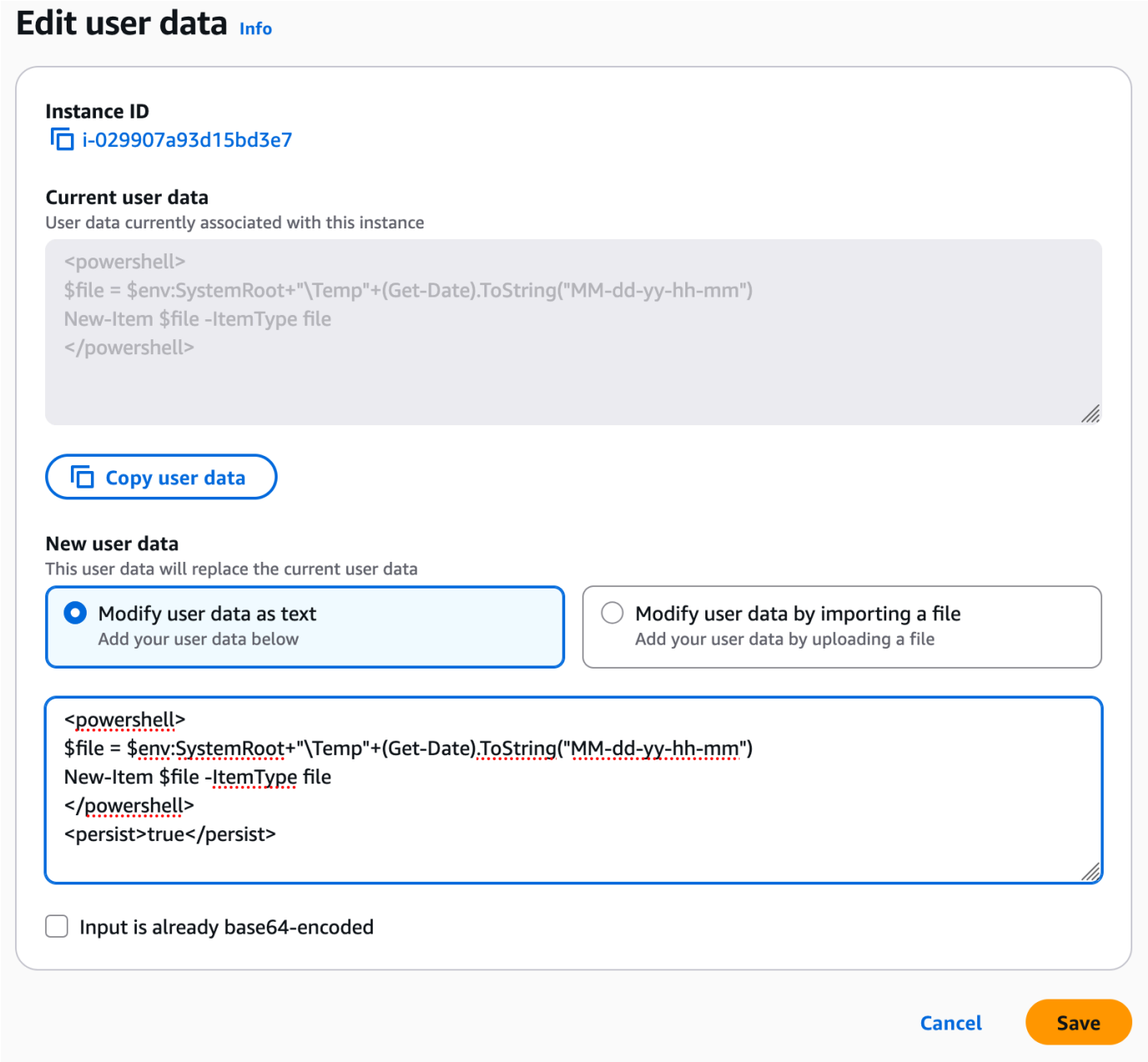
Sie können die Instance-Benutzerdaten für jede beliebige Instance anzeigen und die Instance-Benutzerdaten für eine angehaltene Instance aktualisieren.

So aktualisieren Sie die Benutzerdaten für eine Instance mit der Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance und dann Aktionen, Instance-Status, Instance anhalten aus.

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Stop aus. Das Anhalten der Instance kann einige Minuten dauern.
5. Wählen Sie mit der ausgewählten Instance Aktionen, Instance-Einstellungen, Benutzerdaten bearbeiten aus. Die Benutzerdaten können nicht geändert werden, solange die Instance ausgeführt wird; Sie können die Benutzerdaten nur anzeigen.
6. Aktualisieren Sie die Benutzerdaten im Dialogfeld View/Change User Data (Benutzerdaten anzeigen/ändern) und wählen Sie dann die Option Save (Speichern). Um die Benutzerdaten-Skripts bei jedem Neustart oder Starten der Instance auszuführen, fügen Sie `<persist>true</persist>` hinzu, wie im folgenden Beispiel gezeigt:



7. Starten Sie die Instance. Wenn Sie die Ausführung von Benutzerdaten für nachfolgende Neustarts oder Starts aktiviert haben, werden die aktualisierten Benutzerdaten-Skripts als Teil des Instance-Startprozesses ausgeführt.

Wie Amazon EC2 mit Benutzerdaten für Linux-Instances umgeht

In den folgenden Beispielen werden Benutzerdaten verwendet, um Befehle auszuführen, die beim Start der Instance einen LAMP-Server einrichten. In jedem Beispiel werden die folgenden Aufgaben ausgeführt:

- Die Softwarepakete der Bereitstellung werden aktualisiert.
- Der Webserver, php und `mariadb`-Pakete werden installiert.
- Der `httpd`-Service wird gestartet und aktiviert.
- Der Benutzer `ec2-user` wird der Apache-Gruppe hinzugefügt.
- Eigentümer und Dateiberechtigungen für das Webverzeichnis und die darin enthaltenen Daten werden festgelegt.
- Zum Testen des Webservers und der PHP-Engine wird eine einfache Webseite erstellt.

Inhalt

- Voraussetzungen
- Benutzerdaten und Shell-Skripts
- Instance-Benutzerdaten aktualisieren
- Benutzerdaten und Cloud-Init-Anweisungen
- Benutzerdaten und die AWS CLI
- Kombinieren von Shell-Skripts und cloud-init-Anweisungen

Voraussetzungen

Die Beispiele in diesem Thema setzen Folgendes voraus:

- Ihre Instance verfügt bereits über einen öffentlichen DNS-Namen, der über das Internet erreichbar ist.
- Die Ihrer Instance zugeordnete Sicherheitsgruppe ist so konfiguriert, dass sie SSH-Datenverkehr (Port 22) zulässt, sodass Sie eine Verbindung zur Instance herstellen können, um die Ausgabeprotokolldateien anzuzeigen.
- Ihre Instance wird mit einem Amazon-Linux-AMI gestartet. Die Befehle und Direktiven funktionieren unter Umständen nicht für andere Linux-Distributionen. Weitere Informationen zu anderen Distributionen, z. B. zur Unterstützung für cloud-init, finden Sie in der jeweiligen Dokumentation.

Benutzerdaten und Shell-Skripts

Shell-Skripts sind, sofern Sie sich damit auskennen, die einfachste und vollständigste Methode, mit der Sie einer Instance beim Start Anweisungen übermitteln. Wenn diese Skripts beim Start

ausgeführt werden, verlängert sich dadurch die Dauer des Instance-Starts. Erlauben Sie einige Minuten für die vollständige Ausführung der Aufgaben, bevor Sie überprüfen, ob die Benutzerskripte vollständig ausgeführt wurden.

> **Important**
>
> Standardmäßig werden Benutzerdatenskripte und Cloud-init-Direktiven nur während des Startzyklus ausgeführt, wenn Sie eine Instance zum ersten Mal starten. Sie können Ihre Konfiguration aktualisieren, um sicherzustellen, dass Ihre Benutzerdatenskripte und Cloud-Init-Direktiven bei jedem Neustart der Instance ausgeführt werden. Weitere Informationen finden Sie unter Wie kann ich Benutzerdaten verwenden, um bei jedem Neustart meiner Amazon EC2 Linux-Instance automatisch ein Skript auszuführen? im AWS Knowledge Center.

Benutzerdaten-Shell-Skripts müssen mit den Zeichen #! und dem Pfad zu dem Interpreter beginnen, der das Skript lesen soll (üblicherweise /bin/bash)). Eine Einführung in Shell-Scripting finden Sie im Bash-Referenzhandbuch auf der Website des GNU-Betriebssystems.

Als Benutzerdaten eingegebene Skripte werden als Stammbenutzer ausgeführt. Verwenden Sie daher nicht den sudo-Befehl im Skript. Denken Sie daran, dass alle von Ihnen erstellten Dateien dem Stammbenutzer gehören. Wenn Sie Zugriff auf die Dateien durch einen anderen Benutzer als den Stammbenutzer benötigen, sollten Sie die Berechtigungen im Skript entsprechend ändern. Außerdem können Sie keine Befehle verwenden, die Benutzerfeedback erfordern (z. B. yum update ohne das -y-Flag), da das Skript nicht interaktiv ausgeführt wird.

Wenn Sie eine AWS API, einschließlich der AWS CLI, in einem Benutzerdatenskript verwenden, müssen Sie beim Starten der Instance ein Instanzprofil verwenden. Ein Instanzprofil stellt die entsprechenden AWS Anmeldeinformationen bereit, die das Benutzerdatenskript benötigt, um den API-Aufruf auszuführen. Weitere Informationen finden Sie unter Verwenden von Instance-Profilen im IAM-Benutzerhandbuch. Die Berechtigungen, die Sie der IAM-Rolle zuweisen, hängen davon ab, welche Dienste Sie mit der API aufrufen. Weitere Informationen finden Sie unter IAM-Rollen für Amazon EC2.

Die Ausgabeprotokolldatei von Cloud-Init zeichnet die Ausgabe der Konsole auf, was die Behebung von Fehlern an den Skripts vereinfacht, falls sich die Instance nach dem Start nicht verhält wie erwartet. Um die Protokolldatei anzuzeigen, stellen Sie eine Verbindung mit der Instance her und öffnen Sie `/var/log/cloud-init-output.log`.

Wird ein Benutzerdatenskript verarbeitet, dann wird es nach kopiert und von dort aus ausgeführ `/var/lib/cloud/instances/instance-id/`. Das Skript wird nach der Ausführung nicht gelöscht. Stellen Sie sicher, dass Sie die Benutzerdatenskripts aus `/var/lib/cloud/instances/instance-id/` löschen, bevor Sie ein AMI aus der Instance erstellen. Andernfalls ist das Skript in diesem Verzeichnis auf jeder Instance vorhanden, die vom AMI gestartet wird.

Instance-Benutzerdaten aktualisieren

Um die Instance-Benutzerdaten aktualisieren zu können, müssen Sie zuerst die Instance anhalten. Wenn die Instance ausgeführt wird, können Sie die Benutzerdaten anzeigen, sie können jedoch nicht ändern.

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

Ändern von Instance-Benutzerdaten

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance und dann Instance-Status, Instance anhalten aus. Wenn diese Option deaktiviert ist, wurde die Instance entweder bereits angehalten oder das Root-Volume ist ein Instance-Speicher-Volume.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Stop aus. Das Anhalten der Instance kann einige Minuten dauern.
5. Wählen Sie mit der ausgewählten Instance Aktionen, Instance-Einstellungen, Benutzerdaten bearbeiten aus.
6. Ändern Sie die Benutzerdaten nach Bedarf und wählen Sie dann Speichern.
7. Starten Sie die Instance. Die neuen Benutzerdaten werden nach dem Start in Ihrer Instance angezeigt, Benutzerdatenskripts werden jedoch nicht ausgeführt.

Benutzerdaten und Cloud-Init-Anweisungen

Das Cloud-Init-Paket konfiguriert bestimmte Aspekte einer neuen Amazon Linux-Instance bei deren Start. Insbesondere wird die Datei `.ssh/authorized_keys` für den ec2-user konfiguriert, sodass Sie sich mit dem eigenen privaten Schlüssel anmelden können. Weitere Informationen zu den Konfigurationsaufgaben, die das cloud-init-Paket für Amazon-Linux-Instances ausführt, finden Sie in der folgenden Dokumentation:

- Amazon Linux 2023 – Maßgeschneiderte cloud-init
- Amazon Linux 2 – Cloud-init in Amazon Linux 2 verwenden

Die Cloud-Init-Anweisungen können wie ein Skript auch beim Start einer Instance an diese weitergeleitet werden, wenngleich sich die Syntax unterscheidet. Weitere Informationen zu Cloud-Init finden Sie unter. https://cloudinit.readthedocs.org/en/latest/index.html

> **Important**
>
> Standardmäßig werden Benutzerdatenskripte und Cloud-init-Direktiven nur während des Startzyklus ausgeführt, wenn Sie eine Instance zum ersten Mal starten. Sie können Ihre Konfiguration aktualisieren, um sicherzustellen, dass Ihre Benutzerdatenskripte und Cloud-Init-Direktiven bei jedem Neustart der Instance ausgeführt werden. Weitere Informationen finden Sie unter Wie kann ich Benutzerdaten verwenden, um bei jedem Neustart meiner Amazon EC2 Linux-Instance automatisch ein Skript auszuführen? im AWS Knowledge Center.

Wenn diese Skripts beim Start ausgeführt werden sollen, verlängert sich dadurch die Dauer des Instance-Starts. Erlauben Sie einige Minuten für die vollständige Ausführung der Aufgaben, bevor Sie überprüfen, ob die Benutzerdatenanweisungen vollständig durchgeführt wurden.

So leiten Sie cloud-init-Anweisungen an eine Amazon-Linux-Instance weiter

1. Folgen Sie dem Verfahren unter Starten einer Instance. Das Feld User data (Benutzerdaten) befindet sich im Abschnitt Erweiterte Details des Launch Instance Wizard. Geben Sie den Text Ihrer cloud-init-Anweisung im Feld User Data (Benutzerdaten) ein und führen Sie dann das Verfahren zum Starten der Instance aus.

Die folgenden Beispiele zeigen, wie Anweisungen einen Webserver in Amazon Linux erstellen und konfigurieren. Die Zeile `#cloud-config` ganz oben ist erforderlich, um die Befehle als cloud-init-Anweisungen zu identifizieren.

AL2023

```
#cloud-config
package_update: true
package_upgrade: all

packages:
- httpd
- mariadb105-server
- php8.1
- php8.1-mysqlnd

runcmd:
- systemctl start httpd
- systemctl enable httpd
- [ sh, -c, "usermod -a -G apache ec2-user" ]
- [ sh, -c, "chown -R ec2-user:apache /var/www" ]
- chmod 2775 /var/www
- [ find, /var/www, -type, d, -exec, chmod, 2775, {}, \; ]
- [ find, /var/www, -type, f, -exec, chmod, 0664, {}, \; ]
- [ sh, -c, 'echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php' ]
```

AL2

```
#cloud-config
package_update: true
package_upgrade: all

packages:
- httpd
- mariadb-server

runcmd:
- [ sh, -c, "amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2" ]
- systemctl start httpd
- systemctl enable httpd
- [ sh, -c, "usermod -a -G apache ec2-user" ]
- [ sh, -c, "chown -R ec2-user:apache /var/www" ]
```

```
- chmod 2775 /var/www
- [ find, /var/www, -type, d, -exec, chmod, 2775, {}, \; ]
- [ find, /var/www, -type, f, -exec, chmod, 0664, {}, \; ]
- [ sh, -c, 'echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php' ]
```

2. Geben Sie der Instance ausreichend Zeit zum Starten und zum Ausführen der Anweisungen in Ihren Benutzerdaten, dann überprüfen Sie, ob die Anweisungen die gewünschten Aufgaben ausgeführt haben.

   Geben Sie für dieses Beispiel in einem Webbrowser die URL der PHP-Testdatei ein, die die Anweisungen erstellt haben. Diese URL ist die öffentliche DNS-Adresse Ihrer Instance, gefolgt von einem Schrägstrich und dem Dateinamen.

   ```
   http://my.public.dns.amazonaws.com/phpinfo.php
   ```

   Die PHP-Informationsseite wird angezeigt. Wenn Sie die PHP-Informationsseite nicht anzeigen können, prüfen Sie, ob die verwendete Sicherheitsgruppe eine Regel enthält, um den HTTP-Datenverkehr (Port 80) zuzulassen. Weitere Informationen finden Sie unter Sicherheitsgruppenregeln konfigurieren.

3. (Optional) Wenn Ihre Anweisungen nicht die Aufgaben erfüllt haben, die Sie erwartet haben oder wenn Sie nur überprüfen möchten, ob Ihre Direktiven ohne Fehler abgeschlossen wurden, stellen Sie eine Verbindung mit der Instance her, untersuchen Sie die Ausgabeprotokolldatei (`/var/log/cloud-init-output.log`) und suchen Sie nach Fehlermeldungen in der Ausgabe. Weitere Informationen zur Fehlerbehebung erhalten Sie, indem Sie den Anweisungen die folgende Zeile hinzufügen:

   ```
   output : { all : '| tee -a /var/log/cloud-init-output.log' }
   ```

   Diese Anweisung übermittelt die Ausgabe von runcmd an `/var/log/cloud-init-output.log`.

Benutzerdaten und die AWS CLI

Sie können den verwenden, AWS CLI um die Benutzerdaten für Ihre Instanz anzugeben, zu ändern und anzuzeigen. Informationen zum Anzeigen von Benutzerdaten Ihrer Instance mithilfe von Instance-Metadaten erhalten Sie unter Auf Instanz-Metadaten für eine EC2 Instanz zugreifen.

Unter Windows können Sie den AWS Tools for Windows PowerShell anstelle von verwenden AWS CLI. Weitere Informationen finden Sie unter Benutzerdaten und die Tools für Windows PowerShell.

Beispiel: Angeben von Benutzerdaten beim Start

Verwenden Sie den Befehl run-instances mit dem Parameter `--user-data`, um Benutzerdaten beim Start Ihrer Instance anzugeben. Mit run-instances AWS CLI führt der die Base64-Kodierung der Benutzerdaten für Sie durch.

Im folgenden Beispiel wird gezeigt, wie Sie ein Skript als String auf der Befehlszeile angeben:

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
    --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234
 \
    --user-data echo user data
```

Im folgenden Beispiel wird gezeigt, wie Sie ein Skript mithilfe einer Textdatei angeben: Verwenden Sie beim Angeben der Datei das Präfix `file://`.

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
    --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234
 \
    --user-data file://my_script.txt
```

Das folgende Element ist eine Beispieltextdatei mit einem Shell-Skript.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Beispiel: Modifizieren der Benutzerdaten einer angehaltenen Instance

Sie können die Benutzerdaten einer gestoppten Instanz mit dem modify-instance-attributeBefehl ändern. Mit modify-instance-attribute AWS CLI führt der keine Base64-Kodierung der Benutzerdaten für Sie durch.

- Verwenden Sie auf einem Linux-Computer den Befehl „base64“, um die Benutzerdaten zu codieren.

```
base64 my_script.txt >my_script_base64.txt
```

- Verwenden Sie auf einem, Windows-Computer den Befehl „certutil“, um die Benutzerdaten zu codieren. Bevor Sie diese Datei mit dem verwenden können AWS CLI, müssen Sie die erste (BEGIN CERTIFICATE) und die letzte Zeile (END CERTIFICATE) entfernen.

```
certutil -encode my_script.txt my_script_base64.txt
notepad my_script_base64.txt
```

Verwenden Sie die Parameter `--attribute` und `--value`, um die codierte Textdatei zur Angabe der Benutzerdaten zu verwenden. Verwenden Sie beim Angeben der Datei das Präfix `file://`.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --value file://my_script_base64.txt
```

Beispiel: Löschen der Benutzerdaten einer angehaltenen Instance

Verwenden Sie den modify-instance-attributeBefehl wie folgt, um die vorhandenen Benutzerdaten zu löschen:

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --user-data Value=
```

Beispiel: Anzeigen von Benutzerdaten

Verwenden Sie den describe-instance-attributeBefehl, um die Benutzerdaten für eine Instanz abzurufen. Mit describe-instance-attribute AWS CLI führt der keine Base64-Decodierung der Benutzerdaten für Sie durch.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData
```

Im folgenden Beispiel wird die Ausgabe mit base64-Benutzerdaten verschlüsselt.

```
{
    "UserData": {
        "Value":
 "IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAteQpzZXJ2aWNlIGh0dHBkIHN0YXJ0CmNoa2NvbmZpZyBodHRwZCBvbg=="
    },
```

```
    "InstanceId": "i-1234567890abcdef0"
}
```

- Verwenden Sie auf einem Linux-Computer die Option `--query`, um die codierten Benutzerdaten abzurufen, und den Befehl „base64“, um sie zu decodieren.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --output text --query "UserData.Value" | base64 --decode
```

- Verwenden Sie auf einem Windows-Computer die Option `--query`, um die codierten Benutzerdaten abzurufen, und den Befehl „certutil“, um sie zu decodieren. Die codierte Ausgabe wird in einer, die decodierte Ausgabe in einer anderen Datei gespeichert.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --output text --query "UserData.Value" >my_output.txt
certutil -decode my_output.txt my_output_decoded.txt
type my_output_decoded.txt
```

Es folgt eine Beispielausgabe.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Kombinieren von Shell-Skripts und cloud-init-Anweisungen

Standardmäßig können Sie jeweils nur einen Inhaltstyp in Benutzerdaten einbeziehen. Allerdings können Sie die Inhaltstypen `text/cloud-config` und `text/x-shellscript` in einer mehrteiligen MIME-Datei verwenden, um sowohl ein Shell-Skript als auch cloud-init-Anweisungen in Ihren Benutzerdaten einzubeziehen.

Nachfolgend wird das mehrteilige MIME-Format veranschaulicht.

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
```

```
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
cloud-init directives

--//
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash
shell script commands
--//--
```

Die folgenden Benutzerdaten enthalten beispielsweise cloud-init-Anweisungen und ein Bash-Shell-Skript. Die cloud-init-Anweisungen erstellen eine Datei (`/test-cloudinit/cloud-init.txt`) und schreiben `Created by cloud-init` in diese Datei. Das Bash-Shell-Skript erstellt eine Datei (`/test-userscript/userscript.txt`) und schreibt `Created by bash shell script` in diese Datei.

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
runcmd:
- [ mkdir, /test-cloudinit ]
write_files:
- path: /test-cloudinit/cloud-init.txt
content: Created by cloud-init

--//
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"
```

```
#!/bin/bash
mkdir test-userscript
touch /test-userscript/userscript.txt
echo "Created by bash shell script" >> /test-userscript/userscript.txt
--//--
```

Wie Amazon EC2 mit Benutzerdaten für Windows-Instances umgeht

Auf Windows-Instances führt der Start-Agent die Aufgaben im Zusammenhang mit Benutzerdaten aus. Weitere Informationen finden Sie hier:

- EC2Launch v2
- EC2Launch
- EC2Config-Service

Beispiele für die Zusammenstellung einer `UserData` Eigenschaft in einer CloudFormation Vorlage finden Sie unter Base64 Encoded Property und Base64 Encoded UserData UserData Property with and. AccessKey SecretKey

Ein Beispiel für die Ausführung von Befehlen auf einer Instance innerhalb einer Amazon EC2 Auto Scaling Scaling-Gruppe, die mit Lifecycle-Hooks arbeitet, finden Sie unter Tutorial: Benutzerdaten konfigurieren, um den Ziellebenszyklusstatus über Instance-Metadaten abzurufen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Inhalt

- Benutzerdatenskripts
- Komprimierte Benutzerdaten
- Ausführung von Benutzerdaten
- Benutzerdaten und die Tools für Windows PowerShell

Benutzerdatenskripts

Damit `EC2Config` oder `EC2Launch` Skripte ausführen können, müssen Sie das Skript in ein spezielles Tag einschließen, wenn Sie es zu den Benutzerdaten hinzufügen. Welches Tag Sie verwenden, hängt davon ab, ob die Befehle in einem Befehlszeilenfenster (Batch-Befehle) oder unter Windows ausgeführt werdenPowerShell.

Wenn Sie sowohl ein Batch-Skript als auch ein PowerShell Windows-Skript angeben, wird das Batch-Skript zuerst und das PowerShell Windows-Skript als Nächstes ausgeführt, unabhängig von der Reihenfolge, in der sie in den Instanzbenutzerdaten erscheinen.

Wenn Sie eine AWS API, einschließlich der AWS CLI, in einem Benutzerdatenskript verwenden, müssen Sie beim Starten der Instanz ein Instanzprofil verwenden. Ein Instanzprofil stellt die entsprechenden AWS Anmeldeinformationen bereit, die das Benutzerdatenskript für den API-Aufruf benötigt. Weitere Informationen finden Sie unter Instance-Profile. Die Berechtigungen, die Sie der IAM-Rolle zuweisen, hängen davon ab, welche Dienste Sie mit der API aufrufen. Weitere Informationen finden Sie unter IAM-Rollen für Amazon EC2.

Skripttyp

- Syntax für Batch-Skripts
- Syntax für PowerShell Windows-Skripts
- Syntax für YAML-Konfigurationsskripts
- Base64-Codierung

Syntax für Batch-Skripts

Geben Sie ein Batch-Skript unter Verwendung des `script`-Tags (Markierung) an. Trennen Sie die Befehle durch Zeilenumbrüche, wie im folgenden Beispiel gezeigt.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
```

In der Standardeinstellung werden Benutzerdatenskripte einmal ausgeführt, wenn Sie die Instance starten. Um die Benutzerdaten-Skripts bei jedem Neustart oder Starten der Instance auszuführen, fügen Sie den Benutzerdaten `<persist>true</persist>` hinzu.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
<persist>true</persist>
```

EC2Starten Sie den v2-Agenten

Um ein XML-Benutzerdatenskript als eigenständigen Prozess mit der executeScript Aufgabe EC2 Launch v2 in der `UserData` Phase auszuführen, fügen Sie `<detach>true</detach>` weitere Benutzerdaten hinzu.

> **Note**
>
> Das detach-Tag wird auf früheren Start-Agenten nicht unterstützt.

```
<script>
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
<detach>true</detach>
```

Syntax für PowerShell Windows-Skripts

Die AWS Windows AMIs enthalten die AWS Tools for Windows PowerShell, sodass Sie diese Cmdlets in Benutzerdaten angeben können. Wenn Sie Ihrer Instance eine IAM-Rolle zuordnen, müssen Sie keine Anmeldeinformationen für die Cmdlets angeben, da Anwendungen, die auf der Instance ausgeführt werden, die Anmeldeinformationen der Rolle verwenden, um auf AWS Ressourcen (z. B. Amazon S3 S3-Buckets) zuzugreifen.

Geben Sie mithilfe des Tags ein PowerShell Windows-Skript an. `<powershell>` Trennen Sie die Befehle mithilfe von Zeilenumbrüchen voneinander. Beim `<powershell>`-Tag wird die Groß- und Kleinschreibung beachtet.

Zum Beispiel:

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
```

Standardmäßig werden Benutzerdaten-Skripts einmal ausgeführt, wenn Sie die Instance starten. Um die Benutzerdaten-Skripts bei jedem Neustart oder Starten der Instance auszuführen, fügen Sie den Benutzerdaten `<persist>true</persist>` hinzu.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
```

```
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Sie können ein oder mehrere PowerShell Argumente mit dem `<powershellArguments>` Tag angeben. Wenn keine Argumente übergeben werden, fügen EC2 EC2 Launch und Launch v2 standardmäßig das folgende Argument hinzu:`-ExecutionPolicy Unrestricted`.

Beispiel:

```
<powershell>
    $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

EC2Starten Sie den v2-Agenten

Um ein XML-Benutzerdatenskript als eigenständigen Prozess mit der executeScript Aufgabe EC2 Launch v2 in der `UserData` Phase auszuführen, fügen Sie `<detach>true</detach>` weitere Benutzerdaten hinzu.

> **Note**
>
> Das detach-Tag wird auf früheren Start-Agenten nicht unterstützt.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<detach>true</detach>
```

Syntax für YAML-Konfigurationsskripts

Wenn Sie EC2 Launch v2 zum Ausführen von Skripten verwenden, können Sie das YAML-Format verwenden. Konfigurationsaufgaben, Details und Beispiele für EC2 Launch v2 finden Sie unterAufgabenkonfiguration in EC2Launch v2.

Geben Sie ein YAML-Skript mit der Aufgabe `executeScript` an.

Beispiel für eine YAML-Syntax zum Ausführen eines Skripts PowerShell

```
version: 1.0
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: powershell
    runAs: localSystem
    content: |-
      $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
      New-Item $file -ItemType file
```

YAML-Beispielsyntax zum Ausführen eines Batch-Skripts

```
version: 1.1
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: batch
    runAs: localSystem
    content: |-
      echo Current date and time >> %SystemRoot%\Temp\test.log
      echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
```

Base64-Codierung

Wenn Sie die EC2 Amazon-API oder ein Tool verwenden, das keine Base64-Kodierung der Benutzerdaten durchführt, müssen Sie die Benutzerdaten selbst codieren. Andernfalls wird ein Fehler ausgegeben, der darauf hinweist, dass keine auszuführenden `script`- oder `powershell`-Tags gefunden wurden. Im Folgenden finden Sie ein Beispiel für die Verschlüsselung mit Windows. PowerShell

```
$UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Das Folgende ist ein Beispiel für die Dekodierung mit. PowerShell

```
$Script =
 [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData))
```

Weitere Informationen zur Base64-Kodierung finden Sie unter https://www.ietf. org/rfc/rfc4648.txt.

Komprimierte Benutzerdaten

EC2Launch v2 unterstützt komprimierte Benutzerdaten als Methode zum Senden von Benutzerdaten, die das IMDS-Limit von 16 KB überschreiten. Um diese Funktion zu verwenden, komprimieren Sie Ihr Benutzerdatenskript in ein `.zip` Archiv und übergeben es an Ihre EC2 Instanz. Wenn EC2 Launch v2 komprimierte Benutzerdaten erkennt, wird das komprimierte Benutzerdatenskript automatisch entpackt und ausgeführt.

Wie bei Standardbenutzerdaten müssen Sie, wenn Sie die EC2 Amazon-API oder ein Tool verwenden, das keine Base64-Kodierung der Benutzerdaten durchführt, die komprimierten Benutzerdaten selbst codieren. Weitere Informationen zur Größenbeschränkung für Benutzerdaten und base64-Codierung finden Sie unter Auf Instanz-Metadaten für eine EC2 Instanz zugreifen.

Ausführung von Benutzerdaten

Standardmäßig ist in allen AWS Windows-Versionen AMIs die Ausführung von Benutzerdaten für den ersten Start aktiviert. Sie können vorgeben, dass die Benutzerdaten-Skripts beim nächsten Neustart oder erneuten Starten der Instance ausgeführt werden sollen. Alternativ können Sie vorgeben, dass die Benutzerdaten-Skripts bei jedem Neustart oder erneuten Starten der Instance ausgeführt werden sollen.

> **Note**
>
> Benutzerdaten können nach dem ersten Start nicht standardmäßig ausgeführt werden. Informationen darüber, wie Sie Benutzerdaten beim Neustart oder beim Starten der Instance ausführen können, finden Sie unter Skripts bei nachfolgenden Neustarts oder Starts ausführen.

Benutzerdaten-Skripts werden vom lokalen Administratorkonto ausgeführt, wenn ein zufälliges Passwort generiert wird. Andernfalls werden Benutzerdaten-Skripts vom Systemkonto ausgeführt.

Skripte zum Starten von Instances

Skripts in den Instance-Benutzerdaten werden beim ersten Start der Instance ausgeführt. Ist der `persist`-Tag (Markierung) vorhanden, wir die Ausführung der Benutzerdaten für nachfolgende Neustarts oder Starts aktiviert. Die Protokolldateien für EC2 Launch v2, EC2 Launch und EC2 Config enthalten die Ausgabe der Standardausgabe- und Standardfehlerstreams.

EC2Starten Sie v2

Die Protokolldatei für EC2 Launch v2 ist`C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> Der Ordner `C:\ProgramData` ist möglicherweise ausgeblendet. Zum Anzeigen des Ordners müssen Sie die ausgeblendeten Dateien und Ordner einblenden.

Bei der Ausführung von Benutzerdaten werden die folgenden Informationen protokolliert:

- `Info: Converting user-data to yaml format`: Wenn die Benutzerdaten im XML-Format bereitgestellt wurden
- `Info: Initialize user-data state`: Der Beginn der Benutzerdatenausführung
- `Info: Frequency is: always`: Wenn die Benutzerdatenaufgabe bei jedem Start ausgeführt wird
- `Info: Frequency is: once`: Wenn die Benutzerdatenaufgabe nur einmal ausgeführt wird
- `Stage: postReadyUserData execution completed`: Das Ende der Ausführung von Benutzerdaten

EC2Starten

Die Protokolldatei für EC2 Launch ist`C:\ProgramData\Amazon\EC2-Windows\Launch\Log\UserdataExecution.log`.

Der Ordner `C:\ProgramData` ist möglicherweise ausgeblendet. Zum Anzeigen des Ordners müssen Sie die ausgeblendeten Dateien und Ordner einblenden.

Bei der Ausführung von Benutzerdaten werden die folgenden Informationen protokolliert:

- `Userdata execution begins`: Der Beginn der Benutzerdatenausführung
- `<persist> tag was provided: true`: Wenn das persist-Tag (Markierung) gefunden wird
- `Running userdata on every boot`: Wenn der persist-Tag (Markierung) gefunden wird
- `<powershell> tag was provided.. running powershell content`: Wenn der powershell-Tag (Markierung) gefunden wird
- `<script> tag was provided.. running script content`: Wenn der Skript-Tag (Markierung) gefunden wird

- `Message: The output from user scripts`: Wenn Benutzerdatenskripte ausgeführt werden, wird deren Ausgabe protokolliert

EC2Config

Die Protokolldatei für EC2 Config ist`C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2Config.log`. Bei der Ausführung von Benutzerdaten werden die folgenden Informationen protokolliert:

- `Ec2HandleUserData: Message: Start running user scripts`: Der Beginn der Benutzerdatenausführung
- `Ec2HandleUserData: Message: Re-enabled userdata execution`: Wenn der persist-Tag (Markierung) gefunden wird
- `Ec2HandleUserData: Message: Could not find <persist> and </persist>`: Wenn der persist-Tag (Markierung) nicht gefunden wird
- `Ec2HandleUserData: Message: The output from user scripts`: Wenn Benutzerdatenskripte ausgeführt werden, wird deren Ausgabe protokolliert

Skripts bei nachfolgenden Neustarts oder Starts ausführen

Wenn Sie Instance-Benutzerdaten aktualisieren, wird der aktualisierte Benutzerdateninhalt automatisch in den Instance-Metadaten wiedergegeben, wenn Sie die Instance das nächste Mal starten oder neu starten. Je nach installiertem Launch-Agent kann jedoch eine zusätzliche Konfiguration erforderlich sein, um Benutzerdatenskripts so zu konfigurieren, dass sie bei nachfolgenden Starts oder Neustarts ausgeführt werden.

Wenn Sie die Option Herunterfahren mit Sysprep wählen, werden Benutzerdatenskripts beim Start oder Neustart der Instance ausgeführt, auch wenn Sie die Ausführung der Benutzerdaten für nachfolgende Starts oder Neustarts nicht aktiviert haben.

Für Anweisungen zur Aktivierung der Benutzerdatenausführung wählen Sie die Registerkarte aus, die Ihrem Start-Agenten entspricht.

EC2Launch v2

> Im Gegensatz zu EC2 EC2 Launch v1 wertet Launch v2 die Benutzerdatenaufgabe bei jedem Start aus. Es ist nicht erforderlich, die Benutzerdatenaufgabe manuell zu planen. Die

Benutzerdaten werden auf der Grundlage der angegebenen Frequenz- oder Persistenzoptionen ausgeführt.

Für XML-Benutzerdatenskripts

Um Benutzerdatenskripts bei jedem Start auszuführen, fügen Sie den Benutzerdaten das `<persist>true</persist>`-Flag hinzu. Wenn das Persist-Flag nicht enthalten ist, wird das Benutzerdatenskript nur beim ersten Start ausgeführt.

Für YAML-Benutzerdaten

- Wenn eine Aufgabe beim ersten Start für Benutzerdaten ausgeführt werden soll, setzen Sie die Aufgaben-`frequency` auf `once`.
- Wenn eine Aufgabe bei jedem Start für Benutzerdaten ausgeführt werden soll, setzen Sie die Aufgaben-`frequency` auf `always`.

EC2Launch

1. Herstellen einer Verbindung mit Ihrer Windows-Instance.
2. Öffnen Sie ein PowerShell Befehlsfenster und führen Sie einen der folgenden Befehle aus:

   Einmal ausführen

   Um Benutzerdaten beim nächsten Start einmal auszuführen, verwenden Sie das `-Schedule`-Flag.

   ```
   C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
   Schedule
   ```

   Bei allen nachfolgenden Systemstarts ausführen

   Um Benutzerdaten bei allen nachfolgenden Starts auszuführen, verwenden Sie das `-SchedulePerBoot`-Flag.

   ```
   C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
   SchedulePerBoot
   ```
3. Trennen Sie die Verbindung zu Ihrer Windows-Instance. Um beim nächsten Starten der Instance aktualisierte Skripts auszuführen, halten Sie die Instance an und aktualisieren die Benutzerdaten.

EC2Config

1. Herstellen einer Verbindung mit Ihrer Windows-Instance.
2. Öffnen `C:\Program Files\Amazon\Ec2ConfigService\Ec2ConfigServiceSetting.exe`.
3. Wählen Sie unter Benutzerdaten die Option UserDataAusführung für den nächsten Dienststart aktivieren aus.
4. Trennen Sie die Verbindung zu Ihrer Windows-Instance. Um beim nächsten Starten der Instance aktualisierte Skripts auszuführen, halten Sie die Instance an und aktualisieren die Benutzerdaten.

Benutzerdaten und die Tools für Windows PowerShell

Sie können die Tools für Windows verwenden, PowerShell um die Benutzerdaten für Ihre Instanz anzugeben, zu ändern und anzuzeigen. Informationen zum Anzeigen von Benutzerdaten Ihrer Instance mithilfe von Instance-Metadaten erhalten Sie unter Auf Instanz-Metadaten für eine EC2 Instanz zugreifen. Hinweise zu Benutzerdaten und dem AWS CLI finden Sie unterBenutzerdaten und die AWS CLI.

Beispiel: Angeben von Instance-Benutzerdaten beim Start

Erstellen Sie eine Textdatei mit Instance-Benutzerdaten. Um die Benutzerdaten-Skripts bei jedem Neustart oder Starten der Instance auszuführen, fügen Sie `<persist>true</persist>` hinzu, wie im folgenden Beispiel gezeigt.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Verwenden Sie den New-EC2InstanceBefehl, um die Benutzerdaten für die Instanz anzugeben, wenn Sie Ihre Instance starten. Dieser Befehl führt keine Base64-Codierung der Benutzerdaten für Sie durch Verwenden Sie die folgenden Befehle, um die Benutzerdaten in einer Textdatei namens `script.txt` zu codieren.

```
PS C:\> $Script = Get-Content -Raw script.txt
```

```
PS C:\> $UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Verwenden Sie den Parameter `-UserData`, um die Benutzerdaten an den Befehl New-EC2Instance zu übergeben.

```
PS C:\> New-EC2Instance -ImageId ami-abcd1234 -MinCount 1 -MaxCount 1 -
InstanceType m3.medium \
    -KeyName my-key-pair -SubnetId subnet-12345678 -SecurityGroupIds sg-1a2b3c4d \
    -UserData $UserData
```

Beispiel: Aktualisieren von Instance-Benutzerdaten einer angehaltenen Instance

Sie können die Benutzerdaten einer gestoppten Instance mithilfe des Edit-EC2InstanceAttributeBefehls ändern.

Erstellen Sie eine Textdatei mit dem neuen Skript. Verwenden Sie die folgenden Befehle, um die Benutzerdaten in der Textdatei namens `new-script.txt` zu codieren.

```
PS C:\> $NewScript = Get-Content -Raw new-script.txt
PS C:\> $NewUserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($NewScript))
```

Verwenden Sie die Parameter `-UserData` und `-Value`, um die Benutzerdaten anzugeben.

```
PS C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute userData -
Value $NewUserData
```

Beispiel: Anzeige von Instance-Benutzerdaten

Verwenden Sie den Get-EC2InstanceAttributeBefehl, um die Benutzerdaten für eine Instanz abzurufen.

```
PS C:\> (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute
 userData).UserData
```

Es folgt eine Beispielausgabe. Beachten Sie, dass die Benutzerdaten codiert sind.

```
PHBvd2Vyc2hlbGw
+DQpSZW5hbWUtQ29tcHV0ZXIgLU5ld05hbWUgdXNlci1kYXRhLXRlc3QNCjwvcG93ZXJzaGVsbD4=
```

Verwenden Sie die folgenden Befehle, um die codierten Benutzerdaten in einer Variablen zu speichern und anschließend zu decodieren.

```
PS C:\> $UserData_encoded = (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -
Attribute userData).UserData
PS C:
\> [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData_encoded)
```

Es folgt eine Beispielausgabe.

```
<powershell>
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Beispiel: Umbenennen der Instance entsprechend des Tag (Markierung)-Werts

Sie können den Get-EC2TagBefehl verwenden, um den Tag-Wert zu lesen, die Instance beim ersten Start so umzubenennen, dass sie dem Tag-Wert entspricht, und den Computer neu zu starten. Um diesen Befehl erfolgreich auszuführen, müssen Sie über eine Rolle mit `ec2:DescribeTags`-Berechtigungen verfügen, die der Instance zugeordnet sind, da Tag-Informationen per API-Aufruf abgerufen werden müssen. Weitere Informationen zu Einstellungsberechtigungen unter Verwendung von IAM-Rollen finden Sie unter Anfügen einer IAM-Rolle an eine Instance.

IMDSv2

```
<powershell>
    [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri 'http://169.254.169.254/latest/api/token' -
UseBasicParsing
    $instanceId = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" =
 $token} -Method GET -Uri 'http://169.254.169.254/latest/meta-data/instance-id' -
UseBasicParsing
 $nameValue = (Get-EC2Tag -Filter @{Name="resource-id";Value=
$instanceid},@{Name="key";Value="Name"}).Value
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
```

```
        {$ErrorMessage = $_.Exception.Message
        Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

IMDSv1

```
<powershell>
 $instanceId = (Invoke-WebRequest http://169.254.169.254/latest/meta-data/instance-
id -UseBasicParsing).content
 $nameValue = (Get-EC2Tag -Filter @{Name="resource-id";Value=
$instanceid},@{Name="key";Value="Name"}).Value
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

Sie können die Instance auch mit Tags aus Instance-Metadaten umbenennen, wenn Ihre Instance so konfiguriert ist, dass über die Instance-Metadaten auf Tags zugegriffen wird. Weitere Informationen finden Sie unter Zeigen Sie Tags für Ihre EC2 Instances mithilfe von Instanz-Metadaten an.

IMDSv2

```
<powershell>
    [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri 'http://169.254.169.254/latest/api/token' -
UseBasicParsing
 $nameValue = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token}
 -Method GET -Uri 'http://169.254.169.254/latest/meta-data/tags/instance/Name' -
UseBasicParsing
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
```

```
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

IMDSv1

```
<powershell>
 $nameValue = Get-EC2InstanceMetadata -Path /tags/instance/Name
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between
 1 and 15 characters in length and contains only alphanumeric or hyphen characters"}
</powershell>
```

Identifizieren Sie jede Instance, die in einer einzelnen Anfrage gestartet wurde

Dieses Beispiel zeigt, wie Sie sowohl Benutzerdaten als auch Instance-Metadaten verwenden können, um Ihre EC2 Amazon-Instances zu konfigurieren.

> **Note**
>
> Die Beispiele in diesem Abschnitt verwenden die IPv4 Adresse des IMDS:`169.254.169.254`. Wenn Sie Instanz-Metadaten für EC2 Instances über die IPv6 Adresse abrufen, stellen Sie sicher, dass Sie stattdessen die IPv6 Adresse aktivieren und verwenden:. `[fd00:ec2::254]` Die IPv6 Adresse des IMDS ist mit Befehlen kompatibel

IMDSv2 . Die IPv6 Adresse ist nur auf Nitro-basierten Instances in Subnetzen zugänglich, die von IPv6 -unterstützt werden (Dual-Stack oder nur). IPv6

Alice möchte vier Instances ihres bevorzugten Datenbank-AMI starten; die erste soll dabei als Master-Instance fungieren, die übrigen drei als Replikate. Beim Start der Instances möchte sie Benutzerdaten für die Replikationsstrategien der einzelnen Replikate hinzufügen. Sie weiß, dass diese Daten in allen vier Instances verwendet werden, d. h. sie muss die Benutzerdaten so strukturieren, dass jede Instance erkennt, welcher Teile für sie gedacht ist. Dies kann mithilfe des Instance-Metadatenwerts `ami-launch-index` erreicht werden; dieser ist für jede Instance eindeutig. Wenn sie mehrere Instances gleichzeitig startet, gibt das `ami-launch-index` die Reihenfolge an, in der die Instances gestartet wurden. Der Wert für die zuerst gestartete Instance ist `0`.

Hier sind die Benutzerdaten, die Alice erstellt hat.

```
replicate-every=1min | replicate-every=5min | replicate-every=10min
```

Die `replicate-every=1min`-Daten definieren die Konfiguration für das erste Replikat, `replicate-every=5min` definiert die Konfiguration für das zweite Replikat usw. Alice beschließt, diese Daten als ASCII-Zeichenfolge bereitzustellen; die Daten für die einzelnen Instances werden dabei durch ein Pipe-Symbol (`|`) voneinander getrennt.

Alice startet vier Instances mit dem Befehl run-instances unter Angabe der Benutzerdaten.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 4 \
    --instance-type t2.micro \
    --user-data "replicate-every=1min | replicate-every=5min | replicate-every=10min"
```

Nach dem Start sind in jeder Instance eine Kopie der Benutzerdaten und die folgenden Metadaten vorhanden:

- AMI-ID: ami-0abcdef1234567890
- Reservation ID: r-1234567890abcabc0
- Public keys: none
- Security group name: default

- Instance type: t2.micro

Jede Instance hat jedoch eindeutige Metadaten, wie in den folgenden Tabellen dargestellt.

Metadaten	Value
instance-id	i-1234567890abcdef0
ami-launch-index	0
public-hostname	ec2-203-0-113-25.compute-1.amazonaws.com
public-ipv4	67.202.51.223
local-hostname	ip-10-251-50-12.ec2.internal
local-ipv4	10.251.50.35

Metadaten	Value
instance-id	i-0598c7d356eba48d7
ami-launch-index	1
public-hostname	ec2-67-202-51-224.compute-1.amazonaws.com
public-ipv4	67.202.51.224
local-hostname	ip-10-251-50-36.ec2.internal
local-ipv4	10.251.50.36

Metadaten	Value
instance-id	i-0ee992212549ce0e7
ami-launch-index	2

Metadaten	Value
public-hostname	ec2-67-202-51-225.compute-1.amazonaws.com
public-ipv4	67.202.51.225
local-hostname	ip-10-251-50-37.ec2.internal
local-ipv4	10.251.50.37

Metadaten	Value
instance-id	i-1234567890abcdef0
ami-launch-index	3
public-hostname	ec2-67-202-51-226.compute-1.amazonaws.com
public-ipv4	67.202.51.226
local-hostname	ip-10-251-50-38.ec2.internal
local-ipv4	10.251.50.38

Alice mit dem Wert unter `ami-launch-index` bestimmen, welcher Teil der Benutzerdaten für eine bestimmte Instance anzuwenden ist.

1. Sie stellt eine Verbindung mit einer der Instances her und ruft den `ami-launch-index` für diese Instance ab, um sicherzustellen, dass es sich um eines der Replikate handelt:

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/meta-data/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/ami-launch-index
   2
   ```

Für die folgenden Schritte verwenden die IMDSv2 Anfragen das gespeicherte Token aus dem vorherigen IMDSv2 Befehl, vorausgesetzt, das Token ist nicht abgelaufen.

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-launch-index
2
```

2. Sie speichert das `ami-launch-index` als Variable.

   IMDSv2

   ```
   [ec2-user ~]$ ami_launch_index=`curl -H "X-aws-ec2-metadata-token: $TOKEN"
    http://169.254.169.254/latest/meta-data/ami-launch-index`
   ```

   IMDSv1

   ```
   [ec2-user ~]$ ami_launch_index=`curl http://169.254.169.254/latest/meta-data/ami-
   launch-index`
   ```

3. Sie speichert die Benutzerdaten als Variable.

   IMDSv2

   ```
   [ec2-user ~]$ user_data=`curl -H "X-aws-ec2-metadata-token: $TOKEN"
    http://169.254.169.254/latest/user-data`
   ```

   IMDSv1

   ```
   [ec2-user ~]$ user_data=`curl http://169.254.169.254/latest/user-data`
   ```

4. Schließlich verwendet Alice den Befehl cut, um den Teil der Benutzerdaten zu extrahieren, der für diese Instance gilt.

   IMDSv2

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   replicate-every=5min
   ```

   IMDSv1

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   ```

```
replicate-every=5min
```

Ermitteln, ob es sich bei einem Host um eine EC2-Instance handelt

Sie müssen möglicherweise ermitteln, ob Ihre Anwendung oder Website auf einer EC2-Instance ausgeführt wird, insbesondere in einer gemischten Computerumgebung. Sie können eine der folgenden Optionen verwenden, um zu ermitteln, ob der Host für Ihre Anwendung oder Website eine EC2-Instance ist.

Optionen

- Untersuchen von Instance-Identitätsdokument
- Überprüfen des System-UUID
- Überprüfen der System-ID zur Generierung der virtuellen Maschine

Untersuchen von Instance-Identitätsdokument

Jede Instance verfügt über ein signiertes Identitätsdokument für die Instance, das Sie kryptografisch überprüfen können. Sie können diese Dokumente über den Instance Metadata Service (IMDS) finden.

Weitere Informationen finden Sie unter Instance-Identitätsdokumente.

Überprüfen des System-UUID

Sie können die System-UUID abrufen und im ersten Oktett der UUID nach `EC2` suchen (unter Linux ist dies möglicherweise ein klein geschriebenes `ec2`). Diese Methode ist zwar schnell aber potenziell ungenau, weil auch Systeme, die keine EC2 Instance sind, eine UUID haben können, die mit diesen Zeichenfolgen beginnt. Darüber hinaus verwenden einige Versionen von SMBIOS das Little-Endian-Format, das `EC2` am Anfang der UUID nicht einschließt. Dies kann bei EC2-Instances der Fall sein, die SMBIOS 2.4 für Windows verwenden, oder bei anderen Linux-Distributionen als Amazon Linux, die über eine eigene Implementierung von SMBIOS verfügen.

Linux-Beispiel: Abrufen der UUID von DMI (nur HVM-AMIs)

Verwenden Sie den folgenden Befehl, um die UUID mit dem Desktop Management Interface (DMI) abzurufen:

```
[ec2-user ~]$ sudo dmidecode --string system-uuid
```

In der folgenden Beispielausgabe beginnt die UUID mit „EC2“. Es handelt sich daher wahrscheinlich um eine EC2 Instance.

```
EC2E1916-9099-7CAF-FD21-012345ABCDEF
```

In der folgenden Beispielausgabe ist die UUID im Little-Endian-Format dargestellt.

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Alternativ können Sie für Instances, die auf dem Nitro-System basieren, den folgenden Befehl verwenden:

```
[ec2-user ~]$ cat /sys/devices/virtual/dmi/id/board_asset_tag
```

Wenn die Ausgabe eine Instance-ID ist, ist das System als folgende Beispielausgabe eine EC2-Instance:

```
i-0af01c0123456789a
```

Linux-Beispiel: Abrufen der UUID vom Hypervisor (nur PV-AMIs)

Verwenden Sie den folgenden Befehl, um die UUID vom Hypervisor zu erhalten:

```
[ec2-user ~]$ cat /sys/hypervisor/uuid
```

In der folgenden Beispielausgabe beginnt die UUID mit „ec2“. Es handelt sich daher wahrscheinlich um eine EC2 Instance.

```
ec2e1916-9099-7caf-fd21-012345abcdef
```

Windows-Beispiel: Abrufen der UUID mit WMI oder Windows PowerShell

Verwenden Sie die Windows-Verwaltungsinstrumentation-Befehlszeile (WMIC) wie folgt:

```
wmic path win32_computersystemproduct get uuid
```

Wenn Sie Windows PowerShell verwenden, verwenden Sie das cmdlet Get-WmiObject wie folgt:

```
PS C:\> Get-WmiObject -query "select uuid from Win32_ComputerSystemProduct" | Select
 UUID
```

In der folgenden Beispielausgabe beginnt die UUID mit „EC2“. Es handelt sich daher wahrscheinlich um eine EC2 Instance.

```
EC2AE145-D1DC-13B2-94ED-012345ABCDEF
```

Bei Instances mit SMBIOS 2.4 kann die UUID im Little-Endian-Format angegeben werden, zum Beispiel:

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Überprüfen der System-ID zur Generierung der virtuellen Maschine

Eine ID zur Generierung virtueller Maschinen besteht aus einem eindeutigen Puffer von 128 Bit, der als kryptografische, zufällige Ganzzahl-ID interpretiert wird. Sie können die ID zur Generierung der virtuellen Maschine abrufen, um Ihre Amazon-Elastic-Compute-Cloud-Instance zu identifizieren. Die Generierungs-ID wird im Gastbetriebssystem der Instance durch einen ACPI-Tabelleneintrag verfügbar gemacht. Der Wert ändert sich, wenn Ihre Maschine geklont, kopiert oder in AWS importiert wird, z. B. mit VM Import/Export.

Beispiel: Die ID zur Generierung der virtuellen Maschine aus Linux abrufen

Sie können die folgenden Befehle verwenden, um die ID zur Generierung der virtuellen Maschine von Ihren Instances abzurufen, auf denen Linux ausgeführt wird.

Amazon Linux 2

1. Aktualisieren Sie Ihre vorhandenen Softwarepakete bei Bedarf mit dem folgenden Befehl:

   ```
   sudo yum update
   ```

2. Wenn nötig, beziehen Sie das busybox-Paket mit dem folgenden Befehl:

   ```
   sudo curl https://www.rpmfind.net/linux/epel/next/8/Everything/x86_64/Packages/
   b/busybox-1.35.0-2.el8.next.x86_64.rpm --output busybox.rpm
   ```

3. Installieren Sie ggf. die Voraussetzungspakete mit dem folgenden Befehl:

```
sudo yum install busybox.rpm iasl -y
```

4. Führen Sie den folgenden `iasl`-Befehl aus, um eine Ausgabe aus der ACPI-Tabelle zu erzeugen:

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

5. Führen Sie den folgenden Befehl aus, um die Ausgabe des `iasl`-Befehls zu prüfen:

```
cat SSDT2.dsl
```

Die Ausgabe sollte den Adressraum liefern, der zum Abrufen der ID zur Generierung der virtuellen Maschine erforderlich ist:

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
```

```
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
*     OEM ID           "AMAZON"
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
        })
    }
}
}
```

6. (Optional) Erweitern Sie Ihre Terminalberechtigungen für die verbleibenden Schritte mit dem folgenden Befehl:

```
sudo -s
```

7. Verwenden Sie den folgenden Befehl, um den zuvor erfassten Adressraum zu speichern:

```
VMGN_ADDR=0xFED01000
```

8. Verwenden Sie den folgenden Befehl, um den Adressraum zu durchlaufen und die ID zur Generierung der virtuellen Maschine zu erstellen:

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

9. Rufen Sie die ID zur Generierung der virtuellen Maschine mit dem folgenden Befehl aus der Ausgabedatei ab:

```
cat vmgenid ; echo
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
EC2F335D979132C4165896753E72BD1C
```

Ubuntu

1. Aktualisieren Sie Ihre vorhandenen Softwarepakete bei Bedarf mit dem folgenden Befehl:

```
sudo apt update
```

2. Installieren Sie ggf. die Voraussetzungspakete mit dem folgenden Befehl:

```
sudo apt install busybox iasl -y
```

3. Führen Sie den folgenden `iasl`-Befehl aus, um eine Ausgabe aus der ACPI-Tabelle zu erzeugen:

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

4. Führen Sie den folgenden Befehl aus, um die Ausgabe des `iasl`-Befehls zu prüfen:

```
cat SSDT2.dsl
```

Die Ausgabe sollte den Adressraum liefern, der zum Abrufen der ID zur Generierung der virtuellen Maschine erforderlich ist:

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
```

```
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
*     OEM ID           "AMAZON"
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
        })
```

```
    }
}
}
```

5. (Optional) Erweitern Sie Ihre Terminalberechtigungen für die verbleibenden Schritte mit dem folgenden Befehl:

```
sudo -s
```

6. Verwenden Sie die folgenden Befehle, um den zuvor erfassten Adressraum zu speichern:

```
VMGN_ADDR=0xFED01000
```

7. Verwenden Sie den folgenden Befehl, um den Adressraum zu durchlaufen und die ID zur Generierung der virtuellen Maschine zu erstellen:

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

8. Rufen Sie die ID zur Generierung der virtuellen Maschine mit dem folgenden Befehl aus der Ausgabedatei ab:

```
cat vmgenid ; echo
```

   Die Ausgabe sollte in etwa wie folgt aussehen:

```
EC2F335D979132C4165896753E72BD1C
```

Beispiel: Die ID zur Generierung der virtuellen Maschine aus Windows abrufen

Sie können eine Beispielanwendung erstellen, um die ID zur Generierung der virtuellen Maschine von Ihren Instances abzurufen, auf denen Windows ausgeführt wird. Weitere Informationen finden Sie unter Erhalten der ID zur Generierung der virtuellen Maschine in der Microsoft-Dokumentation.

Instance-Identitätsdokumente für Amazon-EC2-Instances

Jede Instance, die Sie starten, hat ein Instance-Identitätsdokument, das Informationen über die Instance selbst liefert. Sie können die Attribute der Instance mit Instance-Identitätsdokument validieren.

Das Instance-Identitätsdokument wird generiert, wenn die Instance angehalten und gestartet, neu gestartet oder gelauncht wird. Sie können über den Instance Metadata Service (IMDS) auf das Instance-Identitätsdokument einer Instance zugreifen. Die Anweisungen finden Sie unter Abrufen des Instance-Identitätsdokuments.

Das Instance-Identitätsdokument verwendet das Klartext-JSON-Format. Es enthält folgende Informationen.

Daten	Beschreibung
`accountId`	Die ID des AWS-Kontos, das die Instance gestartet hat.
`architecture`	Die Architektur des AMIs, das zum Starten der Instance verwendet wird (i386 | x86_64 | arm64).
`availabilityZone`	Der Name der Availability Zone, in der die Instance ausgeführt wird. Beispiel, `us-east-1` . Beachten Sie, dass sich die Namen der Availability Zones in verschiedenen AWS-Konten unterscheiden können.
`billingProducts`	Die Abrechnungsprodukte der Instance.
`devpayProductCodes`	Veraltet.
`imageId`	Die ID des zum Start der Instance verwendeten AMI.
`instanceId`	Die ID der Instance.
`instanceType`	Der Instance-Typ der Instance.
`kernelId`	Die ID des mit der Instance verknüpften Kernels, falls zutreffend.
`marketplaceProductCodes`	Der AWS Marketplace-Produkt-Code des AMIs, mit dem die Instance gestartet wurde.

Daten	Beschreibung
`pendingTime`	Das Datum und die Uhrzeit, zu der die Instance gestartet wurde.
`privateIp`	Die private IP-Adresse der Instance. Bei reinen IPv4-Instances und Dual-Stack-Instances enthält dies die IPv4-Adresse. Bei reinen IPv6-Instances enthält dies die IPv6-Adresse.
`ramdiskId`	Die ID der mit der Instance verknüpften RAM-Disk, falls zutreffend.
`region`	Die Region, in der die Instance ausgeführt wird.
`version`	Die Version des Instance-Identitätsdokument-Formats.

Das Instance-Identitätsdokument für eine EC2-Instance abrufen

Das Instance-Identitätsdokument für eine Amazon-EC2-Instance verwendet ein Klartext-JSON-Format. Eine Beschreibung des Inhalts eines Instance-Identitätsdokuments finden Sie unter the section called “Instance-Identitätsdokumente”.

Das Instance-Identitätsdokument ist in den Instance-Metadaten der Instance in der Kategorie dynamische `instance-identity/document`-Daten gespeichert. Sie greifen auf das Instance-Identitätsdokument für eine Instance zu, indem Sie eine Verbindung mit der Instance herstellen und es aus den Instance-Metadaten abrufen.

Sie können mithilfe der IPv4-Adresse 169.254.169.254 oder der IPv6-Adresse fd00:ec2::254 zu einer Instance zugreifen. Dies sind Link-lokale Adressen, was bedeutet, dass Sie nur von der Instance aus auf sie zugreifen können. In den Beispielen in diesem Abschnitt wird die IPv4-Adresse des IMDS verwendet: 169.254.169.254. Um Instance-Metadaten für EC2-Instances über IPv6 abzurufen, verwenden Sie fd00:ec2::254.

Informationen zum Überprüfen der Echtheit eines Instance-Identitätsdokuments, nachdem Sie es abgerufen haben, finden Sie unter Verifizieren des Instance-Identitätsdokuments.

IMDSv2

Linux

Führen Sie den folgenden Befehl in Ihrer Linux-Instance aus, um das Instance-Identitätsdokument abzurufen.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/document
```

Windows

Führen Sie das folgende cmdlet in Ihrer Windows-Instance aus, um das Instance-Identitätsdokument abzurufen.

```
[string]$token = (Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token-ttl-seconds' = '21600'} `
    -Method PUT -Uri 'http://169.254.169.254/latest/api/token' -UseBasicParsing).Content
```

```
(Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $token} `
    -Uri 'http://169.254.169.254/latest/dynamic/instance-identity/document' -UseBasicParsing).Content
```

IMDSv1

Linux

Führen Sie den folgenden Befehl in Ihrer Linux-Instance aus, um das Instance-Identitätsdokument abzurufen.

```
curl http://169.254.169.254/latest/dynamic/instance-identity/document
```

Windows

Führen Sie das folgende cmdlet in Ihrer Windows-Instance aus, um das Instance-Identitätsdokument abzurufen.

```
(Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/document).Content
```

Es folgt eine Beispielausgabe.

```
{
```

```
    "devpayProductCodes" : null,
    "marketplaceProductCodes" : [ "1abc2defghijklm3nopqrs4tu" ],
    "availabilityZone" : "us-west-2b",
    "privateIp" : "10.158.112.84",
    "version" : "2017-09-30",
    "instanceId" : "i-1234567890abcdef0",
    "billingProducts" : null,
    "instanceType" : "t2.micro",
    "accountId" : "123456789012",
    "imageId" : "ami-5fb8c835",
    "pendingTime" : "2016-11-19T16:32:11Z",
    "architecture" : "x86_64",
    "kernelId" : null,
    "ramdiskId" : null,
    "region" : "us-west-2"
}
```

Instance-Identitätsdokument für eine Amazon-EC2-Instance verifizieren

Wenn Sie beabsichtigen, den Inhalt des Instance-Identitätsdokument für einen wichtigen Zweck zu verwenden, sollten Sie den Inhalt und die Authentizität überprüfen, bevor Sie es verwenden.

Das Klartext-Instance-Identitätsdokument wird von drei gehashten und verschlüsselten Signaturen ergänzt. Sie können diese Signaturen verwenden, um die Herkunft und Authentizität des Instance-Identitätsdokument und der darin enthaltenen Informationen zu überprüfen. Die folgenden Signaturen werden bereitgestellt:

- Base64-kodierte Signatur—Dies ist ein Base64-kodierter SHA256-Hash des Instance-Identitätsdokument, der mit einem RSA-Schlüsselpaar verschlüsselt wird.
- PKCS7-Signatur—Dies ist ein SHA1-Hash des Instance-Identitätsdokument, der mit einem DSA-Schlüsselpaar verschlüsselt wird.
- RSA-2048-Signatur—Dies ist ein SHA256-Hash des Instance-Identitätsdokument, der mit einem RSA-2048-Schlüsselpaar verschlüsselt wird.

Jede Signatur ist an einem anderen Endpunkt in den Metadaten der Instance verfügbar. Sie können je nach Ihren Hashing- und Verschlüsselungsanforderungen eine beliebige dieser Signaturen verwenden. Um die Signaturen zu verifizieren, müssen Sie das entsprechende öffentliche AWS Zertifikat verwenden.

Optionen

- Option 1: Verwenden der PKCS7-Signatur zur Verifizierung des Instance-Identitätsdokuments
- Option 2: Verwendung der Base64-kodierten Signatur zur Verifizierung des Instance-Identitätsdokuments
- Option 3: Verwenden der RSA-2048-Signatur zur Verifizierung des Instance-Identitätsdokuments

Option 1: Verwenden der PKCS7-Signatur zur Verifizierung des Instance-Identitätsdokuments

In diesem Thema wird erläutert, wie Sie das Instance-Identitätsdokument mit der PKCS7-Signatur und dem öffentlichen AWS-DSA-Zertifikat validieren.

Linux-Instances

Instance-Identitätsdokument mit der PKCS7-Signatur und dem öffentlichen AWS-DSA-Zertifikat verifizieren

1. Stellen Sie eine Verbindung mit der Instance her.
2. Rufen Sie die PKCS7-Signatur aus den Metadaten der Instance ab und fügen Sie sie zu einer Datei namens `pkcs7` mit benötigter Kopf- und Fußzeile hinzu. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

   IMDSv2

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
    && TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/pkcs7 >> pkcs7 \
    && echo "" >> pkcs7 \
    && echo "-----END PKCS7-----" >> pkcs7
   ```

   IMDSv1

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
    && curl -s http://169.254.169.254/latest/dynamic/instance-identity/pkcs7 >> pkcs7 \
    && echo "" >> pkcs7 \
    && echo "-----END PKCS7-----" >> pkcs7
   ```

3. Suchen Sie das öffentliche DSA-Zertifikat für Ihre Region in Öffentliche Zertifikate von AWS für Instance-Identitätsdokument-Signaturen und fügen Sie den Inhalt in eine neue Datei mit dem Namen `certificate` ein.
4. Verwenden Sie den Befehl OpenSSL smime, um die Signatur zu überprüfen. Fügen Sie die Option `-verify` ein, um anzugeben, dass die Signatur verifiziert werden muss, und die Option `-noverify`, um anzugeben, dass das Zertifikat nicht verifiziert werden muss.

   ```
   $ openssl smime -verify -in pkcs7 -inform PEM -certfile certificate -noverify | tee
    document
   ```

   Wenn die Signatur gültig ist, wird die Meldung `Verification successful` angezeigt.

   Der Befehl schreibt außerdem den Inhalt des Instance-Identitätsdokuments in eine neue Datei namens `document`. Mit den folgenden Befehlen können Sie den Inhalt des Instance-Identitätsdokuments aus den Instance-Metadaten mit dem Inhalt dieser Datei vergleichen.

   ```
   $ openssl dgst -sha256 < document
   ```

   ```
   $ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/document | openssl dgst -sha256
   ```

   Wenn die Signatur nicht verifiziert werden kann, wenden Sie sich an Support.

Windows-Instances

Voraussetzungen

Dieses Verfahren erfordert die `System.Security` Microsoft .NET Core-Klasse. Um die Klasse zu Ihrer PowerShell-Sitzung hinzuzufügen, führen Sie den folgenden Befehl aus.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> Der Befehl fügt die Klasse nur der aktuellen PowerShell-Sitzung hinzu. Wenn Sie eine neue Sitzung starten, müssen Sie den Befehl erneut ausführen.

Instance-Identitätsdokument mit der PKCS7-Signatur und dem öffentlichen AWS-DSA-Zertifikat verifizieren

1. Stellen Sie eine Verbindung mit der Instance her.
2. Rufen Sie die PKCS7-Signatur aus den Metadaten der Instance ab, konvertieren Sie sie in ein Byte-Array und fügen Sie sie an eine Variable namens a `$Signature`. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-ec2-
   metadata-token-ttl-seconds' = '21600'} -Uri http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} -Uri http://169.254.169.254/latest/
   dynamic/instance-identity/pkcs7).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Uri
    http://169.254.169.254/latest/dynamic/instance-identity/pkcs7).Content)
   ```

3. Rufen Sie das Klartext-Identitätsdokument der Instance aus den Instance-Metadaten ab, konvertieren Sie es in ein Byte-Array und fügen Sie es zu einer Variablen namens hinz `$Document`. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} -Uri http://169.254.169.254/latest/
   dynamic/instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Suchen Sie das öffentliche DSA-Zertifikat für Ihre Region in Öffentliche Zertifikate von AWS für Instance-Identitätsdokument-Signaturen und fügen Sie den Inhalt in eine neue Datei mit dem Namen `certificate.pem` ein.
5. Extrahieren Sie das Zertifikat aus der Zertifikatsdatei und speichern Sie es in einer Variablen mit dem Namen `$Store`.

```
PS C:\> $Store =
 [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
Path certificate.pem)))
```

6. Überprüfen Sie die Signatur.

```
PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
```

```
PS C:\> $SignatureDocument.Decode($Signature)
```

```
PS C:\> $SignatureDocument.CheckSignature($Store, $true)
```

   Wenn die Signatur gültig ist, gibt der Befehl keine Ausgabe zurück. Wenn die Signatur nicht verifiziert werden kann, gibt der Befehl zurüc `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer`. Wenn Ihre Signatur nicht verifiziert werden kann, wenden Sie sich an AWS -Support.

7. Validieren Sie den Inhalt des Instance-Identitätsdokuments.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

   Wenn der Inhalt des Identitätsdokuments der Instance gültig ist, gibt der Befehl zurüc `True`. Wenn das Instance-Identitätsdokument nicht validiert werden kann, wenden Sie sich an AWS -Support.

Option 2: Verwendung der Base64-kodierten Signatur zur Verifizierung des Instance-Identitätsdokuments

In diesem Thema wird erläutert, wie Sie das Instance-Identitätsdokument mit der base64-codierten Signatur und dem öffentlich AWS-RSA-Zertifikat verifizieren.

Linux-Instances

Instance-Identitätsdokument mit der base64-codierten Signatur und dem öffentlichen AWS-RSA-Zertifikat validieren

1. Stellen Sie eine Verbindung mit der Instance her.
2. Rufen Sie die base64-kodierte Signatur aus den Metadaten der Instance ab, konvertieren Sie sie in ein Binärformat und fügen Sie sie zu einer Datei namens hinz `signature`. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

   IMDSv2

   ```
   $ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/signature | base64 -d >> signature
   ```

   IMDSv1

   ```
   $ curl -s http://169.254.169.254/latest/dynamic/instance-identity/signature |
    base64 -d >> signature
   ```

3. Rufen Sie die Klartext-Instance-Identitätsdokument aus den Metadaten der Instance ab und fügen Sie sie zu einer Datei mit dem Namen hinz `document`. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

   IMDSv2

   ```
   $ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/document >> document
   ```

   IMDSv1

   ```
   $ curl -s http://169.254.169.254/latest/dynamic/instance-identity/document
    >> document
   ```

4. Suchen Sie das öffentliche RSA-Zertifikat für Ihre Region in Öffentliche Zertifikate von AWS für Instance-Identitätsdokument-Signaturen und fügen Sie den Inhalt in eine neue Datei mit dem Namen `certificate` ein.
5. Extrahieren Sie den öffentlichen Schlüssel aus dem öffentlichen AWS-RSA-Zertifikat und speichern Sie ihn in einer Datei namens `key`.

```
$ openssl x509 -pubkey -noout -in certificate >> key
```

6. Verwenden Sie den Befehl OpenSSL dgst, um die Instance-Identitätsdokument zu überprüfen.

```
$ openssl dgst -sha256 -verify key -signature signature document
```

Wenn die Signatur gültig ist, wird die Meldung `Verification successful` angezeigt.

Der Befehl schreibt außerdem den Inhalt des Instance-Identitätsdokuments in eine neue Datei namens `document`. Mit den folgenden Befehlen können Sie den Inhalt des Instance-Identitätsdokuments aus den Instance-Metadaten mit dem Inhalt dieser Datei vergleichen.

```
$ openssl dgst -sha256 < document
```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/document | openssl dgst -sha256
```

Wenn die Signatur nicht verifiziert werden kann, wenden Sie sich an Support.

Windows-Instances

Instance-Identitätsdokument mit der base64-codierten Signatur und dem öffentlichen AWS-RSA-Zertifikat validieren

1. Stellen Sie eine Verbindung mit der Instance her.
2. Rufen Sie die base64-kodierte Signatur aus den Metadaten der Instance ab, konvertieren Sie sie in ein Byte-Array und fügen Sie sie der Variablen mit dem Namen hinz `$Signature`. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

IMDSv2

```
PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
token).Content
```

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
 @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
instance-identity/signature).Content)
```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/signature).Content)
```

3. Rufen Sie das Klartext-Identitätsdokument der Instance aus den Instance-Metadaten ab, konvertieren Sie es in ein Byte-Array und fügen Sie es zu einer Variablen namens hinz `$Document`. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Suchen Sie das öffentliche RSA-Zertifikat für Ihre Region in Öffentliche Zertifikate von AWS für Instance-Identitätsdokument-Signaturen und fügen Sie den Inhalt in eine neue Datei mit dem Namen `certificate.pem` ein.

5. Überprüfen Sie das Instance-Identitätsdokument.

   ```
   PS C:\> [Security.Cryptography.X509Certificates.X509Certificate2]::new((Resolve-
   Path certificate.pem)).PublicKey.Key.VerifyData($Document, 'SHA256', $Signature)
   ```

Wenn die Signatur gültig ist, gibt der Befehl zurüc `True`. Wenn die Signatur nicht verifiziert werden kann, wenden Sie sich an Support.

Option 3: Verwenden der RSA-2048-Signatur zur Verifizierung des Instance-Identitätsdokuments

In diesem Thema wird erläutert, wie Sie das Instance-Identitätsdokument mit der RSA-2048-Signatur und dem öffentlichen AWS-RSA-2048-Zertifikat verifizieren.

Linux-Instances

Instance-Identitätsdokument mit der RSA-2048-Signatur und dem öffentlichen AWS-RSA-2048-Zertifikat verifizieren

1. Stellen Sie eine Verbindung mit der Instance her.
2. Rufen Sie die RSA-2048-Signatur aus den Metadaten der Instance ab und fügen Sie sie zusammen mit der notwendigen Kopf- und Fußzeile zu einer Datei namens `rsa2048` hinzu. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

   IMDSv2

   ```
   $ echo "-----BEGIN PKCS7-----" >> rsa2048 \
    && TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/rsa2048 >> rsa2048 \
    && echo "" >> rsa2048 \
    && echo "-----END PKCS7-----" >> rsa2048
   ```

   IMDSv1

   ```
   $ echo "-----BEGIN PKCS7-----" >> rsa2048 \
    && curl -s http://169.254.169.254/latest/dynamic/instance-identity/rsa2048 >> rsa2048 \
    && echo "" >> rsa2048 \
    && echo "-----END PKCS7-----" >> rsa2048
   ```

3. Suchen Sie das öffentliche RSA-2048-Zertifikat für Ihre Region in Öffentliche Zertifikate von AWS für Instance-Identitätsdokument-Signaturen und fügen Sie den Inhalt in eine neue Datei mit dem Namen `certificate` ein.
4. Verwenden Sie den Befehl OpenSSL smime, um die Signatur zu überprüfen. Fügen Sie die Option `-verify` ein, um anzugeben, dass die Signatur verifiziert werden muss, und die Option `-noverify`, um anzugeben, dass das Zertifikat nicht verifiziert werden muss.

   ```
   $ openssl smime -verify -in rsa2048 -inform PEM -certfile certificate -noverify |
    tee document
   ```

   Wenn die Signatur gültig ist, wird die Meldung `Verification successful` angezeigt. Wenn die Signatur nicht verifiziert werden kann, wenden Sie sich an Support.

Windows-Instances

Voraussetzungen

Dieses Verfahren erfordert die `System.Security` Microsoft .NET Core-Klasse. Um die Klasse zu Ihrer PowerShell-Sitzung hinzuzufügen, führen Sie den folgenden Befehl aus.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> Der Befehl fügt die Klasse nur der aktuellen PowerShell-Sitzung hinzu. Wenn Sie eine neue Sitzung starten, müssen Sie den Befehl erneut ausführen.

Instance-Identitätsdokument mit der RSA-2048-Signatur und dem öffentlichen AWS-RSA-2048-Zertifikat verifizieren

1. Stellen Sie eine Verbindung mit der Instance her.
2. Rufen Sie die RSA-2048-Signatur aus den Metadaten der Instance ab, konvertieren Sie sie in ein Byte-Array und fügen Sie sie an eine Variable namens a `$Signature`. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

IMDSv2

```
PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
token).Content
```

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
 @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
instance-identity/rsa2048).Content)
```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/rsa2048).Content)
```

3. Rufen Sie das Klartext-Identitätsdokument der Instance aus den Instance-Metadaten ab, konvertieren Sie es in ein Byte-Array und fügen Sie es zu einer Variablen namens hinz `$Document`. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Suchen Sie das öffentliche RSA-2048-Zertifikat für Ihre Region in Öffentliche Zertifikate von AWS für Instance-Identitätsdokument-Signaturen und fügen Sie den Inhalt in eine neue Datei mit dem Namen `certificate.pem` ein.

5. Extrahieren Sie das Zertifikat aus der Zertifikatsdatei und speichern Sie es in einer Variablen mit dem Namen `$Store`.

```
PS C:\> $Store =
 [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
Path certificate.pem)))
```

6. Überprüfen Sie die Signatur.

```
PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
```

```
PS C:\> $SignatureDocument.Decode($Signature)
```

```
PS C:\> $SignatureDocument.CheckSignature($Store, $true)
```

   Wenn die Signatur gültig ist, gibt der Befehl keine Ausgabe zurück. Wenn die Signatur nicht verifiziert werden kann, gibt der Befehl zurück `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer`. Wenn Ihre Signatur nicht verifiziert werden kann, wenden Sie sich an AWS -Support.

7. Validieren Sie den Inhalt des Instance-Identitätsdokuments.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

   Wenn der Inhalt des Identitätsdokuments der Instance gültig ist, gibt der Befehl zurück `True`. Wenn das Instance-Identitätsdokument nicht validiert werden kann, wenden Sie sich an AWS -Support.

Öffentliche Zertifikate von AWS für Instance-Identitätsdokument-Signaturen

Die folgenden öffentlichen AWS-Zertifikate können verwendet werden, um den Inhalt des Instance-Identitätsdokuments einer Instance zu überprüfen, wie in Verifizieren des Instance-Identitätsdokuments beschrieben.

Stellen Sie sicher, dass Sie das richtige Zertifikat für Ihre Region und das von Ihnen verwendete Überprüfungsverfahren verwenden. Wenn Sie die PKCS7-Signatur verifizieren, verwenden Sie das DSA-Zertifikat. Wenn Sie die Base64-codierte Signatur verifizieren, verwenden Sie das RSA-Zertifikat. Wenn Sie die RSA-2048-Signatur verifizieren, verwenden Sie das RSA-2048-Zertifikat.

Erweitern Sie unten jede Region, um die regionsspezifischen Zertifikate anzuzeigen.

USA Ost (Nord-Virginia) – us-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUE1y2NIKCU+Rg4uu4u32koG9QEYIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MzQwMVoXDTI5MDQyODE3MzQwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUE1y2NIKC
U+Rg4uu4u32koG9QEYIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAlxSmwcWnhT4uAeSinJuz+1BTcKhVSWb5jT8pYjQb8ZoZkXXRGb09mvYeU
```

```
NeqOBr27rvRAnaQ/9LUQf72+SahDFuS4CMI8nwowytqbmwquqFr4dxA/SDADyRiF
ea1UoMuNHTY49J/1vPomqsVn7mugTp+TbjqCfOJTpu0temHcFA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALFpzEAVWaQZMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU5MTJaGA8yMTk1MDExNzA4NTkxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjS2vqZu9mEOhOq+0bRpAbCUiapbZMFNQqRg7kTlr7Cf+gDqXKpHPjsng
SfNz+JHQd8WPI+pmNs+q0Z2aTe23klmf2U52KH9/j1k8RlIbap/yFibFTSedmegX
E5r447GbJRsHUmuIIfZTZ/oRlpuIIO5/Vz7SOj22tdkdY2ADp7caZkNxhSP915fk
2jJMTBUOzyXUS2rBU/ulNHbTTeePjcEkvzVYPahD30TeQ+/A+uWUu89bHSQOJR8h
Um4cFApzZgN3aD5j2LrSMu2pctkQwf9CaWyVznqrsGYjYOY66LuFzSCXwqSnFBfv
fFBAFsjCgY24G2DoMyYkF3MyZlu+rwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUrynSPp4uqSECwy+PiO4qyJ8TWSkwgY4GA1UdIwSBhjCBg4AUrynS
Pp4uqSECwy+PiO4qyJ8TWSmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALFpzEAVWaQZMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADW/s8lXijwdP6NkEoH1m9XLrvK4YTqkNfR6
er/uRRgTx2QjFcMNrx+g87gAml11z+D0crAZ5LbEhDMs+JtZYR3ty0HkDk6SJM85
haoJNAFF7EQ/zCp1EJRIkLLsC7bcDL/Eriv1swt78/BB4RnC9W9kSp/sxd5svJMg
N9a6FAplpNRsWAnbP8JBlAP93oJzblX2LQXgykTghMkQO7NaY5hg/H5o4dMPclTK
lYGqlFUCH6A2vdrxmpKDLmTn5//5pujdD2MN0df6sZWtxwZ0osljV4rDjm9Q3VpA
NWIsDEcp3GUB4proOR+C7PNkY+VGODitBOw09qBGosCBstwyEqY=
-----END CERTIFICATE-----
```

USA Ost (Ohio) – us-east-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
```

```
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUVJTc+hOU+8Gk3JlqsX438Dk5c58wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MTE0OVoXDTI5MDQyODE3MTE0OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUVJTc+hOU
+8Gk3JlqsX438Dk5c58wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAywJQaVNWJqW0R0T0xVOSoN1GLk9x9kKEuN67RN9CLin4dA97qa7Mr5W4P
FZ6vnh5CjOhQBRXV9xJUeYSdqVItNAUFK/fEzDdjf1nUfPlQ3OJ49u6CV01NoJ9m
usvY9kWcV46dqn2bk2MyfTTgvmeqP8fiMRPxxnVRkSzlldP5Fg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM07oeX4xevdMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA2MTAx
MjU4MThaGA8yMTk1MTExNDEyNTgxOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```

```
CgKCAQEA6v6kGMnRmFDLxBEqXzP4npnL65OO0kmQ7w8YXQygSdmNIoScGSU5wfh9
mZdcvCxCdxgALFsFqPvH8fqiE9ttI0fEfuZvHOs8wUsIdKr0Zz0MjSx3cik4tKET
ch0EKfMnzKOgDBavraCDeX1rUDU0Rg7HFqNAOry3uqDmnqtk00XC9GenS3z/7ebJ
fIBEPAam5oYMVFpX6M6St77WdNE8wEU8SuerQughiMVx9kMB07imeVHBiELbMQ0N
lwSWRL/61fA02keGSTfSp/0m3u+lesf2VwVFhqIJs+JbsEscPxOkIRlzy8mGd/JV
ONb/DQpTedzUKLgXbw7KtO3HTG9iXQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU2CTGYE5fTjx7gQXzdZSGPEWAJY4wgY4GA1UdIwSBhjCBg4AU2CTG
YE5fTjx7gQXzdZSGPEWAJY6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM07oeX4xevdMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANdqkIpVypr2PveqUsAKke1wKCOSuw1UmH9k
xX1/VRoHbrI/UznrXtPQOPMmHA2LKSTedwsJuorUn3cFH6qNs8ixBDrl8pZwfKOY
IBJcTFBbI1xBEFkZoO3wczzo5+8vPQ60RVqAaYb+iCa1HFJpccC3Ovajfa4GRdNb
n6FYnluIcDbmpcQePoVQwX7W3oOYLB1QLN7fE6H1j4TBIsFdO3OuKzmaifQlwLYt
DVxVCNDabpOr6Uozd5ASm4ihPPoEoKo7Ilp0fOT6fZ41U2xWA4+HF/89UoygZSo7
K+cQ90xGxJ+gmlYbLFR5rbJOLfjrgDAb2ogbFy8LzHo2ZtSe60M=
-----END CERTIFICATE-----
```

USA West (Nordkalifornien) – us-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUK2zmY9PUSTR7rc1k2OwPYu4+g7wwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MDI0M1oXDTI5MDQyODE3MDI0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUK2zmY9PU
STR7rc1k2OwPYu4+g7wwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQA1Ng4QmN4n7iPh5CnadSOc0ZfM7by0dBePwZJyGvOHdaw6P6E/vEk76KsC
Q8p+akuzVzVPkU4kBK/TRqLp19wEWoVwhhTaxHjQ1tTRHqXIVlrkw4JrtFbeNM21
GlkSLonuzmNZdivn9WuQYeGe7nUD4w3q9GgiF3CPorJe+UxtbA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJANNPkIpcyEtIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAzMDdaGA8yMTk1MDQwMzA5MDMwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApHQGvHvq3SVCzDrC7575BW7GWLzcj8CLqYcL3YY7Jffupz7OjcftO57Z
4fo5Pj0CaS8DtPzh8+8vdwUSMbiJ6cDd3ooio3MnCq6DwzmsY+pY7CiI3UVG7KcH
4TriDqr1Iii7nB5MiPJ8wTeAqX89T3SYaf6Vo+4GCb3LCDGvnkZ9TrGcz2CHkJsj
AIGwgopFpwhIjVYm7obmuIxSIUv+oNH0wXgDL029Zd98SnIYQd/njiqkzE+lvXgk
4h4Tu17xZIKBgFcTtWPky+POGu81DYFqiWVEyR2JKKm2/iR1dL1YsT39kbNg47xY
aR129sS4nB5Vw3TRQA2jL0ToTIxzhQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUgepyiONs8j+q67dmcWu+mKKDa+gwgY4GA1UdIwSBhjCBg4AUgepy
iONs8j+q67dmcWu+mKKDa+ihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJANNPkIpcyEtIMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGLFWyutf1u0xcAc+kmnMPqtc/Q6b79VIX0E
tNoKMI2KR8lcV8ZElXDb0NC6v8UeLpe1WBKjaWQtEjL1ifKg9hdY9RJj4RXIDSK7
```

```
33qCQ8juF4vep2U5TTBd6hfWxt1Izi88xudjixmbpUU4YKr8UPbmixldYR+BEx0u
B1KJi9l1lxvuc/Igy/xeHOAZEjAXzVvHp8Bne33VVwMiMxWECZCiJxE4I7+Y6fqJ
pLLSFFJKbNaFyXlDiJ3kXyePEZSc1xiWeyRB2ZbTi5eu7vMG4i3AYWuFVLthaBgu
lPfHafJpj/JDcqt2vKUKfur5edQ6j1CGdxqqjawhOTEqcN8m7us=
-----END CERTIFICATE-----
```

USA West (Oregon) – us-west-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFx8PxCkbHwpD31bOyCtyz3GclbgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MjM1OVoXDTI5MDQyODE3MjM1OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
```

```
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFx8PxCkb
HwpD31bOyCtyz3GclbgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBzOl+9Xy1+UsbUBI95HO9mbbdnuX+aMJXgG9uFZNjgNEbMcvx+h8P9IMko
z7PzFdheQQ1NLjsHH9mSR1SyC4m9ja6BsejH5nLBWyCdjfdP3muZM4O5+r7vUa1O
dWU+hP/T7DUrPAIVMOE7mpYa+WPWJrN6BlRwQkKQ7twm9kDalA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALZL3lrQCSTMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAxMzJaGA8yMTk1MDExNzA5MDEzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA02Y59qtAA0a6uzo7nEQcnJ26OKF+LRPwZfixBH+EbEN/Fx0gYy1jpjCP
s5+VRNg6/WbfqAsV6X2VSjUKN59ZMnMY9ALA/Ipz0n00Huxj38EBZmX/NdNqKm7C
qWu1q5kmIvYjKGiadfboU8wLwLcHo8ywvfgI6FiGGsEO9VMC56E/hL6Cohko11LW
dizyvRcvg/IidazVkJQCN/4zC9PUOVyKdhW33jXy8BTg/QH927QuNk+ZzD7HH//y
tIYxDhR6TIZsSnRjz3bOcEHxt1nsidc65mY0ejQty4hy7ioSiapw316mdbtE+RTN
fcH9FPIFKQNBpiqfAW5Ebp3Lal3/+wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU7coQx8Qnd75qA9XotSWT3IhvJmowgY4GA1UdIwSBhjCBg4AU7coQ
x8Qnd75qA9XotSWT3IhvJmqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALZL3lrQCSTMMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFZ1e2MnzRaXCaLwEC1pW/f0oRG8nHrlPZ9W
OYZEWbh+QanRgaikBNDtVTwARQcZm3z+HWSkaIx3cyb6vM0DSkZuiwzm1LJ9rDPc
aBm03SEt5v8mcc7sXWvgFjCnUpzosmky6JheCD4O1Cf8k0olZ93FQnTrbg62OK0h
83mGCDeVKU3hLH97FYoUq+3N/IliWFDhvibAYYKFJydZLhIdlCiiB99AM6Sg53rm
oukS3csyUxZyTU2hQfdjyo1nqW9yhvFAKjnnggiwxNKTTPZzstKW8+cnYwiiTwJN
QpVoZdt0SfbuNnmwRUMi+QbuccXweav29QeQ3ADqjgB0CZdSRKk=
-----END CERTIFICATE-----
```

Afrika (Kapstadt) – af-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7DCCAqwCCQCncbCtQbjuyzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
```

```
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA2MDQxMjQ4MDVaFw00
NTA2MDQxMjQ4MDVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQC12Nr1gMrHcFSZ7S/A
pQBSCMHWmn2qeoQTMVWqe50fnTd0zGFxDdIjKxUK58/8zjWG5uR4TXRzmZpGpmXB
bSufAR6BGqud2LnT/HIWGJAsnX2uOtSyNfCoJigqwhea5w+CqZ6I7iBDdnB4TtTw
qO6TlnExHFVj8LMkylZgiaE1CQIVAIhdobse4K0QnbAhCL6R2euQzloXAoGAV/21
WUuMz/79Ga0JvQcz1FNy1sT0pU9rU4TenqLQIt5iccn/7EIfNtvVO5TZKulIKq7J
gXZr0x/KIT8zsNweetLOaGehPIYRMPX0vunMMR7hN7qA7W17WZv/76adywIsnDKq
ekfe15jinaX8MsKUdyDK7Y+ifCG4PVhoM4+W2XwDgYQAAoGAIxOKbVgwLxbn6Pi2
6hBOihFv16jKxAQI0hHzXJLV0Vyv9QwnqjJJRfOCy3dB0zicLXiIxeIdYfvqJr+u
hlN8rGxEZYYJjEUKMGvsc0DW85jonXz0bNfcP0aaKH0lKKVjL+OZi5n2kn9wgdo5
F3CVnMl8BUra8A1Tr2yrrE6TVZ4wCQYHKoZIzjgEAwMvADAsAhQfa7MCJZ+/TEY5
AUr0J4wm8VzjoAIUSYZVu2NdRJ/ERPmDfhW5EsjHlCA=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAKumfZiRrNvHMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTExMjcw
NzE0MDVaGA8yMTk5MDUwMjA3MTQwNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDFd571nUzVtke3rPyRkYfvs3jh0C0EMzzG72boyUNjnfw1+m0TeFraTLKb9T6F
7TuB/ZEN+vmlYqr2+5Va8U8qLbPF0bRH+FdaKjhgWZdYXxGzQzU3ioy5W5ZM1VyB
7iUsxEAlxsybC3ziPYaHI42UiTkQNahmoroNeqVyHNnBpQIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAAJLylWyElEgOpW4B1XPyRVD4pAds8Guw2+krgqkY0HxLCdjosuH
RytGDGN+q75aAoXzW5a7SGpxLxk6Hfv0xp3RjDHsoeP0i1d8MD3hAC5ezxS4oukK
s5gbPOnokhKTMPXbTdRn5ZifCbWlx+bYN/mTYKvxho7b5SVg2o1La9aK
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAIFI+O5A6/ZIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA2MDQx
MjQ4MDRaGA8yMTk4MTEwNzEyNDgwNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```

```
CgKCAQEAy7/WHBBHOrk+20aumT07g8rxrSM0UXgki3eYgKauPCG4Xx//vwQbuZwI
oeVmR9nqnhfij2wOcQdbLandh0EGtbxerete3IoXzd1KXJb11PVmzrzyu5SPBPuP
iCeV4qdjjkXo2YWM6t9YQ911hcG96YSp89TBXFYUh3KLxfqAdTVhuC0NRGhXpyii
j/czo9njofHhqhTr7UEyPun8NVS2QWctLQ86N5zWR3Q0GRoVqqMrJs0cowHTrVw2
9Qr7QBjjBOVbyYmtYxm/DtiKprYV/e6bCAVok015X1sZDd3oCOQNoGlv5XbHJe2o
JFD8GRRy2rkWO/lNwVFDcwec6zC3QwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCE
goqzjpCpmMgCpszFHwvRaSMbspKtK7wNImUjrSBOfBJsfFulyg1Zgn2nDCK7kQhx
jMJmNIvXbps3yMqQ2cHUkKcKf5t+WldfeT4Vk1Rz6HSA8sd0kgVcIesIaoy2aaXU
VEB/oQziRGyKdN1d4TGYVZXG44CkrzSDvlbmfiTq5tL+kAieznVF3bzHgPZW6hKP
EXC3G/IXrXicFEe6YyE1Rakl62VncYSXiGe/i2XvsiNH3Qlmnx5XS7W0SCN0oAxW
EH9twibauv82DVg1WOkQu8EwFw8hFde9X0Rkiu0qVcuU8lJgFEvPWMDFU5sGB6ZM
gkEKTzMvlZpPbBhg99Jl
-----END CERTIFICATE-----
```

Asien-Pazifik (Hongkong) – ap-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQCO7MJe5Y3VLjAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDMwMjIxMjFaFw00
NTAyMDMwMjIxMjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDvQ9RzVvf4MAwGbqfX
blCvCoVb9957OkLGn/04CowHXJ+vTBR7eyIa6AoXltsQXBOmrJswToFKKxT4gbuw
jK7s9QQX4CmTRWcEgO2RXtZSVjOhsUQMh+yf7Ht4OVL97LWnNfGsX2cwjcRWHYgI
7lvnuBNBzLQHdSEwMNq0Bk76PwIVAMan6XIEEPnwr4e6u/RNnWBGKd9FAoGBAOCG
eSNmxpW4QFu4pIlAykm6EnTZKKHT87gdXkAkfoC5fAfOxxhnE2HezZHp9Ap2tMV5
8bWNvoPHvoKCQqwfm+OUBlAxC/3vqoVkKL2mG1KgUH9+hrtpMTkwO3RREnKe7I5O
x9qDimJpOihrL4I0dYvy9xUOoz+DzFAW8+ylWVYpA4GFAAKBgQDbnBAKSxWr9QHY
6Dt+EFdGz6lAZLedeBKpaP53Z1DTO34J0C55YbJTwBTFGqPtOLxnUVDlGiD6GbmC
80f3jvogPR1mSmGsydbNbZnbUEVWrRhe+y5zJ3g9qs/DWmDW0deEFvkhWVnLJkFJ
9pdOu/ibRPH1lE2nz6pK7GbOQtLyHTAJBgcqhkjOOAQDAzAAMC0CFQCoJlwGtJQC
cLoM4p/jtVFOj26xbgIUUS4pDKyHaG/eaygLTtFpFJqzWHc=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICSzCCAbQCCQDtQvkVxRvK9TANBgkqhkiG9w0BAQsFADBqMQswCQYDVQQGEwJV
UzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHU2VhdHRsZTEYMBYGA1UE
```

```
ChMPQW1hem9uLmNvbSBJbmMuMRowGAYDVQQDExFlYzIuYW1hem9uYXdzLmNvbTAe
Fw0xOTAyMDMwMzAwMDZaFw0yOTAyMDIwMzAwMDZaMGoxCzAJBgNVBAYTAlVTMRMw
EQYDVQQIEwpXYXNoaW5ndG9uMRAwDgYDVQQHEwdTZWF0dGxlMRgwFgYDVQQKEw9B
bWF6b24uY29tIEluYy4xGjAYBgNVBAMTEWVjMi5hbWF6b25hd3MuY29tMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1kkHXYTfc7gY5Q55JJhjTieHAgacaQkiR
Pity9QPDE3b+NXDh4UdP1xdIw73JcIIG3sG9RhWiXVCHh6KkuCTqJfPUknIKk8vs
M3RXflUpBe8Pf+P92pxqPMCz1Fr2NehS3JhhpkCZVGxxwLC5gaG0Lr4rFORubjYY
Rh84dK98VwIDAQABMA0GCSqGSIb3DQEBCwUAA4GBAA6xV9f0HMqXjPHuGILDyaNN
dKcvplNFwDTydVg32MNubAGnecoEBtUPtxBsLoVYXCOb+b5/ZMDubPF9tU/vSXuo
TpYM5Bq57gJzDRaBOntQbX9bgHiUxw6XZWaTS/6xjRJDT5p3S1E0mPI3lP/eJv4o
Ezk5zb3eIf10/sqt4756
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMoxixvs3YssMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA3MjAw
ODQ0NDRaGA8yMTk3MTIyMzA4NDQ0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA4T1PNsOg0FDrGlWePoHeOSmOJTA3HCRy5LSbYD33GFU2eBrOIxoU/+SM
rInKu3GghAMfH7WxPW3etIAZiyTDDU5RLcUq2Qwdr/ZpXAWpYocNc/CEmBFtfbxF
z4uwBIN3/drM0RSbe/wP9EcgmNUGQMMZWeAji8sMtwpOblNWAP9BniUG0Flcz6Dp
uPovwDTLdAYT3TyhzlohKL3f6O48TR5yTaV+3Ran2SGRhyJjfh3FRpP4VC+z5LnT
WPQHN74Kdq35UgrUxNhJraMGCzznolUuoR/tFMwR93401GsM9fVA7SW3jjCGF81z
PSzjy+ArKyQqIpLW1YGWDFk3sf08FQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDK
2/+C3nPMgtyOFX/I3Cyk+Pui44IgOwCsIdNGwuJysdqp5VIfnjegEu2zIMWJSKGO
lMZoQXjffkVZZ97J7RNDW06oB7kj3WVE8a7U4WEOfnO/CbMUf/x99CckNDwpjgW+
K8V8SzAsQDvYZs2KaE+18GFfLVF1TGUYK2rPSZMHyX+v/TIlc/qUceBycrIQ/kke
jDFsihUMLqgmOV2hXKUpIsmiWMGrFQV4AeV0iXP8L/ZhcepLf1t5SbsGdUA3AUY1
3If8s81uTheiQjwY5t9nM0SY/1Th/tL3+RaEI79VNEVfG1FQ8mgqCK0ar4m0oZJl
tmmEJM7xeURdpBBx36Di
-----END CERTIFICATE-----
```

Asien-Pazifik (Hyderabad) – ap-south-2

DSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIC8DCCArCgAwIBAgIGAXjrQ4+XMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAJCKGBBoxIUxqBk94JHhwZZbgvbP0DAOoHENQWxp/98lI7/
YOfYJOVMJS22aCnHDurofmo5rvNIkgXi7Rztbhu
+lko9rK6DgpmpUwBU0WZtf34aZ2IWNBwHaVhHvWAQf9/46u18dMa2YucK1Wi+Vc+M
+KldrvgXmhym6ErNlzhJyMAkGByqGSM44BAMDLwAwLAIUaaPKxaOHoYvwz709xXpsQueIq+UCFFa/
GpzoDOSokl1057NU/2hnsiW4
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjwLj9CMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+sFcobrjvcAYm0PNRD8f4R1jAzvoLt2+qGeOTAyO1Httj6cmsYN3AP1hN5iYuppFiYsl2eNPa/
CD0Vg0BAfDFlV5rzjpA0j7TJabVh4kj7JvtD+xYMi6wEQA4x6SPONY4OeZ2+8o/
HS8nucpWDVdPRO6ciWUlMhjmDmwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAAy6sgTdRkTqELHBeWj69q60xHyUmsWqHAQ
TGGbYP0yP2qfMl0cCImzRI5W0gn8gogdervfeT7nH5ih0TWEy/QDWfkQ601L4erm4yh4YQq8vcqAPSkf04N
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAIVWfPw/X82fMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MDQx
NDMwMjhaGA8yMjAxMTIwODE0MzAyOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAg29QEFriG+qFEjYW/v62nN70lMJY/Hevx5TtmU/VIYBPQa3HUGTBAbbI
2Tmy8UMpa8kZeaYeI3RAfiQWt0Ws7wUrBuO2Pdp518WDPaJUH7RWEuu1BDDkyZRW
NAMNPCn3ph7Od243IFcLGku7HVekel5poqRpSfojrMasjlf+CvixUeAJbmFoxUHK
kh5unzG2sZyO4wHXcJPQkRf5a8zSTPe9YZP1kXPPEv4p/jTSggaYPxXyS6QVaTlV
zLeLFZ0fesLPMeil3KYQtV7IKLQiEA2F6dxWnxNWQlyMHtdq6PucfEmVx17i/Xza
yNBRo0azY8WUNVkEXrRhp/pU8Nh3GQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU9AO1aZk9RLXk2ZvRVoUxYvQy9uwwgY4GA1UdIwSBhjCBg4AU9AO1
aZk9RLXk2ZvRVoUxYvQy9uyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAIVWfPw/X82fMBIGA1UdEwEB/wQIMAYBAf8C
```

```
AQAwDQYJKoZIhvcNAQELBQADggEBADexluMRQRftqViahCnauEWGdMvLCBr8A+Yr
6hJq0guoxEk/lahxR137DnfMPuSbi1Rx5QKo7oBrWfG/zsgQUnF2IwHTzwD+i/2m
XCane6FiS5RpK3lGdILq8ZmlhQk+6iI8yoZLr0LCfTh+CLgIKHOknfR5lFzgzAiF
SI8/Q9mm+uvYtSTZECI6Zh57QZPoETAG/yl+9jiOy2lAelqa/k1i+Qo8gMfOc+Pm
dwY7o6fV+oucgRlsdey6VM45LeyILQqv0RXtVzjuowanzmCCFMjgqiO9oZAWu4Oh
+F3unijELo01vZJs8s2N3KGlo3/jtUFTX6RTKShZlAPLwBi5GMI=
-----END CERTIFICATE-----
```

Asien-Pazifik (Jakarta) – ap-southeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXbVDEikMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAPjuiEx05N3JQ6cVwntJie67D8OuNo4jGRn
+crEtL7YO0jSVB9zGE1ga
+UgRPIaYETL293S8rTJTVgXAqdpBwfaHC6NUzre8U8iJ8FMNnlP9Gw1oUIlgQBjORyynVJexoB31TDZM
+/52g9O/bpq1QqNyKbeIgyBBlc1dAtr1QLnsMAkGByqGSM44BAMDLwAwLAIUK8E6RDIRtwK+9qnaTOBhvO/
njuQCFFocyT1OxK+UDR888oNsdgtif2Sf
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXbVDG2yMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
Vbt0gQ1ebWcur2hSO7PnJifE4OPxQ7RgSAlc4/spJp1sDP+ZrS0LO1ZJfKhXf1R9S3AUwLnsc7b
+IuVXdY5LK9RKqu64nyXP5dx170zoL8loEyCSuRR2fs+04i2QsWBVP+KFNAn7P5L1EHRjkgTO8kjNKviwRV
+OkP9ab5wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAI4WUy6+DKh0JDSzQEZNyBgNlSoSuC2owtMxCwGB6nBfzzfcekWvs
+87w/g9lNwUnUt0ZHYyh2tuBG6hVJuUEwDJ/z3wDd6wQviLOTF3MITawt9P8siR1hXqLJNxpjRQFZrgHqi
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMtdyRcH51j9MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
```

```
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MDgx
MjM5MTZaGA8yMjAxMDkxMjEyMzkxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvUsKCxoH6KXRYJLeYTWAQfaBQeCwhJaR56mfUeFHJE4g8aFjWkiN4uc1
TvOyYNnIZKTHWmzmulmdinWNbwP0GiROHb/i7ro0Hhvnptyyc Gt8ag8affiIbx5X
7ohdwSN2KJ6G0IKflIx7f2NEI0oAMM/9k+T1eVF+MVWzpZoiDp8frLNkqp8+RAgz
ScZsbRfwv3u/if5xJAvdg2nCkIWDMSHEVPoz0lJo7v0ZuDtWWsL1LHnL5ozvsKEk
+ZJyEi23r+U1hIT1NTBdp4yoigNQexedtwCSr7q36oOdDwvZpqYlkLi3uxZ4ta+a
01pzOSTwMLgQZSbKWQrpMvsIAPrxoQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU1GgnGdNpbnL3lLF30Jomg7Ji9hYwgY4GA1UdIwSBhjCBg4AU1Ggn
GdNpbnL3lLF30Jomg7Ji9hahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMtdyRcH51j9MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACVl00qQlatBKVeiWMrhpczsJroxDxlZTOba
6wTMZk7c3akb6XMOSZFbGaifkebPZqTHEhDlrClM2j9AIlYcCx6YCrTf4cuhn2mD
gcJN33143eOWSaeRY3ee4j+V9ne98y3kO2wLz95VrRgclPFR8po2iWGzGhwUi+FG
q8dXeCH3N0DZgQsSgQWwmdNQXZZej6RHLU/8In5trHKLY0ppnLBjn/UZQbeTyW5q
RJB3GaveXjfgFUWj2qOcDuRGaikdS+dYaLsi5z9cA3FolHzWxx9MOs8io8vKqQzV
XUrLTNWwuhZy88cOlqGPxnoRbw7TmifwPw/cunNrsjUUOgs6ZTk=
-----END CERTIFICATE-----
```

Asien-Pazifik (Sydney) – ap-southeast-5

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQC5X6U+vgoLEDAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDAxMDMxMjU3NTRaGA8y
MDUwMDEwMzEyNTc1NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtjCCASsGByqGSM44BAEwggEeAoGBAIzEMPCIPFfOYCg4
BCjKGyl60wOfmwHPzSOXZ3Z2wS/LYNHUtHGwtVNePSTyCu/CuZF6gC9n/wBORtQp
+SSkn+weGc/BmUA1mp/vrN7v+aSCgKJoO+sgpa1PPOgNvUaMw6O5odsZWQCMSjkU
6RTo/PL2v/tMfiCocF4ghvyRC6hvAhUA0VoObKC2IXzXgVvRRupo4qHbcm8CgYAe
bbNuawh3rAxkFvUs9FPzW5E+xllG16Z//61PENKqonmk+zBiBdiIlS1F6ZqmTqkI
z5+qfSt1m3pb3j2W0NT7lEDFvy8Gr6Y2vohCHmL+T1u1Yy4PeqbgrFwcen7y7WoO
/KCV7Y9/ODQMMyuAzT3h5wJNweT7L5MUN8JYpZSi3QOBhAACgYBqaDuG2u6V91Qj
K2wEAElxaaRaNo/ewg/wWDmHYqoeHOR0HfuFCYgASE9f7ULqYtX1VURcgcjw9XN4
BDmPilXvfi04INPTnw4IxFJKDzzC0kVH7esVas982Po8v3megH32H9Rl87r7UG1c
ZEbkSkKVX6YKYg1PR3rfjXgdwVZv/zAJBgcqhkjOOAQDAzAAMC0CFFWeRe2fYW2i
```

```
6mMd26Wzbx87Y0DXAhUAoPCnF+5hGJw0jT9aL7QsgcfLi9Y=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAMuBl6rhZCJKMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDAxMDMx
MjU3NTRaGA8yMjAzMDYwOTEyNTc1NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDFuKydxZsordNH7bLwIluEGOkX7/CdLdpeqkDKEhQkFwzpRxaX4EAlkGh2/o7D
8qneC9cGQhqSG5WVVBrmZG7sfkFOM4m1AtY++kfv+MYto1VFgLk1xJbkpq1r4YeQ
Ul+ZsJYsZpyX/t+g8s7rW0OVcBsYx4L75bf34z38mwK8PQIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBADD9C4pWL8RUvF1CJW8kExj35xmozlFlmrKs8Zpi8+Eg6q+W9dgd
xMdH95tgZtmVMDqlvVR+DK0iO1BNpqPjrqWkk2tTLivpS+sGzCE/jCl18Q28Rk71
/A3gLD7Rtbq5TKNvuFCHwYMjrTDHI6aBjIaAlDm4e2/j/OxVtHyZGTre
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANC3xtbPhQ2GMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDAxMDMx
MjU3NTRaGA8yMjAzMDYwOTEyNTc1NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAt3aMy7Hsp4ySG3mlfi+pdTcZw6H6XNU1Y36fNdi4c+MzinQQbnqMPyt7
QLgU+XCWmcWsVo7GQF6n9N01Rh+UXXUZU4jcXlFocQPCWf9O+IIIPXkd67kFMUV
HAxCELjfxHbC+I8e7dwOJhmdF4Bfi52Ty8zz0HdE8JDypPkTDlXuGvTgDyW7NP56
I/vlQaXLoYSbcQe5pv2a9gyBaaCM1QoeqwAHAeCNXb9Nuj9ZX3GHGJb3TuqAeKCD
5i9TscCB9XjY6Fx+zfSAobjBZwgLEtLOwJhbZnKmx4gJMaaNFipAjVT2FSS3+yev
eTYBoa1dvhk0ivQyQIPpHmihrmkWuwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBC
fdgyI8GjmCqiHAlh+L1bj0LdNql9zl7RXmOEzsuRdtdMumkxYXX88UtROy3fdi1i
VaEwHdAK8ThzRkesgHza/cXzqCMewaYxujSI6p6G7x99FFeGif1x0FJdj8AoeTL7
4h9bmS/6l4/NL7DJI9G7ovES/hoUA9v9TDhv+vauxXlgfrp0MPecprxBYlrc+DH2
adGCdKCp2lQ2YDKOD9TCEjYIli8XSoyevoWHUjfDYrCrCp8l4s/p7HOgYr8fJBAs
EuVy8211LVz1/X4EMBRNtNjXK9sklsxAOX14NDfBFSS0toxl3K6Tf9t/PviBl95d
hncyDAcFgDCK4w8LLlVW
-----END CERTIFICATE-----
```

Asien-Pazifik (Melbourne) ap-southeast-4

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjWF7P2MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAPRXSsQP9E3dw8QXKlrgBgEVCprLHdK/bbrMas0XMu1EhOD
+q
+0PcTr8+iwbtoXlY5MCeatWIp1GrXQjVqsF8vQqxlEuRuYKbR3nq4mWwaeGlx9AG5EjQHRa3GQ44wWHOdof0M3NRI1MP
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjSh40SMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+qWTGAbGsPeMX4hBMjAJUKys2NIRcRZaLM/BCew2FIPVjNtlaj6Gwn9ipU4Mlz3zIwAMWi1AvGMSreppt
+wV6MRtfOjh0Dvj/veJe88aEZJMozNgkJFRS
+WFWsckQeL56tf6kY6QTlNo8V/0CsQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAF7vpPghH0FRo5gu49EArRNPrIvW1egM
wcgkqIwwuXYj+1rhlL+/
iMpQWjdVGEqIZSeXn5fLmdx50eegFCwND837r9e8XYTiQS143Sxt9+Yi6BZ7U7YD8kK9NBWoJxFqUeHdpRCs0O7COjT3
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAN4GTQ64zVs8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTMx
MzMzMDBaGA8yMjAxMTIxNzEzMzMwMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA2BYgeCr+Rk/jIAEDOHS7wJql62vc83QEwjuzk0qOFEReIZzlN1fBRNXK
g0T178Kd3gLYcE59wEFbTe/X5yOA1Lo95x1anSAo7R+Cisf9C2HQuJp+gVb+zx71
lniPF7gHziGpm0M8DdAU/IW+wkZwGbP4z7Hq9+bJ0P2ltvPJ5yxSgkFuDsI9VBHa
CLoprHsCHh2VdP8KcMgQQMmHe1NmBpyTk0ul/aLmQkCQEX6ZIRGOeq228fwlh/t+
Ho+jv87duihVKic6MrL32SlD+maX0LSDUydWdaOLLTGkh7oV7+bFuH6msrXUu+Ur
```

```
ZEP1r/MidCWMhfgrFzeTBzOHA97qxQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUcHMd1cHqzmsQ5hpUK3EMLhHdsi4wgY4GA1UdIwSBhjCBg4AUcHMd
1cHqzmsQ5hpUK3EMLhHdsi6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAN4GTQ64zVs8MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAI4PFyVN+7EGSObioiPnv0LL0f70SSzUZJ8p
XO90d4rWea7jIbgZ2AKb+ErynkU9xVg7XQQ5k6KDWgp/4jYFL2dqnt/YAY4PS0un
RSrYElawxLT0BcLn4rcSDC79vQe1xGC5//wDdV6b399COAHRAK6axWYy5w32u9PL
uw0cIp3Ch8JoNwcgTHKRRGzePmBeR4PNqhHTArG4/dJk6/aUO4OpX0WzI6L67CGY
6Nex3dau+gkLCK93dTEkrXtyXHu4wB0J9zd1w+iQ0SEa9eKc78/NjEsF/FZdGrWC
t57lIMOOXJhQ1kRgSwNeZdQWV1dRakvO6sfcvVYkfj1wAvZvvAw=
-----END CERTIFICATE-----
```

Asien-Pazifik (Mumbai) – ap-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUDLA+x6tTAP3LRTr0z6nOxfsozdMwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
```

```
MB4XDTI0MDQyOTE0MTMwMVoXDTI5MDQyODE0MTMwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUDLA+x6tT
AP3LRTr0z6nOxfsozdMwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAZ7rYKoAwwiiH1M5GJbrT/BEk3OO2VrEPw8ZxgpqQ/EKlzMlOs/0Cyrmp7
UYyUgYFQe5nq37Z94rOUSeMgv/WRxaMwrLlLqD78cuF9DSkXaZIX/kECtVaUnjk8
BZx0QhoIHOpQocJUSlm/dLeMuE0+0A3HNR6JVktGsUdv9ulmKw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPRYyD8TtmC0MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjAzMDcx
MDQ1MDFaGA8yMTk1MDgxMTEwNDUwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA0LSS5I/eCT2PM0+qusorBx67QL26BIWQHd/yF6ARtHBb/1DdFLRqE5Dj
07Xw7eENC+T79mOxOAbeWg91KaODOzw6i9I/2/HpK0+NDEdD6sPKDA1d45jRra+v
CqAjI+nV9Vw91wv7HjMk3RcjWGziM8/hw+3YNIutt7aQzZRwIWlBpcqx3/AFd8Eu
2UsRMSHgkGUW6UzUF+h/U8218XfrauKNGmNKDYUhtmyBrHT+k6J0hQ4pN7fe6h+Z
w9RVHm24BGhlLxLHLmsOIxvbrF277uX9Dxu1HfKfu5D2kimTY7xSZDNLR2dt+kNY
/+iWdIeEFpPT0PLSILt52wP6stF+3QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBI
E6w+WWC2gCfoJO6c9HMyGLMFEpqZmz1n5IcQt1h9iyO7Vkm1wkJiZsMhXpk73zXf
TPxuXEacTX3SOEa07OIMCFwkusO5f6leOyFTynHCzBgZ3U0UkRVZA3WcpbNB6Dwy
h7ysVlqyT9WZd7EOYm5j5oue2G2xdei+6etgn5UjyWm6liZGrcOF6WPTdmzqa6WG
ApEqanpkQd/HM+hUYex/ZS6zEhd4CCDLgYkIjlrFbFb3pJ1OVLztIfSN5J4Oolpu
JVCfIq5u1NkpzL7ys/Ub8eYipbzI6P+yxXiUSuF0v9b98ymczMYjrSQXIf1e8In3
OP2CclCHoZ8XDQcvvKAh
-----END CERTIFICATE-----
```

Asien-Pazifik (Neuseeland) – ap-southeast-6

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQCcP+D4eLFOajAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEyMDMxMjEzMDZaGA8y
MDUwMTIwNDEyMTMwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtjCCASsGByqGSM44BAEwggEeAoGBANBMmM/LbAX13IeB
3yr2pMMpiTW1b1go/axNLfcxEmj0fThKk8y0FAT1frN/UPdI9qRInsyBdEZQLiIH
4WHCXk8IidQLh4DED3G9DvSFFC4Gb8ax+UIQY11wfHPWO4+wA9q8liYTg/FxdJMM
tZS9tZAZxjH6+8yfV8Bt0wUd2Y+lAhUAwg0CxCmZPinHtKbFnpMQfKnzjCMCgYAf
i+D7nGVFOWJ8EYOpRYbG0pHkrpwNy+h01csn6IAwQbIfeOG+SF4N3LeuOAC9vXGY
VGh9XNxuasvqkRAzgRmJ/EYM5Xa/YN62EhddRuN8wCOg66MeczUDh3RTb+Tu6HK0
UR6oTSOQ6rxA5aA1qTc7TqI0+pRZv+QYIZK/ozsZzgOBhAACgYAbVm+rOX8J38cG
LxKjUXVM0KB69SksGLEqjO4ps80EcZ/0W3g1hGLnSX/RjYfAS60hbKK1GX9PpcaO
4mDzCTm3dZ6shbae5t8bBU+mUi8BmaK+Pdu3z5J77y4zv22/yXte8ulZ5J0zKP9K
QP3p3pa7XI9NaXpKGT3yZsJ0BWY2xTAJBgcqhkjOOAQDAzAAMC0CFBs4KQmrxHjQ
OHh0r8JqB8UiwlutAhUAwgxid7wT6FNm8Zwq9hioQ2v2K0A=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAMwLuv2/tk9eMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEyMDMx
MjEzMDZaGA8yMjA0MDUwOTEyMTMwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQC9AsBNOUfT8QpguHqMa9KIXP/YgZOmfRAgEmnLawXTC+40bXUq/fwkx+cebv3x
CvUx6d07/iDlD0dm2Hf2HhPFi3OaCI7vc8c3lqVBvcn6yzmwv35aSEvtVm2NHC3j
4/q6vN2tR2d4a1Mf1QhmOVOJ7XiTEbCy2Yv+pmDbk29V6QIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAHatyQIy612kio8neI4r5VBg8pgKwW+mFGpAzOQ2NOyLCNoOeD1D
lPRaSipBN7WW6jpIozbz7JG7Kqc3N+piPGGzfjH9gZjqUqfOGrNHB5nsxvMHI2iL
e+DwsOcV7qnEVRgYbmLYOVKJv25wCsM/Tcn/6f6scEX2x+H0hAh7rwiP
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
```

```
MIIDOzCCAiOgAwIBAgIJAI/xUfWwSQOtMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEyMDMx
MjEzMDZaGA8yMjA0MDUwOTEyMTMwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArbid9Tnunu0pWCQUqZCkGeiF8hWixi+LBS1AOew2UsT9keAt2rXXGlU/
wSMriKHsvcrfKtuVKj5chArsOyFvagszH5lIKhI+GfWVQEd2aZiOvAJ+iRUQq1+R
gOr2gyjWlf3znZXTcyhHcJoXDhbn5e+kEa3pwS4yKNRpM3P61V4M2702xis08hjP
qMDxwXMa1Fiy4b7nAyNQifgrwb3bCA5k5prmkl/iajaWa1zMMFgLI9vA6UwUSbTK
H9iOuL/xNfMX+Xzq4CCaQYiJ8zdi56kqnB/lrA05NSjOPLskg6sUGkyiDxGK4gzC
DFrO6oygcdlBaxnyAECGdJcOM6TOmwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBg
8yVPNpctrvSvTazf/Ij8qC6+q6df1SptdYKQkOYWeUVZR7+3uTZ9Yiyq+Bh8Hbyf
NcR0eR6UqhgiB3p5slYNhTvLkpuMuqTpVJFvQtzZycnmKXAQ35G5zCYV0+pkF59L
ch26SukWk0+VP3kIM9VmaIZQKJEBlBLcnbDZyXlHUDnZAYPcxxKQ8uFPkW0GOFMr
ekFCGOUmFSItFXOHy5hD2xmctKNk3l12m6cKydYvONtk/3DovKNnw3c5k40WHQW/
Zdh/LWd4/Jrkan+kQnqm4rkrXF+x3aF0qrKTtHMICvpkZ8g7/588hBs4mZnCmFLa
q/g9WqIcd9SMmBkT6KZ8
-----END CERTIFICATE-----
```

Asien-Pazifik (Osaka) – ap-northeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUHTRhxHhBZFOGvTFKxHoy9+f5Hl8wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2NTQwN1oXDTI5MDQyODE2NTQwN1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUHTRhxHhB
ZFOGvTFKxHoy9+f5Hl8wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAUZx7DcYbhWNTD4BNGhr5beruT2OUoGHH9J73UKxwdqeb9bH1LIWhIZO0X
/1mjn3bWBgCwfoS8gjZwsVB6fZbNBRy8urdBZJ87xF/4JPBjt7S9oGx/zthDUYrC
yK0Y0v4G0PgiS81CvYLg09LpmYhLSJbXENlkC04v5yxdKxZxyg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMn1yPk22ditMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA3MTkx
MTEyNThaGA8yMTk2MTIyMjExMTI1OFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArznEYef8IjhrJoazI0QGZkmlmHm/4rEbyQbMNifxjsDE8YWtHNwaM91z
zmyK6Sk/tKlWxcnl3g31iq305ziyFPEewe5Qbwf1iz2cMsvfNBcTh/E6u+mBPH3J
gvGanqUJt6c4IbipdEouIjjnynyVWd4D6erLl/ENijeR1OxVpaqSW5SBK7jms49E
pw3wtbchEl3qsE42Ip4IYmWxqjgaxB7vps91n4kfyzAjUmklcqTfMfPCkzmJCRgp
Vh1C79vRQhmriVKD6BXwfZ8tG3a7mijeDn7kTsQzgO07Z2SAE63PIO48JK8HcObH
tXORUQ/XF1jzi/SIaUJZT7kq3kWl8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBj
ThtO9dLvU2QmKuXAhxXjsIdlQgGG3ZGh/Vke4If1ymgLx95v2Vj9Moxk+gJuUSRL
BzFte3TT6b3jPolbECgmAorjj8NxjC17N8QAAI1d0S0gI8kqkG7V8iRyPIFekv+M
pcai1+cIv5IV5qAz8QOMGYfGdYkcoBjsgiyvMJu/2N2UbZJNGWvcEGkdjGJUYYOO
NaspCAFm+6HA/K7BD9zXB1IKsprLgqhiIUgEaW3UFEbThJT+z8UfHG9fQjzzfN/J
nT6vuY/0RRu1xAZPyh2gr5okN/s6rnmh2zmBHU1n8cbCc64MVfXe2g3EZ9Glq/9n
izPrI09hMypJDP04ugQc
```

```
-----END CERTIFICATE-----
```

Asien-Pazifik (Seoul) – ap-northeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUbBSn2UIO6vYk4iNWV0RPxJJtHlgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEzMzg0NloXDTI5MDQyODEzMzg0NlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUbBSn2UIO
6vYk4iNWV0RPxJJtHlgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
```

```
AAOBgQAmjTjalG8MGLqWTC2uYqEM8nzI3px1eo0ArvFRsyqQ3fgmWcQpxExqUqRy
l3+2134Kv8dFab04Gut5wlfRtc2OwPKKicmv/IXGN+9bKFnQFjTqif08NIzrDZch
aFT/uvxrIiM+oN2YsHq66GUhO2+xVRXDXVxM/VObFgPERbJpyA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANuCgCcHtOJhMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTQx
NTU3NDRaGA8yMTk1MDIxNzE1NTc0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA66iNv6pJPmGM20W8HbVYJSlKcAg2vUGx8xeAbzZIQdpGfkabVcUHGB6m
Gy59VXDMDlrJckDDk6dxUOhmcX9z785TtVZURq1fua9QosdbTzX4kAgHGdp4xQEs
mO6QZqg5qKjBP6xr3+PshfQ1rB8Bmwg0gXEm22CC7o77+7N7Mu2sWzWbiUR7vil4
9FjWS8XmMNwFTlShp4l1TDTevDWW/uYmC30RThM9S4QPvTZ0rAS18hHVam8BCTxa
LHaVCH/Yy52rsz0hM/FlghnSnK105ZKj+b+KIp3adBL8OMCjgc/Pxi0+j3HQLdYE
32+FaXWU84D2iP2gDT28evnstzuYTQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQC1
mA4q+12pxy7By6g3nBk1s34PmWikNRJBwOqhF8ucGRv8aiNhRRye9lokcXomwo8r
KHbbqvtK85l0xUZp/Cx4sm4aTgcMvfJP29jGLclDzeqADIvkWEJ4+xncxSYVlS9x
+78TvF/+8h9U2LnSl64PXaKdxHy2IsHIVRN4GtoaP2Xhpa1S0M328Jykq/571nfN
1WRD1c/fQf1edgzRjhQ4whcAhv7WRRF+qTbfQJ/vDxy8lkiOsvU9XzUaZ0fZSfXX
wXxZamQbONvFcxVHY/0PSiM8nQoUmkkBQuKleDwRWvkoJKYKyr3jvXK7HIWtMrO4
jmXe0aMy3thyK6g5sJVg
-----END CERTIFICATE-----
```

Asien-Pazifik (Singapur) – ap-southeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
```

```
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUSqP6ih+++5KF07NXngrWf26mhSUwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE0MzAxNFoXDTI5MDQyODE0MzAxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUSqP6ih++
+5KF07NXngrWf26mhSUwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAw13BxW11U/JL58j//Fmk7qqtrZTqXmaz1qm2WlIpJpW750MOcP4ux1uPy
eM0RdVZ4jHSMv5gtLAv/PjExBfw9n6vNCk+5GZG4Xec5DoapBZHXmfMo93sjxBFP
4x9rWn0GuwAVO9ukjYPevq2RerilrqSVvppHtbATVNY2qecXDA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAJVMGw5SHkcvMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
ODU3MTlaGA8yMTk1MDQwMzA4NTcxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAlaSSLfBl7OgmikjLReHuNhVuvM20dCsVzptUyRbut+KmIEEc24wd/xVy
2RMIrydGedkW4tUjkUyOyfET5OAyT43jTzDPHZTkRSVkYjBdcYbe9o/0Q4P7IVS3
XlvwrUu0qo9nSID0mxMnOoF1l8KAqnn10tQ0W+lNSTkasW7QVzcb+3okPEVhPAOq
```

```
MnlY3vkMQGI8zX4iOKbEcSVIzf6wuIffXMGHVC/JjwihJ2USQ8fq6oy686g54P4w
ROg415kLYcodjqThmGJPNUpAZ7MOc5Z4pymFuCHgNAZNvjhZDA842Ojecqm62zcm
Tzh/pNMNeGCRYq2EQX0aQtYOIj7bOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU6SSB+3qALorPMVNjToM1Bj3oJMswgY4GA1UdIwSBhjCBg4AU6SSB
+3qALorPMVNjToM1Bj3oJMuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAJVMGw5SHkcvMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAF/0dWqkIEZKg5rca8o0P0VS+tolJJE/FRZO
atHOeaQbWzyac6NEwjYeeV2kY63skJ+QPuYbSuIBLM8p/uTRIvYM4LZYImLGUvoO
IdtJ8mAzq8CZ3ipdMs1hRqF5GRp8lg4w2QpX+PfhnW47iIOBiqSAUkIr3Y3BDaDn
EjeXF6qS4iPIvBaQQ0cvdddNh/pE33/ceghbkZNTYkrwMyBkQlRTTVKXFN7pCRUV
+L9FuQ9y8mP0BYZa5e1sdkwebydU+eqVzsil98ntkhpjvRkaJ5+Drs8TjGaJWlRw
5WuOr8unKj7YxdL1bv7//RtVYVVi296ldoRUYv4SCvJF11z0OdQ=
-----END CERTIFICATE-----
```

Asien-Pazifik (Sydney) – ap-southeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFxWyAdk4oiXIOC9PxcgjYYh71mwwDQYJKoZIhvcNAQEL
```

```
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MjE0M1oXDTI5MDQyODE1MjE0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFxWyAdk4
oiXIOC9PxcgjYYh71mwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQByjeQe6lr7fiIhoGdjBXYzDfkX0lGGvMIhRh57G1bbceQfaYdZd7Ptc0jl
bpycKGaTvhUdkpMOiV2Hi9dOOYawkdhyJDstmDNKu6P9+b6Kak8He5z3NU1tUR2Y
uTwcz7Ye8Nldx//ws3raErfTI7D6s9m63OX8cAJ/f8bNgikwpw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL2bOgb+dq9rMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAwNTdaGA8yMTk1MDQwMzA5MDA1N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAmRcyLWraysQS8yDC1b5Abs3TUaJabjqWu7d5gHik5Icd6dKl8EYpQSeS
vz6pLhkgO4xBbCRGlgE8LS/OijcZ5HwdrxBiKbicR1YvIPaIyEQQvF5sX6UWkGYw
Ma5IRGj4YbRmJkBybw+AAV9Icb5LJNOMWPi34OWM+2tMh+8L234v/JA6ogpdPuDr
sM6YFHMZ0NWo58MQ0FnEj2D7H58Ti//vFPl0TaaPWaAIRF85zBiJtKcFJ6vPidqK
f2/SDuAvZmyHC8ZBHg1moX9bR5FsU3QazfbW+c+JzAQWHj2AaQrGSCITxCMlS9sJ
l51DeoZBjnx8cnRe+HCaC4YoRBiqIQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU/wHIo+r5U31VIsPoWoRVsNXGxowwgY4GA1UdIwSBhjCBg4AU/wHI
o+r5U31VIsPoWoRVsNXGxoyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL2bOgb+dq9rMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACobLvj8IxlQyORTz/9q7/VJL509/p4HAeve
92riHp6+Moi0/dSEYPeFTgdWB9W3YCNc34Ss9TJq2D7t/zLGGlbI4wYXU6VJjL0S
hCjWeIyBXUZOZKFCb0DSJeUElsTRSXSFuVrZ9EAwjLvHni3BaC9Ve34iP71ifr75
8Tpk6PEj0+JwiijFH8E4GhcV5chB0/iooU6ioQqJrMwFYnwo1cVZJD5v6D0mu9bS
TMIJLJKv4QQQqPsNdjiB7G9bfkB6trP8fUVYLHLsVlIy5lGx+tgwFEYkG1N8IOO/
2LCawwaWm8FYAFd3IZl04RImNs/IMG7VmH1bf4swHOBHgCN1uYo=
```

```
-----END CERTIFICATE-----
```

Asien-Pazifik (Taipeh) – ap-east-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7jCCAq4CCQDrb+HArMxssTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA1MjQxNDU2MDZaGA8y
MDUwMDUyNTE0NTYwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtjCCASsGByqGSM44BAEwggEeAoGBAPFb5R5TBUs2N0YW
aJcOjxr4UCDrpVT3x6EeqoGFNAc1yiZw9iv++ff6wsXm0VG5XV1QkWMQcjPfK/2I
TvXh9XEOhsG7vaBHoWkb2gmIxE6C2u8TfoZu0ZmiMceFK7aYz5w/q2J9CmRs38dT
I9qgTq0LYX+VkiNYOQnn7sQXQ8CjAhUAp2Lue9SfYTmubbpH+3j91Sivc+cCgYAi
DiyGU5R5VgiNV3mhuAyiHCft3LEmTIxos/hx/rHzgm+vCMH55tYejIrv9n7YGrIZ
MejOt8bGYxqSf0Ir/aoj3ZfHihxUzwyfyzwH7D8kAodXJNsPUTKi0O0pGl/e+nVD
JhTIFV3AwC8Tt0r2hljbjhOiyhdYy5hxWHa/WokLAQOBhAACgYAkGGHXbFr/JXol
itpS1qfiETWSRkXGHrdSmUkRumgti2y7c57TgXPwCyNlP1sTr1duy/kYDpwSwyqi
qEYfko0b/xWpDEQQPsWBgolpEYP7RIT85IxrTCrC9ohz85n7v6m9oF6BiBQGtZdk
GBN7iqemg85UaF6mXfHvl3tUYjsB2jAJBgcqhkjOOAQDAy8AMCwCFED9Ybn6fEVF
wLNjDvULmki5bPBWAhR64pxsHFRHz0ZQi+SYMWdIpEs5RQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAJp99iy2CTXhMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA1MjQx
NDU2MDZaGA8yMjAzMTAyOTE0NTYwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDVdclgpcIIsyGG51ag8srK1UMfZ+Ioh9E4PLP+cIWQcdh31fv2kV/whKaqfmif
NefBIuHrTPl6L+mJQbsfeA+TiEx1Jamg4lwQfhgQKQCmjZVMaHtK+AY57TVN6FBf
HXxT2MXzktsKxAQRGeSTFQYrHRzSYvu+GkA+37lqyWRfcwIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBABM+WL9MSb7z3bNOTMkM7ufPucvj+LQ+zEAJiuG0rcB8GI2DhGB5
8ohDPUGlq1cP7vYmDkWG/FrLqx7qgIzkbE3zfb62JpdOuX73oHgCmikMfq8ifoS1
CUxMQ36PDZBFNPzGZxv5kEORqhmGBkYCoIUCQ43jh3aALR/A/rfzfij8
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAJt5hgMuWbpMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA1MjQx
NDU2MDZaGA8yMjAzMTAyOTE0NTYwNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA91FXs9Wk9kMI3lkNhjC69C6RTBpSvdLWSohPDlJKXFoaGYIDtyW1ViwO
FORAKz0koarVBx1D4fNKCxf+mhYAf//4Pxt31GzjehHNs2YVGimwhq/SNr+3AuIO
PibA+qScXamaiknE1Pxb4jisbBu2PMAG9OxU2dESNwiqBMvdJvg30YNTUITZ6r0e
MPjR1Y/EFVx/SLHW6wdvwqhNi9hz8HHdThzjCbCQPvmoLBJIKXIfosKqvauSezt1
KJSoS2jMx1OjJB2bBlQTZC8vF0WFNPoiH4jXyJ6+wMUMNSSd5b3uL5stVTMzuIz4
39Hd5YW41rmAy+6jmpGp2eXn6Td0rQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAs
gcgv+Xr67Cj08jKdAUT4GuCoGxveOFAjSDjs5y0cD+kXIT/Yj/+HKFOx5cwThT8F
TxNQ/oVuo3bGeuFEX799H0rT9Jupy0WiE1Vx81mk2M/1EDtns437edM4ofiWR8tR
Q1VNiRgz6Crr0nFgNoQa9HmR6/M+bImxevHJkWB3skvnxtA+lpKGwJs8jo6fA7AW
jr00opK0r731iBd1z/5hjIjkHn5NizAdiJEh3lVY/A3WS82aygW8LvYnKZeaBfZJ
J4NgxeflxocLFKBJD+hyf5u1hhvl7Mn/aGr5VI8/0F2oUqYo+xsHLT3keNghywO4
NNcyLcD9u16HVXhRhGvo
-----END CERTIFICATE-----
```

Asien-Pazifik (Thailand) – ap-southeast-7

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8TCCAq8CCQCOEEMWiJIJpTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA0MTIxNTI4NTZaGA8y
MDUwMDQxMzE1Mjg1NlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtzCCASsGByqGSM44BAEwggEeAoGBAJWKfrIlz9+/U4wm
NDJPX00avUTdksBKX5RwHkY4o0///2G2HWwiBbxw8F1U+RzCXr80gSoe4+/SCSg3
uDuhJyzN5r4jr7c590CAgsiGdWERs7l4gLQCP504feU4TEjJoq9A8MfRZeqMj7Ug
fT5InTUW7S1/r98ddG/rBHMsJwEbAhUAneIckZ1YeyGcCeL32lujMhj+g68CgYA+
RsyTXCy3Tug5aHun51IfcG2d+pn5K/tv/N3WUR18RplVctrLhwIOUoAsDWPWtxNV
sODetezAyo759CK43JAmYGzXKbRFUHm3n46jP88tSdhuSeJhc/D4l5/0+2L7ndXp
L3+W4N05NdiKSGI8e8t452wTZv/RODivPZ3RtuCDywOBhQACgYEAjVS1Huwzdn1J
+kpd2Rcbe1BAGkmvk5sUu0KhyttqIB1kxTxeWZgsdO8REZSC5gJOwkcGFvXnb3DY
+Ms45r0e0s0rx2FFYjqMLwyRpK9wUjJfSXeJMa9iLQEXuyzBz6zPgfemXbS3zNq/
```

```
eoJ9ztIwjB9DMoKL+E1vSLsTGhehqRowCQYHKoZIzjgEAwMxADAuAhUAmljDM3c9
hf0j4XbMjjpnzrx1xhkCFQCASR9pgFNgLK8y6Kojj+P1KJkrSQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAIuIHAhL0xWcMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA0MTIx
NTI4NTZaGA8yMjAzMDkxNzE1Mjg1NlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCajgAeOauwvqGDLrHvxujnZ1BnkMzwjrycMUTkj8jqNtWoDQWUJVNPZJILosEU
VwK2I3oNkEsx/ryl9XfXcNNceoYfVEPzkTzozrZyuOG66FWtUU1LKeJ7h9/rX0Zd
9lZEokrdr6dLPt9FsHWaK5ExlUnWBjNltcQLkkKqoeYaFwIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAE4G5G+FvKTsX3T7BEcId7f5LSCc2J9gZRDiWn2oTr40CrBMOzJT
KsWr9W89YXW3gaGWltzc0WCwYQbJZgAkuEAZItJjbhdnns87ZbsFO+NZhc6gDtjA
WC3dPlSB9b6rfVoVW9O6Xwa7iNXZo8ddYVJ/ZOIv/totUz9qJt4DmmKk
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANaQIrYcijxaMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDA0MTIx
NTI4NTZaGA8yMjAzMDkxNzE1Mjg1NlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAxtMGK4r6WerVtMfpRRCY3DMP9Q/s4jnRIqolPaxeT99BAFp03HXyOrTz
WjggEHArRGGeDowFkL7Vj+QNY7ran2lnYVlAQ7Ow6OLl6WttT6lMsgsLUIcsED6G
eJ1Ko+ovT1qvmuush1U5R2pHkcCJ1IT2s6uQff85l066K7dCFpaoA1QHUk9zACHj
i0DtWuTAWBXirAZSGlmtP6uj1Aw6y5kACDTjIvZJeW/kmswfApTKaJ56eNkJsUBU
NpKwt3um1BMZduy0cjUv0Sc3dIbLNyfOdyPn8tX5u5ck0EPdtBB5WjEh71IXdZJD
oaBREV7AHg5ERPQsm0BqSvMQt09KiwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDG
qJyZbv/GUQnm8dEyVYgilQr3Yu35n8sfTwwZ1OJzIVce7NBPWePMfYii/tvGoKNp
KwFa/Vugbn1EwqpTEKqkPE1dOZvnUa97XxhYkoW5U7sgdKCANi1KWjywn7MiJ3Eg
j4gdqYK8wxvHi21ppqr572UO77uA8YMBoBT/CyQzWYUSmbqwKnnzaQBAZeO2iAk
VHuNU+9UsntNB676gRl9ag3Wfxq3yx5Ee1CeQf+US3HJn/pKk1H8dExXmBHvHwO6
GKUVNPN1rxfjTiaSt8wuO80uElAnyHIM3VOR8rJO7PKsobyEeJV0WI1hURO+wxpL
h3IsW7iBrFVvhX5xx7ZU
-----END CERTIFICATE-----
```

Asien-Pazifik (Tokio) – ap-northeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULgwDh7TiDrPPBJwscqDwiBHkEFQwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEyMjMxMFoXDTI5MDQyODEyMjMxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIEExMQ4IULgwDh7Ti
DrPPBJwscqDwiBHkEFQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBtjAglBde1t4F9EHCZOj4qnY6Gigy07Ou54i+lR77MhbpzE8V28Li9l+YT
QMIn6SzJqU3/fIycIro1OVY1lHmaKYgPGSEZxBenSBHfzwDLRmC9oRp4QMe0BjOC
gepj1lUoiN7OA6PtA+ycNlsP0oJvdBjhvayLiuM3tUfLTrgHbw==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL9KIB7Fgvg/MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAwMjVaGA8yMTk1MDExNzA5MDAyNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAz0djWUcmRW85C5CiCKPFiTIvj6y2OuopFxNE5d3Wtab10bm06vnXVKXu
tz3AndG+Dg0zIL0gMlU+QmrSR0PH2PfV9iejfLak9iwdm1WbwRrCEAj5VxPe0Q+I
KeznOtxzqQ5Wo5NLE9bA61sziUAFNVsTFUzphEwRohcekYyd3bBC4v/RuAjCXHVx
40z6AIksnAOGN2VABMlTeMNvPItKOCIeRLlllSqXX1gbtL1gxSW40JWdF3WPB68E
e+/1U3F7OEr7XqmNODOL6yh92QqZ8fHjG+afOL9Y2Hc4g+P1nk4w4iohQOPABqzb
MPjK7B2Rze0f9OEc51GBQu13kxkWWQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU5DS5IFdU/QwYbikgtWvkU3fDwRgwgY4GA1UdIwSBhjCBg4AU5DS5
IFdU/QwYbikgtWvkU3fDwRihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL9KIB7Fgvg/MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAG/N7ua8IE9IMyno0n5T57erBvLTOQ79fIJN
Mf+mKRM7qRRsdg/eumFft0rLOKo54pJ+Kim2cngCWNhkzctRHBV567AJNt4+ZDG5
hDgV0IxWO1+eaLE4qzqWP/9VrO+p3reuumgFZLVpvVpwXBBeBFUf2drUR14aWfI2
L/6VGINXYs7uP8v/2VBS7r6XZRnPBUy/R4hv5efYXnjwA9gq8+a3stC2ur8m5ySl
faKSwE4H320yAyaZWH4gpwUdbUlYgPHtm/ohRtiWPrN7KEG5Wq/REzMIjZCnxOfS
6KR6PNjlhxBsImQhmBvz6j5PLQxOxBZIpDoiK278e/1Wqm9LrBc=
-----END CERTIFICATE-----
```

Kanada (Zentral) – ca-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUIrLgixJJB5C4G8z6pZ5rB0JU2aQwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MzU0M1oXDTI5MDQyODE1MzU0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUIrLgixJJ
B5C4G8z6pZ5rB0JU2aQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBHiQJmzyFAaSYs8SpiRijIDZW2RIo7qBKb/pI3rqK6yOWDlPuMr6yNI81D
IrKGGftg4Z+2KETYU4x76HSf0s//vfH3QA57qFaAwddhKYy4BhteFQl/Wex3xTlX
LiwI07kwJvJy3mS6UfQ4HcvZy219tY+0iyOWrz/jVxwq7TOkCw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAJNKhJhaJOuMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA3Mjkx
MTM3MTdaGA8yMTk2MDEwMjExMzcxN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAhDUh6j1ACSt057nSxAcwMaGr8Ez87VA2RW2HyY8l9XoHndnxmP50Cqld
+26AJtltlqHpI1YdtnZ6OrVgVhXcVtbvte0lZ3ldEzC3PMvmISBhHs6A3SWHA9ln
```

```
InHbToLX/SWqBHLOX78HkPRaG2k0COHpRy+fG9gvz8HCiQaXCbWNFDHZev9OToNI
xhXBVzIa3AgUnGMalCYZuh5AfVRCEeALG60kxMMC8IoAN7+HG+pMdqAhJxGUcMO0
LBvmTGGeWhi04MUZWfOkwn9JjQZuyLg6B1OD4Y6s0LB2P1MovmSJKGY4JcF8Qu3z
xxUbl7Bh9pvzFR5gJN1pjM2n3gJEPwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAJ
UNKM+gIIHNk0G0tzv6vZBT+o/vt+tIp8lEoZwaPQh1121iw/I7ZvhMLAigx7eyvf
IxUt9/nf8pxWaeGzi98RbSmbap+uxYRynqe1p5rifTamOsguuPrhVpl12OgRWLcT
rjg/K60UMXRsmg2w/cxV45pUBcyVb5h6Op5uEVAVq+CVns13ExiQL6kk3guG4+Yq
LvP1p4DZfeC33a2Rfre2IHLsJH5D4SdWcYqBsfTpf3FQThH0l0KoacGrXtsedsxs
9aRd7OzuSEJ+mBxmzxSjSwM84Ooh78DjkdpQgv967p3d+8NiSLt3/n7MgnUy6WwB
KtDujDnB+ttEHwRRngX7
-----END CERTIFICATE-----
```

Kanada West (Calgary) – ca-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAYPouptUMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAMITzTJUa6cBsIfdHN69zW/
aHjUB4r1ZfKb1FMhIp9EZtEf5n+06oXjUG2+dKRSlFQeEK333ehNZsPd6uqey6TYKtHpFb5XRLS8BpqB
+7gnbAd0CBZM5o4NWesSQ1GLnTdQcGZkYG/
QESkbadoCXQTifCujJE682hTDLIVt1d4ewwCQYHKoZIzjgEAwMvADAsAhRJc4gRS/HWTkCR2MESaQEe/
jOMNQIUNoTwLvuPrmGPupPlGiHe0veZiO8=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAYPou9weMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
v4XBVH13ZCMgqlRHMqV8AWI5iO6gFn2A9sN3AZXTMqwtZeiDdebq3k6Wt7ieYvpXTg0qvgsjQIovRZWaBDBJy9x8C2hW
+w9lMQjFHkJ7Jy/
PHCJ69EzebQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAGe9Snkz1A6rHBH6/5kDtYvtPYwhx2sXNxztbhkXErFk40Nw5l4
gvDVtWG7qyb6fAqgoisyAbk8K9LzxSim2S1nmT9vD84B/t/VvwQBylc
+ej8kRxMH7fquZLp7IXfmtBzyUqu6Dpbne+chG2
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALyTn5IHrIZjMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMzEyMDcx
NTM3MDFaGA8yMjAzMDUxMzE1MzcwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA1GP5os424BJmGPCKOSgOclP7lzUiB85du03M4hfjzSOszsBpmBGFDLz1
owYHtIxlq3+Vi1Lt5Qlx3id/ov1QyaBPFWXVeklHVXy9vieCcI3TdjGjTl1W/8MM
m3X26QPcsnHM/Kk2wJ7s186MrqmdSsp3SCPpxv4vEG2Q9yR2bXY41hpc2rWlW8qU
D0JGXluvmmAdFnto20l1XWZ6xFen1h60DRugek/ufCbN+ljKy0xLqPoavH0Ybjsb
UpsAsBs7phaoN+X/5hIERfbp5LfVnqq54pNG5KNu4KynfW9+kA/WS4cJ6FTTN5t+
y0P1HvcL+BL2RuDy6T2bB21xw5WqtQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQURTvu/Dd4zDnmS5G5CfVLnmUBNOswgY4GA1UdIwSBhjCBg4AURTvu
/Dd4zDnmS5G5CfVLnmUBNOuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALyTn5IHrIZjMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFt523A3Aug6/F8xxyITgA8gkU0btFhlXNSP
U4U2OQ9n0tWI9WqnKNWH3KBxwY5EPitU6b3LM4xc9lDWpz7h2Pto+WhxP9LVKe6f
r8r7teTLCVZ7cfYZHzHg+flZjVpAgzE5BVfrRlj3QKpv0hYT3J1wMtI++Vorq5Nf
aPjzedehJLhmZVALwnfqfLrgv6/gmraP9Vmoa8U4D6AljNiQGYaLwyoPoRm3bUs2
v1Mh9GkEQ1b9+1pFXcqgzJJTGRuiPCyPbECI79FAnx5JM/CkGJV8HlOmjIW1qkK1
Y2qT7wzErrKLJyB53Pw15BdIM1onbDAQreZb0yZQLdoEl/tx7Uk=
-----END CERTIFICATE-----
```

China (Peking) – cn-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
```

```
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAOtrM5XLDSjCMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQx
MDAxNDJaGA8yMTk1MDExNzEwMDE0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvVBz+WQNdPiM9S+aUULOQEriTmNDUrjLWLr7SfaOJScBzis5D5ju0jh1
+qJdkbuGKtFX5OTWTm8pWhInX+hIOoS3exC4BaANoa1A3o6quoG+Rsv72qQf8LLH
```

```
sgEi6+LMlCN9TwnRKOToEabmDKorss4zFl7VSsbQJwcBSfOcIwbdRRaW9Ab6uJHu
79L+mBR3Ea+G7vSDrVIA8goAPkae6jY9WGw9KxsOrcvNdQoEkqRVtHo4bs9fMRHU
Etphj2gh4ObXlFN92VtvzD6QBs3CcoFWgyWGvzg+dNG5VCbsiiuRdmii3kcijZ3H
Nv1wCcZoEAqH72etVhsuvNRC/xAP8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA8
ezx5LRjzUU9EYWYhyYIEShFlP1qDHs7F4L46/5lc4pL8FPoQm5CZuAF31DJhYi/b
fcV7i3n++/ymQbCLC6kAg8DUB7NrcROll5ag8d/JXGzcTCnlDXLXx1905fPNa+jI
0q5quTmdmiSi0taeaKZmyUdhrB+a7ohWdSdlokEIOtbH1P+g5yll3bI2leYE6Tm8
LKbyfK/532xJPqO9abx4Ddn89ZEC6vvWVNDgTsxERg992Wi+/xoSw3XxkgAryIv1
zQ4dQ6irFmXwCWJqc6kHg/M5W+z60S/94+wGTXmp+19U6Rkq5jVMLh16XJXrXwHe
4KcgIS/aQGVgjM6wivVA
-----END CERTIFICATE-----
```

China (Ningxia) – cn-northwest-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
```

```
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPu4ssY3BlzcMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEyMDMy
MTI5MzJaGA8yMTk1MDUwODIxMjkzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAsOiGi4A6+YTLzCdIyP8b8SCT2M/6PGKwzKJ5XbSBoL3gsnSWiFYqPg9c
uJPNbiy9wSA9vlyfWMd90qvTfiNrT6vewP813QdJ3EENZOx4ERcf/Wd22tV72kxD
yw1Q3I1OMH4bOItGQAxU5OtXCjBZEEUZooOkU8RoUQOU2Pql4NTiUpzWacNutAn5
HHS7MDc4lUlsJqbN+5QW6fFrcNG/0Mrib3JbwdFUNhrQ5j+Yq5h78HarnUivnX/3
Ap+oPbentv1qd7wvPJu556LZuhfqI0TohiIT1Ah+yUdN5osoaMxTHKKtf/CsSJ1F
w3qXqFJQA0VWsqjFyHXFI32I/GOupwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCn
Um00QHvUsJSN6KATbghowLynHn3wZSQsuS8E0COpcFJFxP2SV0NYkERbXu0n/Vhi
yq5F8v4/bRA2/xpedLWmvFs7QWlomuXhSnYFkd33Z5gnXPb9vRkLwiMSw4uXls35
qQraczUJ9EXDhrv7VmngIk9H3YsxYrlDGEqh/oz4Ze4ULOgnfkauanHikk+BUEsg
/jsTD+7e+niEzJPihHdsvKFDlud5pakEzyxovHwNJ1GS2I//yxrJFIL91mehjqEk
RLPdNse7N6UvSnuXcOokwu6l6kfzigGkJBxkcq4gre3szZFdCQcUioj7Z4xtuTL8
YMqfiDtN5cbD8R8ojw9Y
-----END CERTIFICATE-----
```

Europa (Frankfurt) – eu-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFD5GsmkxRuecttwsCG763m3u63UwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1NTUyOVoXDTI5MDQyODE1NTUyOVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFD5Gsmkx
RuecttwsCG763m3u63UwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBBh0WaXlBsW56Hqk588MmJxsOrvcKfDjF57RgEDgnGnQaJcStCVWDO9UYO
JX2tdsPw+E7AjDqjsuxYaotLn3Mr3mK0sNOXq9BljBnWD4pARg89KZnZI8FN35HQ
O/LYOVHCknuPL123VmVRNs51qQA9hkPjvw21UzpDLxaUxt9Z/w==
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAKD+v6LeR/WrMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTA4MTlaGA8yMTk1MDExNzA5MDgxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAka8FLhxs1cSJGK+Q+q/vTf8zVnDAPZ3U6oqppOW/cupCtpwMAQcky8DY
Yb62GF7+C6usniaq/9W6xPn/3o//wti0cNt6MLsiUeHqNl5H/4U/Q/fR+GA8pJ+L
npqZDG2tFi1WMvvGhGgIbScrjR4VO3TuKy+rZXMYvMRk1RXZ9gPhk6evFnviwHsE
jV5AEjxLz3duD+u/SjPp1vloxe2KuWnyC+EKInnka909sl4ZAUh+qIYfZK85DAjm
GJP4W036E9wTJQF2hZJrzsiB1MGyC1WI9veRISd30izZZL6VVXLXUtHwVHnVASrS
zZDVpzj+3yD5hRXsvFigGhY0FCVFnwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUxC2l6pvJaRflgu3MUdN6zTuP6YcwgY4GA1UdIwSBhjCBg4AUxC2l
6pvJaRflgu3MUdN6zTuP6YehYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAKD+v6LeR/WrMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAIK+DtbUPppJXFqQMv1f2Gky5/82ZwgbbfXa
HBeGSii55b3tsyC3ZW5ZlMJ7Dtnr3vUkiWbV1EUaZGOUlndUFtXUMABCb/coDndw
CAr53XTv7UwGVNe/AFO/6pQDdPxXn3xBhF0mTKPrOGdvYmjZUtQMSVb9lbMWCFfs
w+SwDLnm5NF4yZchIcTs2fdpoyZpOHDXy0xgxO1gWhKTnYbaZOxkJvEvcckxVAwJ
obF8NyJla0/pWdjhlHafEXEN8lyxyTTyOa0BGTuYOBD2cTYYynauVKY4fqHUkr3v
Z6fboaHEd4RFamShM8uvSu6eEFD+qRmvqlcodbpsSOhuGNLzhOQ=
-----END CERTIFICATE-----
```

Europa (Irland) – eu-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
```

```
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUakDaQ1Zqy87Hy9ESXA1pFC116HkwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MTgxMFoXDTI5MDQyODE2MTgxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUakDaQ1Zq
y87Hy9ESXA1pFC116HkwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQADIkn/MqaLGPuK5+prZZ5Ox4bBZLPtreO2C7r0pqU2kPM2lVPyYYydkvP0
lgSmmsErGu/oL9JNztDe2oCA+kNy17ehcsf8cw0uP861czNFKCeU8b7FgBbL+sIm
qi33rAq6owWGi/5uEcfCR+JP7W+oSYVir5r/yDmWzx+BVH5S/g==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOrmqHuaUt0vMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTA2MTlaGA8yMTk1MDQwMzA5MDYxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjE7nVu+aHLtzp9FYV25Qs1mvJ1JXD7J0iQ1Gs/RirW9a5ZECCtc4ssnf
zQHq2JRVr0GRchvDrbm1HaP/avtFQR/Thvfltwu9AROVT22dUOTvERdkNzveoFCy
```

```
hf52Rqf0DMrLXG8ZmQPPXPDFAv+sVMWCDftcChxRYZ6mP9O+TpgYNT1krD5PdvJU
7HcXrkNHDYqbsg8A+Mu2hzl0QkvUET83Csg1ibeK54HP9w+FsD6F5W+6ZSHGJ88l
FI+qYKs7xsjJQYgXWfEt6bbckWs1kZIaIOyMzYdPF6ClYzEec/UhIe/uJyUUNfpT
VIsI5OltBbcPF4c7Y20jOIwwI2SgOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUF2DgPUZivKQR/Zl8mB/MxIkjZDUwgY4GA1UdIwSBhjCBg4AUF2Dg
PUZivKQR/Zl8mB/MxIkjZDWhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOrmqHuaUt0vMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGm6+57W5brzJ3+T8/XsIdLTuiBSe5ALgSqI
qnO5usUKAeQsa+kZIJPyEri5i8LEodh46DAF1RlXTMYgXXxl0YggX88XPmPtok17
l4hib/D9/lu4IaFIyLzYNSzsETYWKWoGVe7ZFz60MTRTwY2u8YgJ5dec7gQgPSGj
avB0vTIgoW41G58sfw5b+wjXCsh0nROon79RcQFFhGnvup0MZ+JbljyhZUYFzCli
31jPZiKzqWa87xh2DbAyvj2KZrZtTe2LQ48Z4G8wWytJzxEeZdREe4NoETf+Mu5G
4CqoaPR05KWkdNUdGNwXewydb3+agdCgfTs+uAjeXKNdSpbhMYg=
-----END CERTIFICATE-----
```

Europa (London) – eu-west-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIDITCCAoqgAwIBAgIUCgCV/DPxYNND/swDgEKGiC5I+EwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MjkxNFoXDTI5MDQyODE2MjkxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUCgCV/DPx
YNND/swDgEKGiC5I+EwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQATPu/sOE2esNa4+XPEGKlEJSgqzyBSQLQc+VWo6FAJhGG9fp7D97jhHeLC
5vwfmtTAfnGBxadfAOT3ASkxnOZhXtnRna460LtnNHm7ArCVgXKJo7uBn6ViXtFh
uEEw4y6p9YaLQna+VC8Xtgw6WKq2JXuKzuhuNKSFaGGw9vRcHg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANBx0E2bOCEPMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA4MTEx
NDU2NDJaGA8yMTk2MDExNTE0NTY0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArYS3mJLGaMrh2DmiPLbqr4Z+xWXTzBWCjOwpsuHE9H6dWUUyl2Bgnu+Z
d8QvW306Yleec45M4F2RA3J4hWHtShzsMlOJVRt+YulGeTf9OCPr26QmIFfs5nD4
fgsJQEry2MBSGA9Fxq3Cw6qkWcrOPsCR+bHOU0XykdKl0MnIbpBf0kTfciAupQEA
dEHnM2J1L2iI0NTLBgKxy5PXLH9weX20BFauNmHH9/J07OpwL20SN5f8TxcM9+pj
Lbk8h1V4KdIwVQpdWkbDL9BCGlYjyadQJxSxz1J343NzrnDM0M4h4HtVaKOS7bQo
Bqt2ruopLRCYgcuFHck/1348iAmbRQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBG
wujwU1Otpi3iBgmhjMClgZyMMn0aQIxMigoFNqXMUNx1Mq/e/Tx+SNaOEAu0n2FF
aiYjvY0/hXOx75ewzZvM7/zJWIdLdsgewpUqOBH4DXFhbSk2TxggSPb0WRqTBxq5
Ed7F7+7GRIeBbRzdLqmISDnfqey8ufW0ks51XcQNomDIRG5s9XZ5KHviDCar8FgL
HngBCdFI04CMagM+pwTO9XN1Ivt+NzUj208ca3oP1IwEAd5KhIhPLcihBQA5/Lpi
h1s3170z1JQ1HZbDrH1pgp+8hSI0DwwDVb3IIH8kPR/J0Qn+hvOl2HOpaUg2Ly0E
pt1RCZe+W7/dF4zsbqwK
-----END CERTIFICATE-----
```

Europa (Mailand) – eu-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAqwCCQCMElHPdwG37jAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA0MjkyMDM1MjJaFw00
NTA0MjkyMDM1MjJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQDAkoL4YfdMI/MrQ0oL
NPfeEk94eiCQA5xNOnU7+2eVQtEqjFbDADFENh1p3sh9Q9OoheLFH8qpSfNDWn/0
ktCS909ApTY6Esx1ExjGSeQq/U+SC2JSuuTT4WFMKJ63a/czMtFkEPPnVIjJJJmT
HJSKSsVUgpdDIRvJXuyB0zdB+wIVALQ3OLaVGdlPMNfS1nD/Yyn+32wnAoGAPBQ3
7XHg5NLOS4326eFRUT+4ornQFjJjP6dp3pOBEzpImNmZTtkCNNUKE4Go9hv5T4lh
R0pODvWv0CBupMAZVBP9ObplXPCyEIZtuDqVa7ukPOUpQNgQhLLAqkigTyXVOSmt
ECBj9tu5WNP/x3iTZTHJ+g0rhIqpgh012UwJpKADgYQAAoGAV1OEQPYQUg5/M3xf
6vE7jKTxxyFWEyjKfJK7PZCzOIGrE/swgACy4PYQW+AwcUweSlK/Hx2OaZVUKzWo
wDUbeu65DcRdw2rSwCbBTU342sitFo/iGCV/Gjf+BaiAJtxniZze7J1ob8vOBeLv
uaMQmgOYeZ5e0fl04GtqPl+lhcQwCQYHKoZIzjgEAwMwADAtAhQdoeWLrkm0K49+
AeBK+j6m2h9SKQIVAIBNhS2a8cQVABDCQXVXrc0tOmO8
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAOZ3GEIaDcugMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTEwMjQx
NTE5MDlaGA8yMTk5MDMyOTE1MTkwOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCjiPgW3vsXRj4JoA16WQDyoPc/eh3QBARaApJEc4nPIGoUolpAXcjFhWplo2O+
ivgfCsc4AU9OpYdAPha3spLey/bhHPRi1JZHRNqScKP0hzsCNmKhfnZTIEQCFvsp
DRp4zr91/WS06/flJFBYJ6JHhp0KwM81XQG59lV6kkoW7QIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAGLLrY3P+HH6C57dYgtJkuGZGT2+rMkk2n81/abzTJvsqRqGRrWv
XRKRXlKdM/dfiuYGokDGxiC0Mg6TYy6wvsR2qRhtXW1OtZkiHWcQCnOttz+8vpew
wx8JGMvowtuKB1iMsbwyRqZkFYLcvH+Opfb/Aayi20/ChQLdI6M2R5VU
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
```

```
MIIDOzCCAiOgAwIBAgIJAO/+DgYF78KwMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA0Mjky
MDM1MjJaGA8yMTk4MTAwMjIwMzUyMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAv1ZLV+Z/P6INq+R1qLkzETBg7sFGKPiwHekbpuB6lrRxKHhj8V9vaReM
lnv1Ur5LAPpMPYDsuJ4WoUbPYAqVqyMAo7ikJHCCM1cXgZJefgN6z9bpS+uA3YVh
V/0ipHh/X2hc2S9wvxKWiSHu6Aq9GVpqL035tJQD+NJuqFd+nXrtcw4yGtmvA6wl
5Bjn8WdsP3xOTKjrByYY1BhXpP/f1ohU9jE9dstsRXLa+XTgTPWcWdCS2oRTWPGR
c5Aeh47nnDsyQfP9gLxHeYeQItV/BD9kU/2Hn6mnRg/B9/TYH8qzlRTzLapXp4/5
iNwusrTNexGl8BgvAPrfhjDpdgYuTwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB7
5ya11K/hKgvaRTvZwVV8GlVZt0CGPtNvOi4AR/UN6TMm51BzUB5nurB4z0R2MoYO
Uts9sLGvSFALJ4otoB77hyNpH3drttU1CVVwal/yK/RQLSon/IoUkaGEbqalu+mH
nYad5IG4tEbmepX456XXcO58MKmnczNbPyw3FRzUZQtI/sf94qBwJ1Xo6XbzPKMy
xjL57LHIZCssD+XPifXay69OFlsCIgLim11HgPkRIHEOXLSf3dsW9r+4CjoZqB/Z
jj/P4TLCxbYCLkvglwaMjgEWF40Img0fhx7yT2X92MiSrs3oncv/IqfdVTiN8OXq
jgnq1bf+EZEZKvb6UCQV
-----END CERTIFICATE-----
```

Europa (Paris) – eu-west-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUaC9fX57UDr6u1vBvsCsECKBZQyIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MzczOFoXDTI5MDQyODE2MzczOFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUaC9fX57U
Dr6u1vBvsCsECKBZQyIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCARv1bQEDaMEzYI0nPlu8GHcMXgmgA94HyrXhMMcaIlQwocGBs6VILGVhM
TXP2r3JFaPEpmXSQNQHvGA13clKwAZbni8wtzv6qXb4L4muF34iQRHF0nYrEDoK7
mMPR8+oXKKuPO/mv/XKo6XAV5DDERdSYHX5kkA2R9wtvyZjPnQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALWSfgHuT/ARMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA1MzEx
MTE4MTZaGA8yMTk2MTEwMzExMTgxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy5V7KDqnEvF3DrSProFcgu/oL+QYD62b1U+Naq8aPuljJe127Sm9WnWA
EBdOSASkOaQ9fzjCPoG5SGgWKxYoZjsevHpmzjVv9+Ci+F57bSuMbjgUbvbRIFUB
bxQojVoXQPHgK5v433ODxkQ4sjRyUbf4YV1AFdfU7zabC698YgPVOExGhXPlTvco
8mlc631ubw2g52j0lzaozUkHPSbknTomhQIvO6kUfX0e0TDMH4jLDG2ZIrUB1L4r
OWKG4KetduFrRZyDHF6ILZu+s6ywiMicUd+2UllDFC6oas+a8D11hmO/rpWU/ieV
jj4rWAFrsebpn+Nhgy96iiVUGS2LuQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDE
iYv6FQ6knXCg+svlcaQG9q59xUC5z8HvJZ1+SxzPKKC4PKQdKvIIfE8GxVXqlZG1
cl5WKTFDMapnzb9RV/DTaVzWx3cMYT77vm1Hl1XGjhx611CGcENH1egI3lOTILsa
+KfopuJEQQ9TDMAIkGjhA+KieU/U5Ctv9fdej6d0GC6OEuwKkTNzPWue6UMq8d4H
2xqJboWsE1t4nybEosvZfQJcZ8jyIYcYBnsG13vCLM+ixjuU5MVVQNMY/gBJzqJB
V+U0QiGiuT5cYgY/QihxdHt99zwGaE0ZBC7213NKrlNuLSrqhDI2NLu8NsExqOFy
OmY0v/xVmQUQl26jJXaM
```

```
-----END CERTIFICATE-----
```

Europa (Spanien) – eu-south-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAq
+gAwIBAgIGAXjwLk46MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAGG2m8EKmaf5qQqj3Z
+rzSaTaXE3B/R/4A2VuGqRYR7MljPtwdmU6/3CPjCACcZmTIcOAKbFiDHqadQgBZXfzGpzw8Zo
+eYmmk5fXycgnj57PYH1dIWU6I7mCbAah5MZMcmHaTmIsomGrhcnWB8d8qOU7oZ0UWK4lbiAQs1MihoUwCQYHKoZIzjg
WmbaU7YM5GwCFCvIJOesO5hZ8PHC52dAR8WWC6oe
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjwLkiaMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
VvR1+45Aey5zn3vPk6xBm5o9grSDL6D2iAuprQnfVXn8CIbSDbWFhA3fi5ippjKkh3sl8VyCvCOUXKdOaNrYBrPRkrdH
+3m/
rxIUZ2IK1fDlC6sWAjddf6sBrV2w2a78H0H8EwuwiSgttURBjwJ7KPPJCqaqrQIDAQABMA0GCSqGSIb3DQEBBQUAA4GB
+FzqQDzun/
iMMzcFucmLMl5BxEblrFXOz7IIuOeiGkndmrqUeDCykztLku45s7hxdNy4ltTuVAaE5aNBdw5J8U1mRvsKvHLy2ThH6h
+hBgiphYp84DUbWVYeP8YqLEJSqscKscWC
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALWSmO6DvSpQMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
MzU4NDNaGA8yMjAxMTIyMjEzNTg0M1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
```

```
CgKCAQEAuAAhuSpsHC00/fD2zNlBDpNLRndi9qbHsNeuz3WqN7Samj2aSrM2hS+i
hUxx0BspZj0tZCOsbpPZ+i74NOEQtFeqQoEGvKhB1nJiF4y5I81HDhs5qHvoIivm
7rbbik3zgm1PqS/DmDjVQaXPcD31Rd9ILwBmWEwJqHigyNVlxYtCzTQcrlBrvNZM
dnNgCDAdX/HBEFxx9O12xeu0bSt0s+PJWZ1RTbYrNe7LIH6ntUqHxP/ziQ5trXEZ
uqy7aWk1L8uK4jmyNph0lbaqBa3Y6pYmU1nC27UE4i3fnPB0LSiAr+SrwVvX1g4z
ilo8kr+tbIF+JmcgYLBvO8Jwp+EUqQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUwvGzKJL9A5LReJ4Fxo5K6I20xcowgY4GA1UdIwSBhjCBg4AUwvGz
KJL9A5LReJ4Fxo5K6I20xcqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALWSmO6DvSpQMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAJAZd31jyoTGLawAD2+v/vQsaB9vZIx5EImi
G8YGkd61uFWeNhAmtrwyE/i6FDSIphDrMHBkvw/D3BsqK+Ev/JOK/VYuaYDx/8fp
H4cwp9jC57CXzdIDREWNf6M9PsHFg2WA9XNNtClOZL5WJiJwel8eDSg+sqJUxE0l
MW+QChq/20F6niyaRK4bXrZq14as7h+F9u3A9xHEOVP7Zk9C2ehrBXzCMLSDt3GV
fEuMea2RxMhozwz34Hkdb6j18qoCfygubulovRNQjKw/cEmgPR16KfZPP5caILVt
9qkYPvePmbiVswZDee73cDymJYxLqILpOZwyXvUH8StiH42FHZQ=
-----END CERTIFICATE-----
```

Europa (Stockholm) – eu-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUN1c9U6U/xiVDFgJcYKZB4NkH1QEwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MDYwM1oXDTI5MDQyODE2MDYwM1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUN1c9U6U/
xiVDFgJcYKZB4NkH1QEwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBTIQdoFSDRHkpqNPUbZ9WXR2O5v/9bpmHojMYZb3Hw46wsaRso7STiGGX/
tRqjIkPUIXsdhZ3+7S/RmhFznmZc8e0bjU4n5vi9CJtQSt+1u4E17+V2bF+D3h/7
wcfE0l3414Q8JaTDtfEf/aF3F0uyBvr4MDMd7mFvAMmDmBPSlA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALc/uRxg++EnMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
NDAwMTFaGA8yMTk3MDkxMzE0MDAxMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzwCGJEJIxqtr2PD2a1mA6LhRzKhTBa1AZsg3eYfpETXIVlrpojMfvVoN
qHvGshWLgrGTT6os/3gsaADheSaJKavxwX3X6tJA8fvEGqr3a1C1MffH9hBWbQqC
LbfUTAbkwis4GdTUwOwPjT1Cm3u9R/VzilCNwkj7iQ65AFAI8Enmsw3UGldEsop4
yChKB3KW3WI0FTh0+gD0YtjrqqYJxpGOYBpJp5vwdd3fZ4t1vidmDMs7liv4f9Bx
p0oSmUobU4GUlFhBchK1DukICVQdnOVzdMonYm7s+HtpFbVHR8yf6QoixBKGdSal
mBf7+y0ixjCn0pnC0VLVooGo4mi17QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDG
4ONZiixgk2sjJctwbyD5WKLTH6+mxYcDw+3y/F0fWz561YORhP2FNnPOmEkf0Sl/
Jqk4svzJbCbQeMzRoyaya/46d7UioXMHRZam5IaGBhOdQbi97R4VsQjwQj0RmQsq
yDueDyuKTwWLK9KnvI+ZA6e6bRkdNGflK4N8GGKQ+fBhPwVELkbT9f16OJkezeeN
S+F/gDADGJgmPXfjogICb4Kvshq0H5Lm/xZlDULF2g/cYhyNY6EOI/eS5m1I7R8p
D/m6WoyZdpInxJfxW616OMkxQMRVsruLTNGtby3u1g6ScjmpFtvAMhYejBSdzKG4
FEyxIdEjoeO1jhTsck3R
```

```
-----END CERTIFICATE-----
```

Europa (Zürich) – eu-central-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXiKJnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAYNjaCNg/
cfgQOl1BUj5ClUulqwZ9Q+SfDzPZh9D2C0VbiRANiZoxrV8RdgmzzC5T7VcriVwjwvta2Ch//
b+sZ86E5h0XWWr+BeEjD9cu3eDj12XB5sWEbNHNx49p5Tmtu5r2LDtlL8X/
Rpfalu2Z2OJgjFJWGf7hRwxe456n
+lowCQYHKoZIzjgEAwMvADAsAhRChsLcj4U5CVb2cp5M0RE1XbXmhAIUeGSnH+aiUQIWmPEFja+itWDufIk=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjSGFGiMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
opKZAUusJx2hpgU3pUHhlp9ATh/VeVD582jTd9IY
+8t5MDa6Z3fGliByEiXz0LEHdi8MBacLREu1TwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAILlpoE3k9o7KdALAxsFJNit
+g3RMzdbiFM+7MA63Nv5fsf+0xgcjSNBElvPCDKFvTJl4QQhToy056llO5GvdS9RK
+H8xrP2mrqngApoKTApv93vHBixgFSn5KrczRO0YSm3OjkqbydU7DFlmkXXR7GYE+5jbHvQHYiT1J5sMu
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALvT012pxTxNMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
NTEyMDdaGA8yMjAxMTIyMjE1MTIwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAyn+Lsnq1ykrfYlZkk6aAAYNReNd9Iw8AUwCBkgOr2eBiBBepYxHwU85N
++moQ+j0EV2VaahBeTLShGZZS1HsyK8+cYT2QzpghIoamcYhrPXyIxlWiRQlaqSg
```

```
OFiE9bsqL3rCF5Vz+tOiTe5W/7ojfOFls6++g7ZpobwJlpMbuJepqyeHMPyjvO5A
age81lJewc4bxo2ntaW0HCqNksqfYB78j6X6kn3PFpX7FaYAwZA+Xx6C7UCY7rNi
UdQzfAo8htfJi4chz7frpUdQ9kl3IOQrsLshBB5fFUjl09NiFipCGBwi+8ZMeSn1
5qwBI01BWXPfG7WX6Owyjhmh6JtE1wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU8HN4vvJrsZgPQeksMBgJb9xR1yYwgY4GA1UdIwSBhjCBg4AU8HN4
vvJrsZgPQeksMBgJb9xR1yahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALvT012pxTxNMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGlHYDtcHpfBvdHx9HeQE8HgNugJUPdEqxun
t9U33p8VFrs+uLPtrOd9HDJEGvvs5h84EUie/oGJxRt7V1Vlid1PvHf6cRmpjgqY
YdggAVkZtY/PnFVmzf2bMVlSQPrqCl7U0zaw2Kvnj4zgX0rZyCetgrRZSUSxotyp
978Wy9ccXwVSeYG/YAr5rJpS6ZH7eRQvUY0IzwFNeaOPgOTEVpcjWlV6+MQEvsEx
W85q+s6AVr49eppEx8SLJsl0C23yB+L+t32tAveQImRWtJMpzZ5cxh/sYgDVeoC0
85H1NK/7H9fAzT1cPu1oHSnB0xYzzHGOAmXmusMfwUk8fL1RQkE=
-----END CERTIFICATE-----
```

Israel (Tel Aviv) – il-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq+gAwIBAgIGAX0QPi
+9MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcMB1NlYX
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAbazCL5XXyPmcw3+oMYQUF5/9YogW6D0FZbYuyPgjOoUwWdl6fjlzWca
pq+l1ezuK2DFOzNTEyPEwwCQYHKoZIzjgEAwMvADAsAhRt1jkpXsvrS
+xTo2M9h2s2uLAhEQIUOZ2FcnTSrshF2EIdixZZwtNv66Q=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAX0QQGVLMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+S8vOy5hpLoRe4RkOrY0cM3bN07GdEMlin5mU0y1t8y3ct4YewvmkgT42kTyMM
+t1K4S0xsqjXxxS716uGYh7eWtkxrCihj8AbXN/6pa095h
+7TZyl2n83keiNUzM2KoqQVMwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBADwA6VVEIIZD2YL00F12po40xDLzIc9XvqFPS
FmU7H8s62/jD6cOR1A1cClIyZUe1yT1ZbPySCs43J+Thr8i8FSRxzDBSZZi5foW
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOVp1h2I9wW7MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTUx
MjQ0MTJaGA8yMjAxMTIxOTEyNDQxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA13PkyWvl61iV/SYfO1UFO76UpDfPm2SF/Rz/o33cm699X++EYPxTnoEc
vmWeS0I7eDXc4OCUiToG0sEx0klE0CX1Z1tK6qJ+zgWQLZ9SZEC9H0NsSA6LhrHu
Nq0dzeK3LjhdfcX46/4GqdiptpdTuM4m/hOQ5yx4JMQ/n1sdpv4M5VLRWwWW9Lem
ufb79Id7O9SispxgRsz1KXIjp7N9S4BY7itSXz97uSyzTqEjWZ6mDUhTu3t21GKC
6flALGTTrG2yghEhz53rkvLsvwzjPSSlT6LIf0mrRPzHaf+EdaKoasElE1SHh+ZH
9mI81HywpE+HZ+W+5hBCvjYp90Y1fwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU58tN2JO+yEGq5JbIXxGi4vRVPyIwgY4GA1UdIwSBhjCBg4AU58tN
2JO+yEGq5JbIXxGi4vRVPyKhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOVp1h2I9wW7MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANBN0e1EqNy4+IU2yQzMJ+Wy5ZIOtTP6GSBR
7muVY1bDeAwtNTEOpwgrZVlC7/xq5Q0LC1y0Z70hHXEf8au7qStaAoUtxzvhTAZI
NC0lwoFU56UFw4N0vZII17iqEfoqRC4PpI3OxqEJHFy0VLlvAzJoKB4QLLqDAYVA
LXCiOLoVT+y9tRYsxw5MyO0Bi6fxQIIADl2bE9xkunTN1Jkkwqo3LxNy/ryz4QWR
8K7jHUItifv4h/hxBKpHEquN8CkdvM9oeGl7I8PFrSFEpGr1euDXY0euZzzYiDBV
m6GpTJgzpVsEuIX52dPcPemwQncoIfZyhWDW85MJUnby2WTEcFo=
-----END CERTIFICATE-----
```

Mexiko (Zentral) – mx-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq8CCQD4QwfTExrgxTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDExMTQwOTQ4MjRaGA8y
MDUwMTExNTA5NDgyNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtzCCASwGByqGSM44BAEwggEfAoGBAK+pJEOtD2RFlCbf
oAzONffZa42FB8G6OA/30DT81xWvB2Hnmgw7LfiELYqgfuck3YSDffNDcmiFTJuX
AU9u0NtbbxcOytcdUq4HInpHiB85I6WWWKYB66aGbvYowUPpqBZkASb1i/pYAh5W
```

```
nNYvx408008tTzqpMfZDchJHzWqBAhUA0ogoJzTw2/4pKhz9aqTsRCzRVPsCgYEA
qklRUcuU0du/bT/M6kWxYvrTGhO9KXQe+7RtbaIq4dWRsCBnO4smDY/GmI9H8ew1
LRJ9AcLGmxDm795CvVZkHNcht7PDAREagWmz2YvhLA+ev6U0RpfdlBXCck2p1CxQ
LMtoFO7DThksHIQBtnlQdHDvguKEZQz/Iobhne6Kb3wDgYQAAoGAQSTlOqFq6RtR
Jvp406XhGl+eO9SQUpevpzG3Dzbdy6EQ8PBJDOHHJvxbebvpnQssh0CnQfTkSw26
jwPy9V5zRC0ZezwnRTyGSJwiErUKDGeVekEAoNJL1USy8jKkgBajlskZrR+0JHDN
Jv3UwYIPplc4ZS2f2E7btrtlaWt/P70wCQYHKoZIzjgEAwMvADAsAhRXljPWKWYf
61DkDVdgPPHsS2/LuwIUejcGV9WuS3uPvJ6lmn4opxUGBZw=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICPzCCAaigAwIBAgIUCmzpTTMBQYItpMC2VDYsZfIAS7IwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcMB1NlYXR0bGUxIDAeBgNVBAoMF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQwMjEyNTAzNloXDTI5MDQwMTEyNTAzNlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcMB1NlYXR0bGUxIDAe
BgNVBAoMF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDfvOnCzm1iN58Nm7k6ehoy6v0lnnFI617D6CY3bfuq01RCdEQL
96+pYawJieTH8JAQKj02CAa3AeaqdXTE/pDhI/YKLreeMb4K68WMn24Wjjs6oxjB
bAmsKXtt9ihKHGBFNUhgFrNFYyA2i7ieJviwpHjQ/XgXiG2u1/t/4VydUwIDAQAB
MA0GCSqGSIb3DQEBCwUAA4GBAL5+vvj4lhaE+J5tuCqV3XJzDd97lsD4le2O2uGw
P0sGdUcRAdxzU3Bwq/hhtzNWnfwo0aCEQKmLM7xyd3nUa0VvKXLq+DDuayipWINr
OATnNxFRe99d38qHTR1dgkjZdKbbtnl6O4fgM57tVEuQJd/N4ILl9jaRcJ5Ip+9t
3y5t
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALxuE00HoJomMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yNDEwMzEx
MTE0MzNaGA8yMjA0MDQwNjExMTQzM1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA13xWucALo8M/TXbZJgHrqFqFON91dSLPE/eLbmeIJbP1pb9ICd33qKAx
HlKSrXI9b9YS3U1Pl0bF3ZgfeE/x4Y0KDDZwzpf07H8IgRittULJoNLYVKCJXWPq
Ky1qvDJX3653dUbUu9eAdVCTRgk7eKpPBLAmW27+pgAGzEYrVV3u2AvqNTonvfTU
sPgEVnAL1J490pNM85KtFynxFTWGigHkd3BHidxmLrTH4I4eRxNZ9q/3gsDW+zKt
jQlpM7JzZa2OqxsF5YQDh1fF52Emqsr+ufLeGqDLOgT1QWcqpz57AX8GqZpgZULo
itCRNXbQDzZY9FxIgpiFJv3y/qYYDQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCt
```

```
MTeH4EgqjJEjb1qm5tzXYurLprVrEVQ+PhGXJFJd3xAZyeaDVYy7kio08E2xhmHd
HtkBDty2KnOHsTQmeAJCci7d4tYXZ/1qe341wwm9OoFcO8jhIndx6FXJCgQUY4dL
AAr9HQJFWG5dMZgbi1Zuhxdio3sSoOBjL2p7QIsGNkITvCDIs/H0/szpJnyyyIqu
wmUhSel5hdy5MwOsyUKVGnAdaS5Vd9oL4kLszS9nBZ7ny6BC9odIkFAdGqQ5vM4z
vcbfOq14hjatQmJgJhksN/0Dpl78Gheq0pIhP8LTkAOEG2832nQLzCa3oxSk8otG
GJXkzzyQjse+13r8+yNJ
-----END CERTIFICATE-----
```

Naher Osten (Bahrain) – me-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7jCCAq4CCQCVWIgSmP8RhTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDUxMzA2MjFaFw00
NTAyMDUxMzA2MjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDcwojQfgWdV1QliO0B
8n6cLZ38VE7ZmrjZ9OQV//Gst6S1h7euhC23YppKXi1zovefSDwFU54zi3/oJ++q
PHlP1WGL8IZ34BUgRTtG4TVolvp0smjkMvyRu5hIdKtzjV93Ccx15gVgyk+o1IEG
fZ2Kbw/Dd8JfoPS7KaSCmJKxXQIVAIZbIaDFRGa2qcMkW2HWASyNDl7bAoGBANtz
IdhfMq+l2I5iofY2oj3HI21Kj3LtZrWEg3W+/4rVhL3lTm0Nne1rl9yGujrjQwy5
Zp9V4A/w9w2O10Lx4K6hj34Eefy/aQnZwNdNhv/FQP7Az0fju+Yl6L13OOHQrL0z
Q+9cF7zEosekEnBQx3v6psNknKgD3Shgx+GO/LpCA4GFAAKBgQCVS7m77nuNAlZ8
wvUqcooxXMPkxJFl54NxAsAul9KP9KN4svm0O3Zrb7t2FOtXRM8zU3TqMpryq1o5
mpMPsZDg6RXo9BF7Hn0DoZ6PJTamkFA6md+NyTJWJKvXC7iJ8fGDBJqTciUHuCKr
12AztQ8bFWsrTgTzPE3p6U5ckcgV1TAJBgcqhkjOOAQDAy8AMCwCFB2NZGWm5EDl
86ayV3c1PEDukgQIAhQow38rQkN/VwHVeSW9DqEshXHjuQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDPDCCAqWgAwIBAgIJAMl6uIV/zqJFMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0dGxlMSAw
HgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwRZWMyLmFt
YXpvbmF3cy5jb20wIBcNMTkwNDI2MTQzMjQ3WhgPMjE5ODA5MjkxNDMyNDdaMHIx
CzAJBgNVBAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0
dGxlMSAwHgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwR
ZWMyLmFtYXpvbmF3cy5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALVN
CDTZEnIeoX1SEYqq6k1BV0ZlpY5y3KnoOreCAE589TwS4MX5+8Fzd6AmACmugeBP
```

```
Qk7Hm6b2+g/d4tWycyxLaQlcq81DB1GmXehRkZRgGeRge1ePWd1TUA0I8P/QBT7S
gUePm/kANSFU+P7s7u1NNl+vynyi0wUUrw7/wIZTAgMBAAGjgdcwgdQwHQYDVR0O
BBYEFILtMd+T4YgH1cgc+hVsVOV+480FMIGkBgNVHSMEgZwwgZmAFILtMd+T4YgH
1cgc+hVsVOV+480FoXakdDByMQswCQYDVQQGEwJVUzETMBEGA1UECAwKV2FzaGlu
Z3RvbjEQMA4GA1UEBwwHU2VhdHRsZTEgMB4GA1UECgwXQW1hem9uIFdlYiBTZXJ2
aWNlcyBMTEMxGjAYBgNVBAMMEWVjMi5hbWF6b25hd3MuY29tggkAyXq4hX/OokUw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOBgQBhkNTBIFgWFd+ZhC/LhRUY
4OjEiykmbEp6hlzQ79T0Tfbn5A4NYDI2icBP0+hmf6qSnIhwJF6typyd1yPK5Fqt
NTpxxcXmUKquX+pHmIkK1LKDO8rNE84jqxrxRsfDi6by82fjVYf2pgjJW8R1FAw+
mL5WQRFexbfB5aXhcMo0AA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANZkFlQR2rKqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTAyMDUx
MzA2MjBaGA8yMTk4MDcxMTEzMDYyMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy4Vnit2eBpEjKgOKBmyupJzJAiT4fr74tuGJNwwa+Is2vH12jMZn9Il1
UpvvEUYTIboIgISpf6SJ5LmV5rCv4jT4a1Wm0kjfNbiIlkUi8SxZrPypcw24m6ke
BVuxQZrZDs+xDUYIZifTmdgD50u5YE+TLg+YmXKnVgxBU6WZjbuK2INohi71aPBw
2zWUR7Gr/ggIpf635JLU3KIBLNEmrkXCVSnDFlsK4eeCrB7+UNak+4BwgpuykSGG
Op9+2vsuNqFeU1l9daQeG9roHR+4rIWSPa0opmMxv5nctgypOrE6zKXx2dNXQldd
VULv+WH7s6Vm4+yBeG8ctPYH5GOo+QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBs
ZcViiZdFdpcXESZP/KmZNDxB/kktlIEIhsQ+MNn29jayE5oLmtGjHj5dtA3XNKlr
f6PVygVTKbtQLQqunRT83e8+7iCZMKI5ev7pITUQVvTUwI+Fc01JkYZxRFlVBuFA
WGZO+98kxCS4n6tTwVt+nSuJr9BJRVC17apfHBgSS8c5OWna0VU/Cc9ka4eAfQR4
7pYSDU3wSRE01cs30q34lXZ629IyFirSJ5TTOIc0osNL7vwMQYj8HOn4OBYqxKy8
ZJyvfXsIPh0Na76PaBIs6ZlqAOflLrjGzxBPiwRM/XrGmF8ze4KzoUqJEnK13O6A
KHKgfiigQZ1+gv5FlyXH
-----END CERTIFICATE-----
```

Naher Osten (VAE) – me-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXhqnnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
```

```
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAW+csuHsWp/7/
pv8CTKFwxsYudxuR6rbWaHCykIeAydXL9AWnphK6yp1ODEMBFl68Xq8Hp23sOWyf8moOhqCom9+0+ovuUFdpvCie86bp
TOZU568Ty1ff3dDWbdRzeNQRHodRG+XEQSizMkAreeWt4kBa+PUwCQYHKoZIzjgEAwMvADAsAhQD3Z
+XGmzKmgaLgGcVX/Qf1+Tn4QIUH1cgksBSVKbWj81tovBMJeKgdYo=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjRrnDjMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
KyA6zyruJQrYy00a6wqLA7eeUzk3bMiTkLsTeDQfrkaZMfBAjGaaOymRo1C3qzE4rIenmahvUplu9ZmLwL1idWXMRX2R
+d2SeoKOKQWoc2UOFZMHYxDue7zkyk1CIRaBukTeY13/
RIrlc6X61zJ5BBtZXlHwayjQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBABTqTy3R6RXKPW45FA+cgo7YZEj/
Cnz5YaoUivRRdX2A83BHuBTvJE2+WX00FTEj4hRVjameE1nENoO8Z7fUVloAFDlDo69fhkJeSvn51D1WRrPnoWGgEfr1
B+Wqm3kVEz/QNcz6npmA6
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM4h7b1CVhqqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MTEx
MDE1MDNaGA8yMjAxMDkxNTEwMTUwM1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApybTWfMOhSoMpqPo72eqAmnn1dXGZM+G8EoZXzwHwT/+IHEXNB4q5N6k
tudYLre1bJxuzEw+iProSHjmb9bB9YscRTofjVhBlt35Fc+i8BaMeH94SR/eE8QO
mll8gnLNW3d62lyuhzuyv1e5wVlRqzYw+X2zRH4/wRDOCOpzjKoHIgyPKsMgwsw5
aTZhNMsGxZN9dbkf0iCGeQLDytwU/JTh/HqvSr3VfUOapTJJiyAxoCtZWgp1/7wC
RvOCSMRJobpUqxZgl/VsttwNkikSFz1wGkcYeSQvk+odbnYQckA8tdddoVI56eD4
qtREQvfpMAX5v7fcqLexl5d5vH8uZQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUOadrbTs+OhzwoAgUJ7RqQNdwufkwgY4GA1UdIwSBhjCBg4AUOadr
bTs+OhzwoAgUJ7RqQNdwufmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM4h7b1CVhqqMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAICTdAOGEOnII8HaGCpCB8us/hGFaLptJaAf
D5SJAyVy66/mdfjGzE1BKkKxnbxemEVUIzbRidOnyilB+pKwN3edAjTZtWdpVA0V
```

```
R/G/qQPmcVljtycBz4VC6SuOUYflGzLH1GZ6GJWbuDtFzw8r7HGdRN1wrEPe3UF2
sMpuVezqnRUdvVRoVQP4jFgNsE7kNvtn2NiPhb/CtrxpcwIQ7r6YeoHcBSheuV1Z
xZDHynC3KUprQGx1+Z9QqPrDf180MaoqAlTl4+W6Pr2NJYrVUFGS/ivYshMg574l
CPU6r4wWZSKwEUXq4BInYX6z6iclp/p/J5QnJp2mAwyi6M+I13Y=
-----END CERTIFICATE-----
```

Südamerika (São Paulo) – sa-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUX4Bh4MQ86Roh37VDRRX1MNOB3TcwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2NDYwOVoXDTI5MDQyODE2NDYwOVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
```

```
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUX4Bh4MQ8
6Roh37VDRRX1MNOB3TcwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBnhocfH6ZIX6F5K9+Y9V4HFk8vSaaKL5ytw/P5td1h9ej94KF3xkZ5fyjN
URvGQv3kNmNJBoNarcP9I7JIMjsNPmVzqWawyCEGCZImoARxSS3Fc5EAs2PyBfcD
9nCtzMTaKO09Xyq0wqXVYn1xJsE5d5yBDsGrzaTHKjxo61+ezQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMcyoxx4U0xxMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU4MDJaGA8yMTk1MDExNzA4NTgwMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAw45IhGZVbQcy1fHBqzROhO8CsrDzxj/WP4cRbJo/2DAnimVrCCDs5O86
FA39Zo1xsDuJHDlwMKqeXYXkJXHYbcPWc6EYYAnR+PlLG+aNSOGUzsy202S03hT0
B20hWPCqpPp39itIRhG4id6nbNRJOzLm6evHuepMAHR4/OV7hyGOiGaV/v9zqiNA
pMCLhbh2xk0PO35HCVBuWt3HUjsgeks2eEsu9Ws6H3JXTCfiqp0TjyRWapM29OhA
cRJfJ/d/+wBTz1fkWOZ7TF+EWRIN5ITEadlDTPnF1r8kBRuDcS/lIGFwrOOHLo4C
cKoNgXkhTqDDBDu6oNBb2rS0K+sz3QIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUqBy7D847Ya/w321Dfr+rBJGsGTwwgY4GA1UdIwSBhjCBg4AUqBy7
D847Ya/w321Dfr+rBJGsGTyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMcyoxx4U0xxMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACOoWSBf7b9AlcNrl4lr3QWWSc7k90/tUZal
PlT0G3Obl2x9T/ZiBsQpbUvs0lfotG0XqGVVHcIxF38EbVwbw9KJGXbGSCJSEJkW
vGCtc/jYMHXfhx67Szmftm/MTYNvnzsyQQ3v8y3Rdah+xe1NPdpFrwmfL6xe3pFF
cY33KdHA/3PNLdn9CaEsHmcmj3ctaaXLFIzZhQyyjtsrgGfTLvXeXRokktvsLDS/
YgKedQ+jFjzVJqgr4NjfY/Wt7/8kbbdhzaqlB5pCPjLLzv0zp/XmO6k+JvOePOGh
JzGk5t1QrSju+MqNPFk3+1O7o910Vrhqw1QRB0gr1ExrviLbyfU=
-----END CERTIFICATE-----
```

AWS GovCloud (USA-Ost) – us-gov-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
```

```
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULVyrqjjwZ461qelPCiShB1KCCj4wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDUwNzE1MjIzNloXDTI5MDUwNjE1MjIzNlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IULVyrqjjw
Z461qelPCiShB1KCCj4wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBfAL/YZv0y3zmVbXjyxQCsDloeDCJjFKIu3ameEckeIWJbST9LMto0zViZ
puIAf05x6GQiEqfBMk+YMxJfcTmJB4Ebaj4egFlslJPSHyC2xuydHlr3B04INOH5
Z2oCM68u6GGbj0jZjg7GJonkReG9N72kDva/ukwZKgq8zErQVQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALPB6hxFhay8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
```

```
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
MjMyNDlaGA8yMTk3MDkxMzEyMzI0OVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAva9xsI9237KYb/SPWmeCVzi7giKNron8hoRDwlwwMC9+uHPd53UxzKLb
pTgtJWAPkZVxEdl2Gdhwr3SULoKcKmkqE6ltVFrVuPT33La1UufguT9k8ZDDuO9C
hQNHUdSVEuVrK3bLjaSsMOS7Uxmnn7lYT990IReowvnBNBsBlcabfQTBV04xfUG0
/m0XUiUFjOxDBqbNzkEIblW7vK7ydSJtFMSljga54UAVXibQt9EAIF7B8k9l2iLa
mu9yEjyQy+ZQICTuAvPUEWe6va2CHVY9gYQLA31/zU0VBKZPTNExjaqK4j8bKs1/
7dOV1so39sIGBz21cUBec1o+yCS5SwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBt
hO2W/Lm+Nk0qsXW6mqQFsAou0cASc/vtGNCyBfoFNX6aKXsVCHxq2aq2TUKWENs+
mKmYu1lZVhBOmLshyllh3RRoL3Ohp3jCwXytkWQ7ElcGjDzNGc0FArzB8xFyQNdK
MNvXDi/ErzgrHGSpcvmGHiOhMf3UzChMWbIr6udoDlMbSIO7+8F+jUJkh4Xl1lKb
YeN5fsLZp7T/6YvbFSPpmbn1YoE2vKtuGKxObRrhU3h4JHdp1Zel1pZ6lh5iM0ec
SD11SximGIYCjfZpRqI3q50mbxCd7ckULz+UUPwLrfOds4VrVVSj+x0ZdY19Plv2
9shw5ez6Cn7E3IfzqNHO
-----END CERTIFICATE-----
```

AWS GovCloud (USA-West) – us-gov-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUe5wGF3jfb7lUHzvDxmM/ktGCLwwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDUwNzE3MzAzMloXDTI5MDUwNjE3MzAzMlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUe5wGF3jf
b7lUHzvDxmM/ktGCLwwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCbTdpx1Iob9SwUReY4exMnlwQlmkTLyA8tYGWzchCJOJJEPfsW0ryy1A0H
YIuvyUty3rJdp9ib8h3GZR71BkZnNddHhy06kPs4p8ewF8+d8OWtOJQcI+ZnFfG4
KyM4rUsBrljpG2aOCm12iACEyrvgJJrS8VZwUDZS6mZEnn/lhA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANCOF0Q6ohnuMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTAx
OTQyNDdaGA8yMTk1MDIxMzE5NDI0N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzIcGTzNqie3f1olrrqcfzGfbymSM2QfbTzDIOG6xXXeFrCDAmOq0wUhi
3fRCuoeHlKOWAPu76B9os71+zgF22dIDEVkpqHCjBrGzDQZXXUwOzhm+PmBUI8Z1
qvbVD4ZYhjCujWWzrsX6Z4yEK7PEFjtf4M4W8euw0RmiNwjy+knIFa+VxK6aQv94
lW98URFP2fD84xedHp6ozZlr3+RZSIFZsOiyxYsgiwTbesRMI0Y7LnkKGCIHQ/XJ
OwSISWaCddbu59BZeADnyhl4f+pWaSQpQQ1DpXvZAVBYvCH97J1oAxLfH8xcwgSQ
/se3wtn095VBt5b7qTVjOvy6vKZazwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA/
S8+a9csfASkdtQUOLsBynAbsBCH9Gykq2m8JS7YE4TGvqlpnWehz78rFTzQwmz4D
fwq8byPkl6DjdF9utqZ0JUo/Fxelxom0h6oievtBlSkmZJNbgc2WYm1zi6ptViup
Y+4S2+vWZyg/X1PXD7wyRWuETmykk73uEyeWFBYKCHWsO9sI+62O4Vf8Jkuj/cie
1NSJX8fkervfLrZSHBYhxLbL+actVEo00tiyZz8GnhgWx5faCY38D/k4Y/j5Vz99
7lUX/+fWHT3+lTL8ZZK7fOQWh6NQpI0wTP9KtWqfOUwMIbgFQPoxkP00TWRmdmPz
WOwTObEf9ouTnjG9OZ20
```

```
-----END CERTIFICATE-----
```

STIG-Compliance für Ihre EC2-Instance

Security Technical Implementation Guides (STIGs) sind die von der Defense Information Systems Agency (DISA) aufgestellten Konfigurationsstandards zur Sicherung von Informationssystemen und Software. Um Ihre Systeme mit STIG-Standards konform zu machen, müssen Sie eine Vielzahl von Sicherheitseinstellungen installieren, konfigurieren und testen.

STIGs werden auf der Grundlage der folgenden Schwachstellenklassifizierungen angewendet. Wenn Sie ein STIG-Hardening-Image erstellen oder STIG-Einstellungen auf eine bestehende Instance anwenden, können Sie wählen, welche Stufe für das Hardening angewendet werden soll. Höhere Stufen beinhalten STIG-Einstellungen aller niedrigeren Stufen. Beispielsweise umfasst die Stufe High (Kategorie I) Einstellungen sowohl aus den Kategorien Medium als auch Low.

Compliance-Stufen

- Hoch (Kategorie I)

  Das schwerwiegendste Risiko. Schließt jede Schwachstelle ein, die zu einem Verlust der Vertraulichkeit, Verfügbarkeit oder Integrität führen kann.
- Mittel (Kategorie II)

  Schließt jede Schwachstelle ein, die zu einem Verlust der Vertraulichkeit, Verfügbarkeit oder Integrität führen kann, jedoch kann das Risiko gemindert werden.
- Niedrig (Kategorie III)

  Beinhaltet jede Schwachstelle, die Maßnahmen zum Schutz vor einem Verlust der Vertraulichkeit, Verfügbarkeit oder Integrität beeinträchtigt.

Amazon EC2 bietet die folgenden Methoden, um STIG-Hardening-Instances zu erstellen:

- Sie können Windows-Instances, die für STIG-Hardening vorkonfiguriert sind, von speziellen öffentlichen AWS-Windows-AMIs aus starten. Weitere Informationen finden Sie unter STIG-Hardening für AWS Windows Server AMIs in der AMI-Referenz für AWS Windows.

- Sie können ein benutzerdefiniertes AMI erstellen, um vorkonfigurierte Instances zu starten, die mit EC2 Image Builder STIG-Hardening-Komponenten erstellt wurden. Weitere Informationen finden Sie unter STIG-Hardening-Komponenten im Image-Builder-Benutzerhandbuch.
- Sie können das Systems-Manager-Befehlsdokument AWSEC2-ConfigureSTIG verwenden, um STIG-Einstellungen auf eine bestehende EC2-Instance anzuwenden. Das STIG-Befehlsdokument von Systems Manager sucht nach Fehlkonfigurationen und führt ein Korrekturskript aus, um die DoD-Zertifikate zu installieren und zu aktualisieren und unnötige Zertifikate zu entfernen, um die STIG-Compliance aufrechtzuerhalten. Für die Verwendung des STIG-Dokuments von Systems Manager fallen keine zusätzlichen Gebühren an.

Themen

- STIG-Hardening-Einstellungen für EC2-Instances
- STIG-Hardening-Skripte zum Herunterladen
- AWS Systems Manager verwenden, um STIG-Einstellungen auf Ihre Instance anzuwenden

STIG-Hardening-Einstellungen für EC2-Instances

Die STIG-Einstellungen variieren je nach dem Betriebssystem Ihrer Instance und der von Ihnen gewählten Konformitätsstufe. Der folgende Inhalt enthält systemspezifische Informationen zu STIGs, die auf jeder Konformitätsstufe angewendet werden.

Inhalt

- STIG-Einstellungen für EC2-Linux-Instances
- STIG-Hardening-Einstellungen für EC2-Windows-Instances

STIG-Einstellungen für EC2-Linux-Instances

Dieser Abschnitt enthält Informationen zu den STIG-Hardening-Einstellungen für Linux, die Amazon EC2 unterstützt. Das Hardening-Skript wendet unterstützte STIG-Einstellungen anhand der Linux-Distribution auf die Infrastruktur an. Wenn die Linux-Distribution keine eigenen STIG-Hardening-Einstellungen hat, verwendet Amazon EC2 die RHEL-Einstellungen wie folgt.

- STIG-Einstellungen für Red Hat Enterprise Linux (RHEL) 7
  - RHEL 7
  - CentOS 7

  - Amazon Linux 2 (AL2)
- STIG-Einstellungen für RHEL 8
  - RHEL 8
  - CentOS 8
- STIG-Einstellungen für RHEL 9
  - RHEL 9
  - CentOS Stream 9

Linux STIG Low (Kategorie III)

Die folgende Liste enthält STIG-Einstellungen, die Amazon EC2 für Ihre Infrastruktur unterstützt. Wenn eine unterstützte Einstellung für Ihre Infrastruktur nicht anwendbar ist, überspringt Amazon EC2 diese Einstellung und fährt fort. Beispielsweise gelten einige STIG-Hardening-Einstellungen möglicherweise nicht für eigenständige Server. Organisationsspezifische Richtlinien können auch beeinflussen, welche Einstellungen zutreffen, z. B. dass Administratoren die Dokumenteinstellungen überprüfen müssen.

Eine vollständige Liste finden Sie in der STIGs-Dokumentbibliothek. Informationen zum Anzeigen der vollständigen Liste finden Sie unter STIG Viewing Tools.

RHEL 7 STIG Version 3 Release 15

- RHEL 7/CentOS 7/AL2

  V-204452, V-204576 und V-204605

RHEL 8 STIG Version 2 Release 4

- RHEL 8/CentOS 8

  V-230241, V-230269, V-230270, V-230281, V-230285, V-230346, V-230381, V-230395, V-230468, V-230469, V-230485, V-230486, V-230491, V-230494, V-230495, V-230496, V-230497, V-230498, V-230499 und V-244527

RHEL 9 STIG Version 2 Release 5

- RHEL 9/CentOS Stream 9

V-257782, V-257795, V-257796, V-257824, V-257880, V-257946, V-257947, V-258037, V-258067, V-258069, V-258076, V-258138 und V-258173

Amazon Linux 2023 STIG Version 1 Release 1

V-274141

SLES 12 STIG Version 3 Release 3

V-217108, V-217113, V-217140, V-217198, V-217209, V-217211, V-217212, V-217213, V-217214, V-217215, V-217216, V-217236, V-217237, V-217238, V-217239, V-217282 und V-255915

SLES 15 STIG Version 2 Release 5

V-234811, V-234850, V-234868, V-234868, V-234873, V-234873, V-234905, V-234907, V-234908, V-234909, V-234933, V-234934, V-234935, V-234936, V-234955, V-234963, V-234967 und V-255921

Ubuntu 18.04 STIG Version 2 Release 15

V-219163, V-219164, V-219165, V-219172, V-219173, V-219174, V-219175, V-219178, V-219179, V-219180, V-219210, V-219301, V-219327, V-219332 und V-219333

Ubuntu 20.04 STIG Version 2 Release 3

V-238202, V-238203, V-238221, V-238222, V-238223, V-238224, V-238226, V-238234, V-238235, V-238237, V-238308, V-238323, V-238357, V-238362 und V-238373

Ubuntu 22.04 STIG Version 2 Release 5

V-260479, V-260480, V-260481, V-260521, V-260520, V-260476, V-260472, V-260549, V-260550, V-260551, V-260552, V-260581 und V-260596

Ubuntu 24.04 STIG Version 1 Release 2

V-270645, V-270646, V-270664, V-270820, V-270677, V-270690, V-270706, V-270710, V-270695, V-270749, V-270752 und V-270818

Linux STIG Medium (Kategorie II)

Die folgende Liste enthält STIG-Einstellungen, die Amazon EC2 für Ihre Infrastruktur unterstützt. Wenn eine unterstützte Einstellung für Ihre Infrastruktur nicht anwendbar ist, überspringt Amazon

EC2 diese Einstellung und fährt fort. Beispielsweise gelten einige STIG-Hardening-Einstellungen möglicherweise nicht für eigenständige Server. Organisationsspezifische Richtlinien können auch beeinflussen, welche Einstellungen zutreffen, z. B. dass Administratoren die Dokumenteinstellungen überprüfen müssen.

Eine vollständige Liste finden Sie in der STIGs-Dokumentbibliothek. Informationen zum Anzeigen der vollständigen Liste finden Sie unter STIG Viewing Tools.

> **Note**
>
> Die Kategorie Linux STIG Medium umfasst alle aufgelisteten STIG-Hardening-Einstellungen, die auf Linux STIG Low (Kategorie III) anwendbar sind, zusätzlich zu den STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie II unterstützt.

RHEL 7 STIG Version 3 Release 15

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (Low) unterstützt, sowie:

- RHEL 7/CentOS 7/AL2

  V-204405, V-204406, V-204407, V-204408, V-204409, V-204410, V-204411, V-204412, V-204413, V-204414, V-204415, V-204416, V-204417, V-204418, V-204420, V-204422, V-204423, V-204426, V-204427, V-204431, V-204434, V-204435, V-204437, V-204449, V-204450, V-204451, V-204457, V-204466, V-204490, V-204491, V-204503, V-204507, V-204508, V-204510, V-204511, V-204512, V-204514, V-204515, V-204516, V-204517, V-204521, V-204524, V-204531, V-204536, V-204537, V-204538, V-204539, V-204540, V-204541, V-204542, V-204543, V-204544, V-204545, V-204546, V-204547, V-204548, V-204549, V-204550, V-204551, V-204552, V-204553, V-204554, V-204555, V-204556, V-204557, V-204558, V-204559, V-204560, V-204562, V-204563, V-204564, V-204565, V-204566, V-204567, V-204568, V-204572, V-204579, V-204584, V-204585, V-204587, V-204588, V-204589, V-204590, V-204591, V-204592, V-204593, V-204596, V-204597, V-204598, V-204599, V-204600, V-204601, V-204602, V-204609, V-204610, V-204611, V-204612, V-204613, V-204614, V-204615, V-204616, V-204617, V-204619, V-204622, V-204625, V-204630, V-204631, V-204633, V-233307, V-237634, V-237635, V-251703, V-255925, V-255927 und V-256970

RHEL 8 STIG Version 2 Release 4

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (Low) unterstützt, sowie:

- RHEL 8/CentOS 8

  V-230222, V-230228, V-230231, V-230233, V-230236, V-230237, V-230238, V-230239, V-230240, V-230244, V-230245, V-230246, V-230247, V-230248, V-230249, V-230250, V-230255, V-230256, V-230257, V-230258, V-230259, V-230260, V-230261, V-230262, V-230266, V-230267, V-230268, V-230271, V-230273, V-230275, V-230276, V-230277, V-230278, V-230279, V-230280, V-230282, V-230286, V-230287, V-230288, V-230290, V-230291, V-230296, V-230298, V-230310, V-230311, V-230312, V-230313, V-230314, V-230315, V-230316, V-230318, V-230319, V-230320, V-230321, V-230322, V-230324, V-230325, V-230326, V-230327, V-230330, V-230333, V-230335, V-230337, V-230339, V-230341, V-230343, V-230345, V-230347, V-230348, V-230352, V-230353, V-230354, V-230356, V-230357, V-230358, V-230359, V-230360, V-230361, V-230362, V-230363, V-230365, V-230366, V-230368, V-230369, V-230370, V-230372, V-230373, V-230375, V-230376, V-230377, V-230378, V-230380, V-230382, V-230383, V-230385, V-230386, V-230387, V-230389, V-230390, V-230392, V-230393, V-230394, V-230396, V-230397, V-230398, V-230399, V-230400, V-230401, V-230402, V-230403, V-230404, V-230405, V-230406, V-230407, V-230408, V-230409, V-230410, V-230411, V-230412, V-230413, V-230418, V-230419, V-230421, V-230422, V-230423, V-230424, V-230425, V-230426, V-230427, V-230428, V-230429, V-230430, V-230431, V-230432, V-230433, V-230434, V-230435, V-230436, V-230437, V-230438, V-230439, V-230444, V-230446, V-230447, V-230448, V-230449, V-230455, V-230456, V-230462, V-230463, V-230464, V-230465, V-230466, V-230467, V-230470, V-230471, V-230472, V-230473, V-230474, V-230475, V-230478, V-230480, V-230481, V-230482, V-230483, V-230488, V-230489, V-230493, V-230502, V-230503, V-230505, V-230506, V-230507, V-230523, V-230524, V-230525, V-230526, V-230527, V-230532, V-230535, V-230536, V-230537, V-230538, V-230539, V-230540, V-230541, V-230542, V-230543, V-230544, V-230545, V-230546, V-230547, V-230548, V-230549, V-230550, V-230555, V-230556, V-230557, V-230559, V-230560, V-230561, V-237640, V-237642, V-237643, V-244519, V-244523, V-244524, V-244525, V-244526, V-244528, V-244531, V-244533, V-244535, V-244536, V-244538, V-244539, V-244542, V-244543, V-244544, V-244547, V-244550, V-244551, V-244552, V-244553, V-244554, V-250315, V-250316, V-250317, V-251707, V-251708, V-251709, V-251710, V-251711, V-251713, V-251714, V-251715, V-251716, V-251717, V-251718, V-256974, V-257258 und V-274877

RHEL 9 STIG Version 2 Release 5

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (Low) unterstützt, sowie:

- RHEL 9/CentOS Stream 9

V-257780, V-257781, V-257783, V-257786, V-257788, V-257790, V-257791, V-257792, V-257793, V-257794, V-257797, V-257798, V-257799, V-257800, V-257801, V-257802, V-257803, V-257804, V-257805, V-257806, V-257807, V-257808, V-257809, V-257810, V-257811, V-257812, V-257813, V-257814, V-257815, V-257816, V-257817, V-257818, V-257825, V-257827, V-257828, V-257829, V-257830, V-257831, V-257832, V-257833, V-257834, V-257836, V-257838, V-257839, V-257840, V-257841, V-257842, V-257849, V-257882, V-257883, V-257884, V-257885, V-257886, V-257887, V-257888, V-257889, V-257890, V-257891, V-257892, V-257893, V-257894, V-257895, V-257896, V-257897, V-257898, V-257899, V-257900, V-257901, V-257902, V-257903, V-257904, V-257905, V-257906, V-257907, V-257908, V-257909, V-257910, V-257911, V-257912, V-257913, V-257914, V-257915, V-257916, V-257917, V-257918, V-257919, V-257920, V-257921, V-257922, V-257923, V-257924, V-257925, V-257926, V-257927, V-257928, V-257929, V-257930, V-257933, V-257934, V-257935, V-257936, V-257939, V-257940, V-257942, V-257943, V-257944, V-257948, V-257951, V-257952, V-257953, V-257954, V-257957, V-257958, V-257959, V-257960, V-257961, V-257962, V-257963, V-257964, V-257965, V-257966, V-257967, V-257968, V-257969, V-257970, V-257971, V-257972, V-257973, V-257974, V-257975, V-257976, V-257977, V-257978, V-257979, V-257980, V-257982, V-257983, V-257985, V-257987, V-257988, V-257992, V-257993, V-257994, V-257995, V-257996, V-257997, V-257998, V-257999, V-258000, V-258001, V-258002, V-258003, V-258004, V-258005, V-258006, V-258007, V-258008, V-258009, V-258010, V-258011, V-258028, V-258034, V-258035, V-258038, V-258039, V-258040, V-258041, V-258043, V-258046, V-258049, V-258052, V-258054, V-258055, V-258056, V-258057, V-258060, V-258063, V-258064, V-258065, V-258066, V-258068, V-258070, V-258071, V-258072, V-258073, V-258074, V-258075, V-258077, V-258079, V-258080, V-258081, V-258082, V-258083, V-258084, V-258085, V-258088, V-258089, V-258090, V-258091, V-258092, V-258093, V-258095, V-258097, V-258098, V-258099, V-258100, V-258101, V-258102, V-258103, V-258104, V-258105, V-258107, V-258108, V-258109, V-258110, V-258111, V-258112, V-258113, V-258114, V-258115, V-258116, V-258117, V-258118, V-258119, V-258120, V-258122, V-258123, V-258124, V-258125, V-258126, V-258128, V-258129, V-258130, V-258133, V-258137, V-258140, V-258141, V-258142, V-258144, V-258145, V-258146, V-258147, V-258148, V-258150, V-258151, V-258152, V-258153, V-258154, V-258156, V-258157, V-258158, V-258159, V-258160, V-258161, V-258162, V-258163, V-258164, V-258165, V-258166, V-258167, V-258168, V-258169, V-258170, V-258171, V-258172, V-258175, V-258176, V-258177, V-258178, V-258179, V-258180, V-258181, V-258182, V-258183, V-258184, V-258185, V-258186, V-258187, V-258188, V-258189, V-258190, V-258191, V-258192, V-258193, V-258194, V-258195, V-258196, V-258197, V-258198, V-258199, V-258200, V-258201, V-258202, V-258203, V-258204, V-258205, V-258206, V-258207, V-258208, V-258209, V-258210, V-258211, V-258212, V-258213, V-258214, V-258215, V-258216, V-258217, V-258218, V-258219, V-258220, V-258221, V-258222, V-258223, V-258224,

V-258225, V-258226, V-258227, V-258228, V-258229, V-258232, V-258233, V-258234, V-258237, V-258239, V-258240, V-270174, V-270175, V-270176, V-270177, V-272488 und V-274878

Amazon Linux 2023 STIG Version 1 Release 1

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (Low) unterstützt, sowie:

V-273995, V-274000, V-274001, V-274002, V-274003, V-274004, V-274005, V-274006, V-274008, V-274009, V-274010, V-274011, V-274012, V-274013, V-274014, V-274017, V-274018, V-274019, V-274020, V-274021, V-274022, V-274023, V-274024, V-274026, V-274027, V-274028, V-274030, V-274031, V-274032, V-274033, V-274034, V-274035, V-274036, V-274037, V-274040, V-274041, V-274042, V-274044, V-274045, V-274047, V-274048, V-274049, V-274050, V-274051, V-274053, V-274054, V-274059, V-274061, V-274062, V-274065, V-274069, V-274070, V-274071, V-274072, V-274073, V-274074, V-274075, V-274076, V-274077, V-274078, V-274079, V-274081, V-274082, V-274083, V-274084, V-274085, V-274086, V-274087, V-274088, V-274089, V-274090, V-274091, V-274092, V-274093, V-274094, V-274095, V-274096, V-274097, V-274098, V-274099, V-274100, V-274101, V-274102, V-274103, V-274104, V-274105, V-274106, V-274107, V-274108, V-274109, V-274110, V-274111, V-274112, V-274113, V-274114, V-274115, V-274116, V-274117, V-274119, V-274120, V-274121, V-274122, V-274123, V-274124, V-274125, V-274126, V-274127, V-274128, V-274129, V-274130, V-274131, V-274132, V-274133, V-274134, V-274135, V-274136, V-274137, V-274138, V-274139, V-274140, V-274142, V-274143, V-274144, V-274145, V-274147, V-274149, V-274151, V-274152, V-274154, V-274155, V-274156, V-274157, V-274160, V-274161, V-274162, V-274164, V-274165, V-274166, V-274167, V-274168, V-274169, V-274170, V-274173, V-274174, V-274177, V-274181, V-274182, V-274185 und V-274187

SLES 12 STIG Version 3 Release 3

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (Low) unterstützt, sowie:

V-217102, V-217105, V-217110, V-217116, V-217117, V-217118, V-217119, V-217120, V-217121, V-217122, V-217124, V-217125, V-217126, V-217127, V-217128, V-217130, V-217134, V-217138, V-217143, V-217147, V-217152, V-217153, V-217154, V-217155, V-217156, V-217158, V-217161, V-217163, V-217166, V-217167, V-217168, V-217169, V-217170, V-217171, V-217182, V-217183, V-217188, V-217190, V-217191, V-217194, V-217195, V-217196, V-217197, V-217200, V-217201, V-217202, V-217203, V-217204, V-217205, V-217206, V-217207, V-217208, V-217210, V-217217, V-217218, V-217223, V-217227, V-217230, V-217240, V-217241, V-217242, V-217243, V-217244,

V-217245, V-217246, V-217247, V-217248, V-217249, V-217250, V-217251, V-217252, V-217253, V-217254, V-217255, V-217257, V-217258, V-217260, V-217265, V-217266, V-217267, V-217269, V-217272, V-217273, V-217274, V-217275, V-217276, V-217277, V-217278, V-217279, V-217280, V-217283, V-217284, V-217286, V-217287, V-217288, V-217289, V-217290, V-217291, V-217292, V-217293, V-217294, V-217295, V-217296, V-217299, V-217300, V-217301, V-217302, V-233308, V-237606, V-237607, V-237608, V-237609, V-237610, V-237611, V-237612, V-237613, V-237614, V-237615, V-237616, V-237617, V-237618, V-237619, V-237620, V-237621, V-237622, V-237623, V-251720, V-251722, V-255914 und V-256981

SLES 15 STIG Version 2 Release 5

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (Low) unterstützt, sowie:

V-234802, V-234807, V-234808, V-234809, V-234813, V-234815, V-234817, V-234821, V-234822, V-234823, V-234825, V-234827, V-234828, V-234829, V-234830, V-234832, V-234833, V-234834, V-234835, V-234836, V-234837, V-234838, V-234839, V-234840, V-234841, V-234842, V-234843, V-234844, V-234845, V-234848, V-234854, V-234855, V-234856, V-234857, V-234858, V-234861, V-234862, V-234863, V-234869, V-234870, V-234875, V-234880, V-234881, V-234882, V-234883, V-234884, V-234885, V-234886, V-234887, V-234888, V-234889, V-234891, V-234895, V-234896, V-234897, V-234899, V-234900, V-234901, V-234902, V-234903, V-234904, V-234906, V-234910, V-234911, V-234912, V-234913, V-234914, V-234918, V-234924, V-234928, V-234932, V-234937, V-234938, V-234939, V-234940, V-234941, V-234942, V-234943, V-234944, V-234945, V-234946, V-234947, V-234948, V-234949, V-234950, V-234951, V-234952, V-234954, V-234956, V-234957, V-234958, V-234959, V-234961, V-234962, V-234964, V-234966, V-234969, V-234973, V-234975, V-234976, V-234977, V-234978, V-234979, V-234981, V-234982, V-234983, V-234991, V-235002, V-235003, V-235007, V-235008, V-235009, V-235010, V-235013, V-235014, V-235015, V-235016, V-235017, V-235018, V-235019, V-235020, V-235021, V-235022, V-235023, V-235024, V-235025, V-235026, V-235028, V-235029, V-235030, V-251724, V-255920, V-256983 und V-274879

Ubuntu 18.04 STIG Version 2 Release 15

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (Low) unterstützt, sowie:

V-219149, V-219155, V-219156, V-219160, V-219166, V-219168, V-219176, V-219181, V-219184, V-219186, V-219188, V-219189, V-219190, V-219191, V-219192, V-219193, V-219194, V-219195, V-219196, V-219197, V-219198, V-219199, V-219200, V-219201, V-219202, V-219203, V-219204, V-219205, V-219206, V-219207, V-219208, V-219209, V-219213, V-219214, V-219215, V-219216,

V-219217, V-219218, V-219219, V-219220, V-219221, V-219222, V-219223, V-219224, V-219225, V-219226, V-219227, V-219228, V-219229, V-219230, V-219231, V-219232, V-219233, V-219234, V-219235, V-219236, V-219238, V-219239, V-219240, V-219241, V-219242, V-219243, V-219244, V-219250, V-219254, V-219257, V-219263, V-219264, V-219265, V-219266, V-219267, V-219268, V-219269, V-219270, V-219271, V-219272, V-219273, V-219274, V-219275, V-219276, V-219277, V-219279, V-219281, V-219287, V-219291, V-219296, V-219297, V-219298, V-219299, V-219300, V-219303, V-219304, V-219306, V-219309, V-219310, V-219311, V-219315, V-219318, V-219319, V-219323, V-219326, V-219328, V-219330, V-219331, V-219335, V-219336, V-219337, V-219338, V-219339, V-219342, V-219344, V-233779, V-233780 und V-255906

Ubuntu 20.04 STIG Version 2 Release 3

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (Low) unterstützt, sowie:

V-238200, V-238205, V-238207, V-238209, V-238210, V-238211, V-238212, V-238213, V-238220, V-238225, V-238227, V-238228, V-238229, V-238230, V-238231, V-238232, V-238236, V-238238, V-238239, V-238240, V-238241, V-238242, V-238244, V-238245, V-238246, V-238247, V-238248, V-238249, V-238250, V-238251, V-238252, V-238253, V-238254, V-238255, V-238256, V-238257, V-238258, V-238264, V-238268, V-238271, V-238277, V-238278, V-238279, V-238280, V-238281, V-238282, V-238283, V-238284, V-238285, V-238286, V-238287, V-238288, V-238289, V-238290, V-238291, V-238292, V-238293, V-238294, V-238295, V-238297, V-238298, V-238299, V-238300, V-238301, V-238302, V-238303, V-238304, V-238309, V-238310, V-238315, V-238316, V-238317, V-238318, V-238319, V-238320, V-238324, V-238325, V-238329, V-238330, V-238333, V-238334, V-238337, V-238338, V-238339, V-238340, V-238341, V-238342, V-238343, V-238344, V-238345, V-238346, V-238347, V-238348, V-238349, V-238350, V-238351, V-238352, V-238353, V-238355, V-238356, V-238359, V-238360, V-238369, V-238370, V-238371, V-238376, V-238377, V-238378, V-251505, V-255912, V-274852 und V-274853

Ubuntu 22.04 STIG Version 2 Release 5

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (Low) unterstützt, sowie:

V-260471, V-260473, V-260474, V-260475, V-260477, V-260478, V-260485, V-260486, V-260487, V-260488, V-260489, V-260490, V-260491, V-260492, V-260493, V-260494, V-260495, V-260496, V-260497, V-260498, V-260499, V-260500, V-260505, V-260506, V-260507, V-260508, V-260509, V-260510, V-260511, V-260512, V-260513, V-260514, V-260522, V-260527, V-260528, V-260530, V-260533, V-260534, V-260535, V-260537, V-260538, V-260540, V-260542, V-260543, V-260545,

V-260546, V-260547, V-260553, V-260554, V-260555, V-260556, V-260557, V-260560, V-260561, V-260562, V-260563, V-260564, V-260565, V-260566, V-260567, V-260569, V-260572, V-260573, V-260574, V-260575, V-260576, V-260582, V-260584, V-260585, V-260586, V-260588, V-260589, V-260590, V-260591, V-260594, V-260597, V-260598, V-260599, V-260600, V-260601, V-260602, V-260603, V-260604, V-260605, V-260606, V-260607, V-260608, V-260609, V-260610, V-260611, V-260612, V-260613, V-260614, V-260615, V-260616, V-260617, V-260618, V-260619, V-260620, V-260621, V-260622, V-260623, V-260624, V-260625, V-260626, V-260627, V-260628, V-260629, V-260630, V-260631, V-260632, V-260633, V-260634, V-260635, V-260636, V-260637, V-260638, V-260639, V-260640, V-260641, V-260642, V-260643, V-260644, V-260645, V-260646, V-260647, V-260648, V-260649, V-274862, V-274864 und V-274866

Ubuntu 24.04 STIG Version 1 Release 2

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (Low) unterstützt, sowie:

V-270649, V-270651, V-270652, V-270653, V-270654, V-270656, V-270657, V-270659, V-270660, V-270661, V-270662, V-270663, V-270669, V-270672, V-270673, V-270674, V-270676, V-270678, V-270679, V-270680, V-270681, V-270683, V-270684, V-270685, V-270686, V-270687, V-270688, V-270689, V-270692, V-270693, V-270696, V-270697, V-270698, V-270699, V-270700, V-270701, V-270702, V-270703, V-270704, V-270705, V-270709, V-270715, V-270716, V-270718, V-270720, V-270721, V-270722, V-270723, V-270724, V-270725, V-270726, V-270727, V-270728, V-270729, V-270730, V-270731, V-270732, V-270733, V-270737, V-270739, V-270740, V-270741, V-270742, V-270743, V-270746, V-270750, V-270753, V-270755, V-270756, V-270757, V-270758, V-270759, V-270760, V-270765, V-270766, V-270767, V-270768, V-270769, V-270770, V-270771, V-270772, V-270773, V-270775, V-270776, V-270777, V-270778, V-270779, V-270780, V-270781, V-270782, V-270783, V-270784, V-270785, V-270786, V-270787, V-270788, V-270789, V-270790, V-270791, V-270792, V-270793, V-270794, V-270795, V-270796, V-270797, V-270798, V-270799, V-270800, V-270801, V-270802, V-270803, V-270804, V-270805, V-270806, V-270807, V-270808, V-270809, V-270810, V-270811, V-270812, V-270813, V-270814, V-270815, V-270821, V-270822, V-270823, V-270824, V-270825, V-270826, V-270827, V-270828, V-270829, V-270830, V-270831, V-270832, V-274870, V-274871, V-274872 und V-274873

Linux STIG High (Kategorie I)

Die folgende Liste enthält STIG-Einstellungen, die Amazon EC2 für Ihre Infrastruktur unterstützt. Wenn eine unterstützte Einstellung für Ihre Infrastruktur nicht anwendbar ist, überspringt Amazon EC2 diese Einstellung und fährt fort. Beispielsweise gelten einige STIG-Hardening-Einstellungen möglicherweise nicht für eigenständige Server. Organisationsspezifische Richtlinien können auch

beeinflussen, welche Einstellungen zutreffen, z. B. dass Administratoren die Dokumenteinstellungen überprüfen müssen.

Eine vollständige Liste finden Sie in der STIGs-Dokumentbibliothek. Informationen zum Anzeigen der vollständigen Liste finden Sie unter STIG Viewing Tools.

> **Note**
>
> Die Kategorie Linux STIG High umfasst alle aufgelisteten STIG-Hardening-Einstellungen, die für die Kategorien Linux STIG Medium und Low gelten, zusätzlich zu den STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie I unterstützt.

RHEL 7 STIG Version 3 Release 15

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

- RHEL 7/CentOS 7/AL2

  V-204424, V-204425, V-204442, V-204443, V-204447, V-204448, V-204455, V-204497, V-204502, V-204594, V-204620 und V-204621

RHEL 8 STIG Version 2 Release 4

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

- RHEL 8/CentOS 8

  V-230221, V-230223, V-230226, V-230264, V-230265, V-230283, V-230284, V-230487, V-230492, V-230529, V-230530, V-230531, V-230533, V-230558, V-244540 und V-268322

RHEL 9 STIG Version 2 Release 5

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

- RHEL 9/CentOS Stream 9

V-257784, V-257785, V-257820, V-257821, V-257826, V-257835, V-257955, V-257956, V-257984, V-257986, V-258059, V-258078, V-258094, V-258230, V-258235 und V-258238

Amazon Linux 2023 STIG Version 1 Release 1

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

V-273996, V-273997, V-273999, V-274007, V-274038, V-274039, V-274046, V-274052, V-274057 und V-274153

SLES 12 STIG Version 3 Release 3

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

V-217101, V-217139, V-217141, V-217142, V-217159, V-217160, V-217264, V-217268, V-222386 und V-251721

SLES 15 STIG Version 2 Release 5

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

V-234800, V-234804, V-234818, V-234852, V-234859, V-234860, V-234898, V-234984, V-234985, V-234988, V-234989, V-234990, V-235031, V-235032 und V-251725

Ubuntu 18.04 STIG Version 2 Release 15

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

V-219157, V-219158, V-219177, V-219212, V-219308, V-219314, V-219316, V-251507 und V-264388

Ubuntu 20.04 STIG Version 2 Release 3

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

V-238201, V-238218, V-238219, V-238326, V-238327, V-238380 und V-251504

Ubuntu 22.04 STIG Version 2 Release 5

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

V-260469, V-260482, V-260483, V-260523, V-260524, V-260526, V-260529, V-260539, V-260570, V-260571 und V-260579

Ubuntu 24.04 STIG Version 1 Release 2

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

V-270647, V-270648, V-270665, V-270666, V-270708, V-270711, V-270712, V-270713, V-270714, V-270717 und V-270736

STIG-Hardening-Einstellungen für EC2-Windows-Instances

Amazon EC2 unterstützt STIG-Baselines für die folgenden Windows-Betriebssystemversionen:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

In diesem Abschnitt werden die aktuellen STIG-Einstellungen aufgeführt, die Amazon EC2 für Ihre Windows-Infrastruktur unterstützt, gefolgt von einem Versionsverlaufsprotokoll.

Sie können niedrige, mittlere oder hohe STIG-Einstellungen anwenden.

Windows STIG Low (Kategorie III)

Die folgende Liste enthält STIG-Einstellungen, die Amazon EC2 für Ihre Infrastruktur unterstützt. Wenn eine unterstützte Einstellung für Ihre Infrastruktur nicht anwendbar ist, überspringt Amazon EC2 diese Einstellung und fährt fort. Beispielsweise gelten einige STIG-Hardening-Einstellungen möglicherweise nicht für eigenständige Server. Organisationsspezifische Richtlinien können auch beeinflussen, welche Einstellungen zutreffen, z. B. dass Administratoren die Dokumenteinstellungen überprüfen müssen.

Eine vollständige Liste der Windows-STIGs finden Sie in der STIGs-Dokumentbibliothek. Informationen zum Anzeigen der vollständigen Liste finden Sie unter STIG Viewing Tools.

- Windows Server 2022 STIG Version 2 Release 4

  V-254335, V-254336, V-254337, V-254338, V-254351, V-254357, V-254363 und V-254481
- Windows Server 2019 STIG Version 3 Release 4

  V-205691, V-205819, V-205858, V-205859, V-205860, V-205870, V-205871 und V-205923
- Windows Server 2016 STIG Version 2 Release 10

  V-224916, V-224917, V-224918, V-224919, V-224931, V-224942 und V-225060
- Windows Server 2012 R2 MS STIG Version 3 Release 5

  V-225250, V-225318, V-225319, V-225324, V-225327, V-225328, V-225330, V-225331, V-225332, V-225333, V-225334, V-225335, V-225336, V-225342, V-225343, V-225355, V-225357, V-225358, V-225359, V-225360, V-225362, V-225363, V-225376, V-225392, V-225394, V-225412, V-225459, V-225460, V-225462, V-225468, V-225473, V-225476, V-225479, V-225480, V-225481, V-225482, V-225483, V-225484, V-225485, V-225487, V-225488, V-225489, V-225490, V-225511, V-225514, V-225525, V-225526, V-225536 und V-225537
- Microsoft .NET Framework 4.0 STIG Version 2 Release 6

  Auf das Microsoft .NET Framework werden keine STIG-Einstellungen für Schwachstellen der Kategorie III angewendet.
- Windows Firewall STIG Version 2 Release 2

  V-241994, V-241995, V-241996, V-241999, V-242000, V-242001, V-242006, V-242007 und V-242008
- Internet Explorer 11 STIG Version 2 Release 5

  V-223016, V-223056 und V-223078
- Microsoft Edge STIG Version 2 Release 2 (nur Windows Server 2022)

  V-235727, V-235731, V-235751, V-235752 und V-235765

Windows STIG Medium (Kategorie II)

Die folgende Liste enthält STIG-Einstellungen, die Amazon EC2 für Ihre Infrastruktur unterstützt. Wenn eine unterstützte Einstellung für Ihre Infrastruktur nicht anwendbar ist, überspringt Amazon EC2 diese Einstellung und fährt fort. Beispielsweise gelten einige STIG-Hardening-Einstellungen möglicherweise nicht für eigenständige Server. Organisationsspezifische Richtlinien können auch

beeinflussen, welche Einstellungen zutreffen, z. B. dass Administratoren die Dokumenteinstellungen überprüfen müssen.

Eine vollständige Liste der Windows-STIGs finden Sie in der STIGs-Dokumentbibliothek. Informationen zum Anzeigen der vollständigen Liste finden Sie unter STIG Viewing Tools.

> **Note**
>
> Die Kategorie Windows STIG Medium umfasst alle aufgelisteten STIG-Hardening-Einstellungen, die auf Windows STIG Low (Kategorie III) anwendbar sind, zusätzlich zu den STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie II unterstützt.

- Windows Server 2022 STIG Version 2 Release 4

  Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (Low) unterstützt, sowie:

  V-254247, V-254265, V-254269, V-254270, V-254271, V-254272, V-254273, V-254274, V-254276, V-254277, V-254278, V-254285, V-254286, V-254287, V-254288, V-254289, V-254290, V-254291, V-254292, V-254300, V-254301, V-254302, V-254303, V-254304, V-254305, V-254306, V-254307, V-254308, V-254309, V-254310, V-254311, V-254312, V-254313, V-254314, V-254315, V-254316, V-254317, V-254318, V-254319, V-254320, V-254321, V-254322, V-254323, V-254324, V-254325, V-254326, V-254327, V-254328, V-254329, V-254330, V-254331, V-254332, V-254333, V-254334, V-254339, V-254341, V-254342, V-254344, V-254345, V-254346, V-254347, V-254348, V-254349, V-254350, V-254355, V-254356, V-254356, V-254358, V-254359, V-254360, V-254361, V-254362, V-254364, V-254365, V-254366, V-254367, V-254368, V-254369, V-254370, V-254371, V-254372, V-254373, V-254375, V-254376, V-254377, V-254379, V-254380, V-254382, V-254383, V-254384, V-254431, V-254432, V-254433, V-254434, V-254435, V-254436, V-254438, V-254439, V-254442, V-254443, V-254444, V-254445, V-254449, V-254450, V-254451, V-254452, V-254453, V-254454, V-254455, V-254456, V-254459, V-254460, V-254461, V-254462, V-254463, V-254464, V-254468, V-254470, V-254471, V-254472, V-254473, V-254476, V-254477, V-254478, V-254479, V-254480, V-254482, V-254483, V-254484, V-254485, V-254486, V-254487, V-254488, V-254489, V-254490, V-254493, V-254494, V-254495, V-254497, V-254499, V-254501, V-254502, V-254503, V-254504, V-254505, V-254507, V-254508, V-254509, V-254510, V-254511 und V-254512
- Windows Server 2019 STIG Version 3 Release 4

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (Low) unterstützt, sowie:

V-205625, V-205626, V-205627, V-205629, V-205630, V-205633, V-205634, V-205635, V-205636, V-205637, V-205638, V-205639, V-205643, V-205644, V-205648, V-205649, V-205650, V-205651, V-205652, V-205655, V-205656, V-205659, V-205660, V-205662, V-205671, V-205672, V-205673, V-205675, V-205676, V-205678, V-205679, V-205680, V-205681, V-205682, V-205683, V-205684, V-205685, V-205686, V-205687, V-205688, V-205689, V-205690, V-205692, V-205693, V-205694, V-205697, V-205698, V-205708, V-205709, V-205712, V-205714, V-205716, V-205717, V-205718, V-205719, V-205720, V-205722, V-205729, V-205730, V-205733, V-205747, V-205751, V-205752, V-205754, V-205756, V-205758, V-205759, V-205760, V-205761, V-205762, V-205764, V-205765, V-205766, V-205767, V-205768, V-205769, V-205770, V-205771, V-205772, V-205773, V-205774, V-205775, V-205776, V-205777, V-205778, V-205779, V-205780, V-205781, V-205782, V-205783, V-205784, V-205795, V-205796, V-205797, V-205798, V-205801, V-205808, V-205809, V-205810, V-205811, V-205812, V-205813, V-205814, V-205815, V-205816, V-205817, V-205821, V-205822, V-205823, V-205824, V-205825, V-205826, V-205827, V-205828, V-205830, V-205832, V-205833, V-205834, V-205835, V-205836, V-205837, V-205838, V-205839, V-205840, V-205841, V-205842, V-205861, V-205863, V-205865, V-205866, V-205867, V-205868, V-205869, V-205872, V-205873, V-205874, V-205911, V-205912, V-205915, V-205916, V-205917, V-205918, V-205920, V-205921, V-205922, V-205924, V-205925, V-236001 und V-257503

- Windows Server 2016 STIG Version 2 Release 10

  Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (Low) unterstützt, sowie:

  V-224850, V-224852, V-224853, V-224854, V-224855, V-224856, V-224857, V-224858, V-224859, V-224866, V-224867, V-224868, V-224869, V-224870, V-224871, V-224872, V-224873, V-224881, V-224882, V-224883, V-224884, V-224885, V-224886, V-224887, V-224888, V-224889, V-224890, V-224891, V-224892, V-224893, V-224894, V-224895, V-224896, V-224897, V-224898, V-224899, V-224900, V-224901, V-224902, V-224903, V-224904, V-224905, V-224906, V-224907, V-224908, V-224909, V-224910, V-224911, V-224912, V-224913, V-224914, V-224915, V-224920, V-224922, V-224924, V-224925, V-224926, V-224927, V-224928, V-224929, V-224930, V-224935, V-224936, V-224937, V-224938, V-224939, V-224940, V-224941, V-224943, V-224944, V-224945, V-224946, V-224947, V-224948, V-224949, V-224951, V-224952, V-224953, V-224955, V-224956, V-224957, V-224959, V-224960, V-224962, V-224963, V-225010, V-225013, V-225014, V-225015, V-225016, V-225017, V-225018, V-225019, V-225021, V-225022, V-225023, V-225024, V-225028, V-225029, V-225030, V-225031, V-225032, V-225033, V-225034, V-225035, V-225038, V-225039, V-225040,

V-225041, V-225042, V-225043, V-225047, V-225049, V-225050, V-225051, V-225052, V-225055, V-225056, V-225057, V-225058, V-225059, V-225061, V-225062, V-225063, V-225064, V-225065, V-225066, V-225067, V-225068, V-225069, V-225072, V-225073, V-225074, V-225076, V-225078, V-225080, V-225081, V-225082, V-225083, V-225084, V-225086, V-225087, V-225088, V-225089, V-225092, V-225093, V-236000 und V-257502

- Windows Server 2012 R2 MS STIG Version 3 Release 5

  Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (Low) unterstützt, sowie:

  V-225239, V-225259, V-225260, V-225261, V-225263, V-225264, V-225265, V-225266, V-225267, V-225268, V-225269, V-225270, V-225271, V-225272, V-225273, V-225275, V-225276, V-225277, V-225278, V-225279, V-225280, V-225281, V-225282, V-225283, V-225284, V-225285, V-225286, V-225287, V-225288, V-225289, V-225290, V-225291, V-225292, V-225293, V-225294, V-225295, V-225296, V-225297, V-225298, V-225299, V-225300, V-225301, V-225302, V-225303, V-225304, V-225305, V-225314, V-225315, V-225316, V-225317, V-225325, V-225326, V-225329, V-225337, V-225338, V-225339, V-225340, V-225341, V-225344, V-225345, V-225346, V-225347, V-225348, V-225349, V-225350, V-225351, V-225352, V-225353, V-225356, V-225367, V-225368, V-225369, V-225370, V-225371, V-225372, V-225373, V-225374, V-225375, V-225377, V-225378, V-225379, V-225380, V-225381, V-225382, V-225383, V-225384, V-225385, V-225386, V-225389, V-225391, V-225393, V-225395, V-225397, V-225398, V-225400, V-225401, V-225402, V-225404, V-225405, V-225406, V-225407, V-225408, V-225409, V-225410, V-225411, V-225413, V-225414, V-225415, V-225441, V-225442, V-225443, V-225448, V-225452, V-225453, V-225454, V-225455, V-225456, V-225457, V-225458, V-225461, V-225463, V-225464, V-225469, V-225470, V-225471, V-225472, V-225474, V-225475, V-225477, V-225478, V-225486, V-225494, V-225500, V-225501, V-225502, V-225503, V-225504, V-225506, V-225508, V-225509, V-225510, V-225513, V-225515, V-225516, V-225517, V-225518, V-225519, V-225520, V-225521, V-225522, V-225523, V-225524, V-225527, V-225528, V-225529, V-225530, V-225531, V-225532, V-225533, V-225534, V-225535, V-225538, V-225539, V-225540, V-225541, V-225542, V-225543, V-225544, V-225545, V-225546, V-225548, V-225549, V-225550, V-225551, V-225553, V-225554, V-225555, V-225557, V-225558, V-225559, V-225560, V-225561, V-225562, V-225563, V-225564, V-225565, V-225566, V-225567, V-225568, V-225569, V-225570, V-225571, V-225572, V-225573 und V-225574

- Microsoft .NET Framework STIG 4.0 Version 2 Release 6

  Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (Low) unterstützt, sowie:

V-225238

- Windows Firewall STIG Version 2 Release 2

  Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (Low) unterstützt, sowie:

  V-241989, V-241990, V-241991, V-241993, V-241993, V-241998 und V-242003

- Internet Explorer 11 STIG Version 2 Release 5

  Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie III (Low) unterstützt, sowie:

  V-223015, V-223017, V-223018, V-223019, V-223020, V-223021, V-223022, V-223023, V-223024, V-223025, V-223026, V-223027, V-223028, V-223029, V-223030, V-223031, V-223032, V-223033, V-223034, V-223035, V-223036, V-223037, V-223038, V-223039, V-223040, V-223041, V-223042, V-223043, V-223044, V-223045, V-223046, V-223048, V-223049, V-223050, V-223051, V-223052, V-223053, V-223054, V-223055, V-223057, V-223058, V-223059, V-223060, V-223061, V-223062, V-223063, V-223064, V-223065, V-223066, V-223067, V-223068, V-223069, V-223070, V-223071, V-223072, V-223073, V-223074, V-223075, V-223076, V-223077, V-223079, V-223080, V-223081, V-223082, V-223083, V-223084, V-223085, V-223086, V-223087, V-223088, V-223089, V-223090, V-223091, V-223092, V-223093, V-223094, V-223095, V-223096, V-223097, V-223098, V-223099, V-223100, V-223101, V-223102, V-223103, V-223104, V-223105, V-223106, V-223107, V-223108, V-223109, V-223110, V-223111, V-223112, V-223113, V-223114, V-223115, V-223116, V-223117, V-223118, V-223119, V-223120, V-223121, V-223122, V-223123, V-223124, V-223125, V-223126, V-223127, V-223128, V-223129, V-223130, V-223131, V-223132, V-223133, V-223134, V-223135, V-223136, V-223137, V-223138, V-223139, V-223140, V-223141, V-223142, V-223143, V-223144, V-223145, V-223146, V-223147, V-223148, V-223149, V-250540 und V-250541

- Microsoft Edge STIG Version 2 Release 2 (nur Windows Server 2022)

  V-235720, V-235721, V-235723, V-235724, V-235725, V-235726, V-235728, V-235729, V-235730, V-235732, V-235733, V-235734, V-235735, V-235736, V-235737, V-235738, V-235739, V-235740, V-235741, V-235742, V-235743, V-235744, V-235745, V-235746, V-235747, V-235748, V-235749, V-235750, V-235754, V-235756, V-235760, V-235761, V-235763, V-235764, V-235766, V-235767, V-235768, V-235769, V-235770, V-235771, V-235772, V-235773, V-235774 und V-246736

- Microsoft Defender STIG Version 2 Release 4

V-213427, V-213429, V-213430, V-213431, V-213432, V-213433, V-213434, V-213435, V-213436, V-213437, V-213438, V-213439, V-213440, V-213441, V-213442, V-213443, V-213444, V-213445, V-213446, V-213447, V-213448, V-213449, V-213450, V-213451, V-213455, V-213464, V-213465 und V-213466

Windows STIG High (Kategorie I)

Die folgende Liste enthält STIG-Einstellungen, die Amazon EC2 für Ihre Infrastruktur unterstützt. Wenn eine unterstützte Einstellung für Ihre Infrastruktur nicht anwendbar ist, überspringt Amazon EC2 diese Einstellung und fährt fort. Beispielsweise gelten einige STIG-Hardening-Einstellungen möglicherweise nicht für eigenständige Server. Organisationsspezifische Richtlinien können auch beeinflussen, welche Einstellungen zutreffen, z. B. dass Administratoren die Dokumenteinstellungen überprüfen müssen.

Eine vollständige Liste der Windows-STIGs finden Sie in der STIGs-Dokumentbibliothek. Informationen zum Anzeigen der vollständigen Liste finden Sie unter STIG Viewing Tools.

> **Note**
>
> Die Kategorie Windows STIG High umfasst alle aufgelisteten STIG-Hardening-Einstellungen, die für die Kategorien Windows STIG Medium und Low gelten, zusätzlich zu den STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorie I unterstützt.

- Windows Server 2022 STIG Version 2 Release 4

  V-254293, V-254352, V-254353, V-254354, V-254374, V-254378, V-254381, V-254446, V-254465, V-254466, V-254467, V-254469, V-254474, V-254475 und V-254500

- Windows Server 2019 STIG Version 3 Release 4

  Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

  V-205653, V-205654, V-205711, V-205713, V-205724, V-205725, V-205757, V-205802, V-205804, V-205805, V-205806, V-205849, V-205908, V-205913, V-205914 und V-205919

- Windows Server 2016 STIG Version 2 Release 10

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

V-224874, V-224932, V-224933, V-224934, V-224954, V-224958, V-224961, V-225025, V-225044, V-225045, V-225046, V-225048, V-225053, V-225054 und V-225079

- Windows Server 2012 R2 MS STIG Version 3 Release 5

  Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

  V-225274, V-225354, V-225364, V-225365, V-225366, V-225390, V-225396, V-225399, V-225444, V-225449, V-225491, V-225492, V-225493, V-225496, V-225497, V-225498, V-225505, V-225507, V-225547, V-225552 und V-225556

- Microsoft .NET Framework STIG 4.0 Version 2 Release 6

  Enthält alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) für das Microsoft.NET Framework unterstützt. Für Schwachstellen der Kategorie I werden keine zusätzlichen STIG-Einstellungen angewendet.

- Windows Firewall STIG Version 2 Release 2

  Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

  V-241992, V-241997 und V-242002

- Internet Explorer 11 STIG Version 2 Release 5

  Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

  V-252910

- Microsoft Edge STIG Version 2 Release 2 (nur Windows Server 2022)

  Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

  V-235758 und V-235759

- Microsoft Defender STIG Version 2 Release 4

Beinhaltet alle STIG-Hardening-Einstellungen, die Amazon EC2 für Schwachstellen der Kategorien II und III (Medium und Low) unterstützt, sowie:

V-213426, V-213452 und V-213453

STIG-Hardening-Skripte zum Herunterladen

Amazon bündelt STIG-Hardening-Skripte für jede Version zu betriebssystembezogenen Paketen zusammen. Pakete sind Archivdateien, die für das Zielbetriebssystem geeignet sind, auf das sie heruntergeladen und ausgeführt werden. Linux-Skriptpakete werden als TAR-Dateien (Dateierweiterung .tgz) gespeichert. Windows-Skriptpakete werden als ZIP-Dateien (Dateierweiterung .zip) gespeichert.

Amazon speichert die Skriptpakete in jeder AWS-Region im S3-`STIG`-Bucket von EC2 Windows. Die Linux-Pakete haben keinen separaten Bucket. Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.

Themen

- IAM-Voraussetzungen für STIG-Downloads
- Details zum STIG-Download-Paket
- Linux-STIG-Versionsverlauf
- Versionsverlauf für Windows-STIG

IAM-Voraussetzungen für STIG-Downloads

Die IAM-Rolle, die Sie Ihrem Instance-Profil zuordnen, muss über `s3:GetObject`-Berechtigungen zum Herunterladen der Skriptpakete von Amazon S3 verfügen. Sie können der Instance-Profilrolle die folgende Beispielrichtlinie anfügen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DownloadSTIGScriptBundles",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
```

```
            ],
            "Resource": [
                "arn:aws:s3:::aws-windows-downloads*/STIG/*.zip",
                "arn:aws:s3:::aws-windows-downloads*/STIG/*.tgz"
            ]
        }
    ]
}
```

Um das Beispiel für eine STIG-Download-Richtlinie zu Ihrer Instance-Profilrolle als Inline-Richtlinie hinzuzufügen, befolgen Sie das Verfahren Aktualisierung der Berechtigungsrichtlinie für eine Rolle im Benutzerhandbuch für AWS Identity and Access Management. Weitere Informationen zu Instance-Profilen finden Sie unter Instance-Profile verwenden.

Details zum STIG-Download-Paket

> **Important**
>
> Mit wenigen Ausnahmen installieren die STIG-Hardening-Skripts, die das Systems-Manager-Dokument herunterlädt, keine Pakete von Drittanbietern. Wenn Drittanbieter-Pakete bereits auf der Instance installiert sind oder der Parameter `InstallPackage` auf `yes` gesetzt ist, werden verwandte STIGs angewendet, die Amazon EC2 für dieses Paket unterstützt.

Wenn Sie den folgenden Befehl von der AWS CLI ausführen, lädt Amazon S3 die neueste STIG-Hardening-Skriptpaketdatei aus dem Bucket herunter.

```
aws s3 cp s3://aws-windows-downloads-region/STIG/operating system/Latest/bundle-
name destination-directory
```

Beispiel: In ein temporäres Verzeichnis herunterladen

Dieses Beispiel zeigt ein Linux-Paket, das in das `/tmp`-Verzeichnis heruntergeladen wurde

```
aws s3 cp s3://aws-windows-downloads-us-east-1/STIG/Linux/
Latest/LinuxAWSConfigureSTIG.tgz /tmp
```

Im Folgenden finden Sie Muster und Beispiele für Speicherpfade und Paketdateinamen für Download-Dateien:

Dateispeicherpfad des Downloads

`s3://aws-windows-downloads-<region>/STIG/<operating system>/Latest/<bundle file name>`

Pfadvariablen des Downloads

region

AWS-Region (Jede Region hat ihren eigenen Download-Bucket.)

operating system

Die Betriebssystemplattform der Instance, auf die STIGs angewendet werden – entweder `Linux` oder `Windows`.

bundle file name

Das Format ist *<Name des Betriebssystempakets>*.*<Dateierweiterung>*.

os bundle name

Das Standardnamenspräfix für das Betriebssystempaket ist entweder `LinuxAWSConfigureSTIG` oder `AWSConfigureSTIG`. Um die Abwärtskompatibilität zu gewährleisten, enthält der Download für Windows kein Plattformpräfix.

file extension

Komprimiertes Dateiformat `tgz` (Linux) oder `zip` (Windows).

Beispiele für Paketdateinamen

- `LinuxAWSConfigureSTIG.tgz`
- `AWSConfigureSTIG.zip`

Linux-STIG-Versionsverlauf

In diesem Abschnitt wird der Versionsverlauf für Linux-Skriptpakete protokolliert, die vierteljährlich aktualisiert werden. Um die Änderungen und veröffentlichten Versionen für ein Quartal zu sehen, wählen Sie den Titel aus, um die Informationen zu erweitern. Wenn es für das Quartal keine Änderungen gibt, können Sie dies am Titel erkennen.

Änderungen im dritten Quartal 2025 – 04.09.2025:

Unterstützung für das Betriebssystem SUSE Linux Enterprise Server (SLES) und Amazon Linux 2023 wurde hinzugefügt. Die folgenden STIG-Versionen wurden aktualisiert und STIGS für die Version des dritten Quartals 2025 für alle Compliance-Stufen (niedrig/mittel/hoch) angewendet:

STIG-Build-Linux Version 1.0.x

- RHEL 7 STIG Version 3 Release 15
- RHEL 8 STIG Version 2 Release 4
- RHEL 9 STIG Version 2 Release 5
- Amazon Linux 2023 STIG Version 1 Release 1
- SLES 12 STIG Version 3 Release 3
- SLES 15 STIG Version 2 Release 5
- Ubuntu 18.04 STIG Version 2 Release 15
- Ubuntu 20.04 STIG Version 2 Release 3
- Ubuntu 22.04 STIG Version 2 Release 5
- Ubuntu 24.04 STIG Version 1 Release 2

Änderungen im zweiten Quartal 2025 – 26.06.2025:

Die folgenden STIG-Versionen wurden aktualisiert und STIGS für die Version des zweiten Quartals 2025 angewendet:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Release 15
- RHEL 8 STIG Version 2 Release 3
- RHEL 9 STIG Version 2 Release 4
- Ubuntu 18.04 STIG Version 2 Release 15
- Ubuntu 20.04 STIG Version 2 Release 2
- Ubuntu 22.04 STIG Version 2 Release 4
- Ubuntu 24.04 STIG Version 1 Release 1

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Release 15
- RHEL 8 STIG Version 2 Release 3
- RHEL 9 STIG Version 2 Release 4

- Ubuntu 18.04 STIG Version 2 Release 15
- Ubuntu 20.04 STIG Version 2 Release 2
- Ubuntu 22.04 STIG Version 2 Release 4
- Ubuntu 24.04 STIG Version 1 Release 1

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Release 15
- RHEL 8 STIG Version 2 Release 3
- RHEL 9 STIG Version 2 Release 4
- Ubuntu 18.04 STIG Version 2 Release 15
- Ubuntu 20.04 STIG Version 2 Release 2
- Ubuntu 22.04 STIG Version 2 Release 4
- Ubuntu 24.04 STIG Version 1 Release 1

Änderungen im ersten Quartal 2025 – 11.04.2025:

Die folgenden STIG-Versionen wurden aktualisiert, STIGS auf die Version des ersten Quartals 2025 angewendet und Unterstützung für Ubuntu 24.04 hinzugefügt:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Release 15
- RHEL 8 STIG Version 2 Release 2
- RHEL 9 STIG Version 2 Release 3
- Ubuntu 18.04 STIG Version 2 Release 15
- Ubuntu 20.04 STIG Version 2 Release 2
- Ubuntu 22.04 STIG Version 2 Release 3
- Ubuntu 24.04 STIG Version 1 Release 1

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Release 15
- RHEL 8 STIG Version 2 Release 2

- RHEL 9 STIG Version 2 Release 3
- Ubuntu 18.04 STIG Version 2 Release 15
- Ubuntu 20.04 STIG Version 2 Release 2
- Ubuntu 22.04 STIG Version 2 Release 3
- Ubuntu 24.04 STIG Version 1 Release 1

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Release 15
- RHEL 8 STIG Version 2 Release 2
- RHEL 9 STIG Version 2 Release 3
- Ubuntu 18.04 STIG Version 2 Release 15
- Ubuntu 20.04 STIG Version 2 Release 2
- Ubuntu 22.04 STIG Version 2 Release 3
- Ubuntu 24.04 STIG Version 1 Release 1

Änderungen im vierten Quartal 2024 – 10.12.2024:

Die folgenden STIG-Versionen wurden aktualisiert, STIGS für die Version des vierten Quartals 2024 angewendet und Informationen zu zwei neuen Eingabeparametern für die Linux-Komponenten hinzugefügt:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Release 15
- RHEL 8 STIG Version 2 Release 1
- RHEL 9 STIG Version 2 Release 2
- Ubuntu 18.04 STIG Version 2 Release 15
- Ubuntu 20.04 STIG Version 2 Release 1
- Ubuntu 22.04 STIG Version 2 Release 2

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Release 15

- RHEL 8 STIG Version 2 Release 1
- RHEL 9 STIG Version 2 Release 2
- Ubuntu 18.04 STIG Version 2 Release 15
- Ubuntu 20.04 STIG Version 2 Release 1
- Ubuntu 22.04 STIG Version 2 Release 2

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Release 15
- RHEL 8 STIG Version 2 Release 1
- RHEL 9 STIG Version 2 Release 2
- Ubuntu 18.04 STIG Version 2 Release 15
- Ubuntu 20.04 STIG Version 2 Release 1
- Ubuntu 22.04 STIG Version 2 Release 2

Änderungen im dritten Quartal 2024 – 04.10.2024 (keine Änderungen):

Für die Version des dritten Quartals 2024 gab es keine Änderungen für die Linux-Komponenten-STIGS.

Änderungen im zweiten Quartal 2024 – 10.05.2024:

Die STIG-Versionen wurden aktualisiert und STIGS für die Version des zweiten Quartals 2024 angewendet. Außerdem wurde die Unterstützung für RHEL 9, CentOS Stream 9 und Ubuntu 22.04 wie folgt hinzugefügt:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Release 14
- RHEL 8 STIG Version 1 Release 14
- RHEL 9 STIG Version 1 Release 3
- Ubuntu 18.04 STIG Version 2 Release 14
- Ubuntu 20.04 STIG Version 1 Release 12
- Ubuntu 22.04 STIG Version 1 Release 1

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Release 14
- RHEL 8 STIG Version 1 Release 14
- RHEL 9 STIG Version 1 Release 3
- Ubuntu 18.04 STIG Version 2 Release 14
- Ubuntu 20.04 STIG Version 1 Release 12
- Ubuntu 22.04 STIG Version 1 Release 1

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Release 14
- RHEL 8 STIG Version 1 Release 14
- RHEL 9 STIG Version 1 Release 3
- Ubuntu 18.04 STIG Version 2 Release 14
- Ubuntu 20.04 STIG Version 1 Release 12
- Ubuntu 22.04 STIG Version 1 Release 1

Änderungen im ersten Quartal 2024 – 06.02.2024:

Die STIG-Versionen wurden aktualisiert und STIGS für die Version des ersten Quartals 2024 wie folgt angewendet:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Release 14
- RHEL 8 STIG Version 1 Release 13
- Ubuntu 18.04 STIG Version 2 Release 13
- Ubuntu 20.04 STIG Version 1 Release 11

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Release 14
- RHEL 8 STIG Version 1 Release 13

- Ubuntu 18.04 STIG Version 2 Release 13
- Ubuntu 20.04 STIG Version 1 Release 11

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Release 14
- RHEL 8 STIG Version 1 Release 13
- Ubuntu 18.04 STIG Version 2 Release 13
- Ubuntu 20.04 STIG Version 1 Release 11

Änderungen im vierten Quartal 2023 – 07.12.2023:

Die STIG-Versionen wurden aktualisiert und STIGS für die Version des vierten Quartals 2023 wie folgt angewendet:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Release 13
- RHEL 8 STIG Version 1 Release 12
- Ubuntu 18.04 STIG Version 2 Release 12
- Ubuntu 20.04 STIG Version 1 Release 10

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Release 13
- RHEL 8 STIG Version 1 Release 12
- Ubuntu 18.04 STIG Version 2 Release 12
- Ubuntu 20.04 STIG Version 1 Release 10

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Release 13
- RHEL 8 STIG Version 1 Release 12
- Ubuntu 18.04 STIG Version 2 Release 12

- Ubuntu 20.04 STIG Version 1 Release 10

Änderungen im dritten Quartal 2023 – 04.10.2023:

Die STIG-Versionen wurden aktualisiert und STIGS für die Version des dritten Quartals 2023 wie folgt angewendet:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Release 12
- RHEL 8 STIG Version 1 Release 11
- Ubuntu 18.04 STIG Version 2 Release 11
- Ubuntu 20.04 STIG Version 1 Release 9

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Release 12
- RHEL 8 STIG Version 1 Release 11
- Ubuntu 18.04 STIG Version 2 Release 11
- Ubuntu 20.04 STIG Version 1 Release 9

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Release 12
- RHEL 8 STIG Version 1 Release 11
- Ubuntu 18.04 STIG Version 2 Release 11
- Ubuntu 20.04 STIG Version 1 Release 9

Änderungen im zweiten Quartal 2023 – 03.05.2023:

Die STIG-Versionen wurden aktualisiert und STIGS für die Version des zweiten Quartals 2023 wie folgt angewendet:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Release 11

- RHEL 8 STIG Version 1 Release 10
- Ubuntu 18.04 STIG Version 2 Release 11
- Ubuntu 20.04 STIG Version 1 Release 8

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Release 11
- RHEL 8 STIG Version 1 Release 10
- Ubuntu 18.04 STIG Version 2 Release 11
- Ubuntu 20.04 STIG Version 1 Release 8

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Release 11
- RHEL 8 STIG Version 1 Release 10
- Ubuntu 18.04 STIG Version 2 Release 11
- Ubuntu 20.04 STIG Version 1 Release 8

Änderungen im ersten Quartal 2023 – 27.03.2023:

Die STIG-Versionen wurden aktualisiert und STIGS für die Version des ersten Quartals 2023 wie folgt angewendet:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Release 10
- RHEL 8 STIG Version 1 Release 9
- Ubuntu 18.04 STIG Version 2 Release 10
- Ubuntu 20.04 STIG Version 1 Release 7

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Release 10
- RHEL 8 STIG Version 1 Release 9

- Ubuntu 18.04 STIG Version 2 Release 10
- Ubuntu 20.04 STIG Version 1 Release 7

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Release 10
- RHEL 8 STIG Version 1 Release 9
- Ubuntu 18.04 STIG Version 2 Release 10
- Ubuntu 20.04 STIG Version 1 Release 7

Änderungen im vierten Quartal 2022 – 01.02.2023:

Die STIG-Versionen wurden aktualisiert und STIGS für die Version des vierten Quartals 2022 wie folgt angewendet:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Release 9
- RHEL 8 STIG Version 1 Release 8
- Ubuntu 18.04 STIG Version 2 Release 9
- Ubuntu 20.04 STIG Version 1 Release 6

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Release 9
- RHEL 8 STIG Version 1 Release 8
- Ubuntu 18.04 STIG Version 2 Release 9
- Ubuntu 20.04 STIG Version 1 Release 6

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Release 9
- RHEL 8 STIG Version 1 Release 8
- Ubuntu 18.04 STIG Version 2 Release 9
- Ubuntu 20.04 STIG Version 1 Release 6

Änderungen im dritten Quartal 2022 – 30.09.2022 (keine Änderungen):

Für die Version des dritten Quartals 2022 gab es keine Änderungen für die Linux-Komponenten-STIGS.

Änderungen im zweiten Quartal 2022 – 02.08.2022:

Unterstützung für Ubuntu wurde eingeführt, die STIG-Versionen aktualisiert und STIGS für die Version des zweiten Quartals 2022 wie folgt angewendet:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Release 7
- RHEL 8 STIG Version 1 Release 6
- Ubuntu 18.04 STIG Version 2 Release 6 (neu)
- Ubuntu 20.04 STIG Version 1 Release 4 (neu)

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Release 7
- RHEL 8 STIG Version 1 Release 6
- Ubuntu 18.04 STIG Version 2 Release 6 (neu)
- Ubuntu 20.04 STIG Version 1 Release 4 (neu)

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Release 7
- RHEL 8 STIG Version 1 Release 6
- Ubuntu 18.04 STIG Version 2 Release 6 (neu)
- Ubuntu 20.04 STIG Version 1 Release 4 (neu)

Änderungen im ersten Quartal 2022 – 26.04.2022:

Faktorwechsel, um eine bessere Unterstützung für Container zu bieten. Kombiniert das vorherige AL2-Skript mit RHEL 7. Die STIG-Versionen wurden aktualisiert und STIGS für die Version des ersten Quartals 2022 wie folgt angewendet:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Release 6
- RHEL 8 STIG Version 1 Release 5

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Release 6
- RHEL 8 STIG Version 1 Release 5

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Release 6
- RHEL 8 STIG Version 1 Release 5

Änderungen im vierten Quartal 2021 – 20.12.2021:

Die STIG-Versionen wurden aktualisiert und STIGS für die Version des vierten Quartals 2021 wie folgt angewendet:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Release 5
- RHEL 8 STIG Version 1 Release 4

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Release 5
- RHEL 8 STIG Version 1 Release 4

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Release 5
- RHEL 8 STIG Version 1 Release 4

Änderungen im dritten Quartal 2021 – 30.09.2021:

Die STIG-Versionen wurden aktualisiert und STIGS für die Version des dritten Quartals 2021 wie folgt angewendet:

Linux STIG Low (Kategorie III)

- RHEL 7 STIG Version 3 Release 4
- RHEL 8 STIG Version 1 Release 3

Linux STIG Medium (Kategorie II)

- RHEL 7 STIG Version 3 Release 4
- RHEL 8 STIG Version 1 Release 3

Linux STIG High (Kategorie I)

- RHEL 7 STIG Version 3 Release 4
- RHEL 8 STIG Version 1 Release 3

Versionsverlauf für Windows-STIG

In diesem Abschnitt wird der Versionsverlauf für Windows-Skriptpakete protokolliert, die vierteljährlich aktualisiert werden. Um die Änderungen und veröffentlichten Versionen für ein Quartal zu sehen, wählen Sie den Titel aus, um die Informationen zu erweitern. Wenn es für das Quartal keine Änderungen gibt, können Sie dies am Titel erkennen.

Änderungen im dritten Quartal 2025 – 04.09.2025 (keine Änderungen):

In der Version des dritten Quartals 2025 gab es keine Änderungen für die Windows-Komponenten-STIGS.

Änderungen im zweiten Quartal 2025 – 26.06.2025:

Die STIG-Versionen wurden aktualisiert und STIGS für die Version des zweiten Quartals 2025 wie folgt angewendet:

Windows STIG Low (Kategorie III)

- Windows Server 2022 STIG Version 2 Release 4

- Windows Server 2019 STIG Version 3 Release 4
- Windows Server 2016 STIG Version 2 Release 10
- Windows Server 2012 R2 MS STIG Version 3 Release 5
- Microsoft .NET Framework 4.0 STIG Version 2 Release 6
- Windows Firewall STIG Version 2 Release 2
- Internet Explorer 11 STIG Version 2 Release 5
- Microsoft Edge STIG Version 2 Release 2 (nur Windows Server 2022)

Windows STIG Medium (Kategorie II)

- Windows Server 2022 STIG Version 2 Release 4
- Windows Server 2019 STIG Version 3 Release 4
- Windows Server 2016 STIG Version 2 Release 10
- Windows Server 2012 R2 MS STIG Version 3 Release 5
- Microsoft .NET Framework 4.0 STIG Version 2 Release 6
- Windows Firewall STIG Version 2 Release 2
- Internet Explorer 11 STIG Version 2 Release 5
- Microsoft Edge STIG Version 2 Release 2 (nur Windows Server 2022)
- Defender STIG Version 2 Release 4

Windows STIG High (Kategorie I)

- Windows Server 2022 STIG Version 2 Release 4
- Windows Server 2019 STIG Version 3 Release 4
- Windows Server 2016 STIG Version 2 Release 10
- Windows Server 2012 R2 MS STIG Version 3 Release 5
- Microsoft .NET Framework 4.0 STIG Version 2 Release 6
- Windows Firewall STIG Version 2 Release 2
- Internet Explorer 11 STIG Version 2 Release 5
- Microsoft Edge STIG Version 2 Release 2 (nur Windows Server 2022)
- Defender STIG Version 2 Release 4

Änderungen im ersten Quartal 2025 – 04.05.2025:

STIGS für Internet Explorer 11 STIG Version 2 Release 5 für alle STIG-Komponenten für die Version des ersten Quartals 2025 aktualisiert.

Änderungen im vierten Quartal 2024 – 10.12.2024:

Die STIG-Versionen wurden aktualisiert und STIGS für die Version des vierten Quartals 2024 wie folgt angewendet:

Windows STIG Low (Kategorie III)

- Windows Server 2022 STIG Version 2 Release 2
- Windows Server 2019 STIG Version 3 Release 2
- Windows Server 2016 STIG Version 2 Release 9
- Windows Server 2012 R2 MS STIG Version 3 Release 5
- Microsoft .NET Framework 4.0 STIG Version 2 Release 2
- Windows Firewall STIG Version 2 Release 2
- Internet Explorer 11 STIG Version 2 Release 5
- Microsoft Edge STIG Version 2 Release 2 (nur Windows Server 2022)

Windows STIG Medium (Kategorie II)

- Windows Server 2022 STIG Version 2 Release 2
- Windows Server 2019 STIG Version 3 Release 2
- Windows Server 2016 STIG Version 2 Release 9
- Windows Server 2012 R2 MS STIG Version 3 Release 5
- Microsoft .NET Framework 4.0 STIG Version 2 Release 2
- Windows Firewall STIG Version 2 Release 2
- Internet Explorer 11 STIG Version 2 Release 5
- Microsoft Edge STIG Version 2 Release 2 (nur Windows Server 2022)
- Defender STIG Version 2 Release 4

Windows STIG High (Kategorie I)

- Windows Server 2022 STIG Version 2 Release 2

- Windows Server 2019 STIG Version 3 Release 2
- Windows Server 2016 STIG Version 2 Release 9
- Windows Server 2012 R2 MS STIG Version 3 Release 5
- Microsoft .NET Framework 4.0 STIG Version 2 Release 2
- Windows Firewall STIG Version 2 Release 2
- Internet Explorer 11 STIG Version 2 Release 5
- Microsoft Edge STIG Version 2 Release 2 (nur Windows Server 2022)
- Defender STIG Version 2 Release 4

Änderungen im dritten Quartal 2024 – 04.10.2024 (keine Änderungen):

In der Version des dritten Quartals 2024 gab es keine Änderungen für die Windows-Komponenten-STIGS.

Änderungen im zweiten Quartal 2024 – 10.05.2024 (keine Änderungen):

In der Version des zweiten Quartals 2024 gab es keine Änderungen für die Windows-Komponenten-STIGS.

Änderungen im ersten Quartal 2024 – 23.02.2024 (keine Änderungen):

In der Version des ersten Quartals 2024 gab es keine Änderungen für die Windows-Komponenten-STIGS.

Änderungen im vierten Quartal 2023 – 07.12.2023 (keine Änderungen):

In der Version des vierten Quartals 2024 gab es keine Änderungen für die Windows-Komponenten-STIGS.

Änderungen im dritten Quartal 2023 – 04.10.2023 (keine Änderungen):

In der Version des dritten Quartals 2023 gab es keine Änderungen für die Windows-Komponenten-STIGS.

Änderungen im zweiten Quartal 2023 – 03.05.2023 (keine Änderungen):

In der Version des zweiten Quartals 2023 gab es keine Änderungen für die Windows-Komponenten-STIGS.

Änderungen im ersten Quartal 2023 – 27.03.2023 (keine Änderungen):

In der Version des ersten Quartals 2023 gab es keine Änderungen für die Windows-Komponenten-STIGS.

Änderungen im vierten Quartal 2022 – 01.02.2023:

Die STIG-Versionen wurden aktualisiert und STIGS für die Version des vierten Quartals 2022 wie folgt angewendet:

Windows STIG Low (Kategorie III)

- Windows Server 2022 STIG Version 1 Release 1
- Windows Server 2019 STIG Version 2 Release 5
- Windows Server 2016 STIG Version 2 Release 5
- Windows Server 2012 R2 MS STIG Version 3 Release 5
- Microsoft .NET Framework 4.0 STIG Version 2 Release 2
- Windows Firewall STIG Version 2 Release 1
- Internet Explorer 11 STIG Version 2 Release 3
- Microsoft Edge STIG Version 1 Release 6 (nur Windows Server 2022)

Windows STIG Medium (Kategorie II)

- Windows Server 2022 STIG Version 1 Release 1
- Windows Server 2019 STIG Version 2 Release 5
- Windows Server 2016 STIG Version 2 Release 5
- Windows Server 2012 R2 MS STIG Version 3 Release 5
- Microsoft .NET Framework 4.0 STIG Version 2 Release 2
- Windows Firewall STIG Version 2 Release 1
- Internet Explorer 11 STIG Version 2 Release 3
- Microsoft Edge STIG Version 1 Release 6 (nur Windows Server 2022)
- Defender STIG Version 2 Release 4 (nur Windows Server 2022)

Windows STIG High (Kategorie I)

- Windows Server 2022 STIG Version 1 Release 1

- Windows Server 2019 STIG Version 2 Release 5
- Windows Server 2016 STIG Version 2 Release 5
- Windows Server 2012 R2 MS STIG Version 3 Release 5
- Microsoft .NET Framework 4.0 STIG Version 2 Release 2
- Windows Firewall STIG Version 2 Release 1
- Internet Explorer 11 STIG Version 2 Release 3
- Microsoft Edge STIG Version 1 Release 6 (nur Windows Server 2022)
- Defender STIG Version 2 Release 4 (nur Windows Server 2022)

Änderungen im dritten Quartal 2022 – 30.09.2022 (keine Änderungen):

In der Version des dritten Quartals 2022 gab es keine Änderungen für die Windows-Komponenten-STIGS.

Änderungen im zweiten Quartal 2022 – 02.08.2022:

Die STIG-Versionen wurden aktualisiert und STIGS für die Version des zweiten Quartals 2022 angewendet.

Windows STIG Low (Kategorie III)

- Windows Server 2019 STIG Version 2 Release 4
- Windows Server 2016 STIG Version 2 Release 4
- Windows Server 2012 R2 MS STIG Version 3 Release 3
- Microsoft .NET Framework 4.0 STIG Version 2 Release 1
- Windows Firewall STIG Version 2 Release 1
- Internet Explorer 11 STIG Version 1 Release 19

Windows STIG Medium (Kategorie II)

- Windows Server 2019 STIG Version 2 Release 4
- Windows Server 2016 STIG Version 2 Release 4
- Windows Server 2012 R2 MS STIG Version 3 Release 3
- Microsoft .NET Framework 4.0 STIG Version 2 Release 1

- Windows Firewall STIG Version 2 Release 1
- Internet Explorer 11 STIG Version 1 Release 19

Windows STIG High (Kategorie I)

- Windows Server 2019 STIG Version 2 Release 4
- Windows Server 2016 STIG Version 2 Release 4
- Windows Server 2012 R2 MS STIG Version 3 Release 3
- Microsoft .NET Framework 4.0 STIG Version 2 Release 1
- Windows Firewall STIG Version 2 Release 1
- Internet Explorer 11 STIG Version 1 Release 19

Änderungen im ersten Quartal 2022 – 02.08.2022 (keine Änderungen):

In der Version des ersten Quartals 2022 gab es keine Änderungen für die Windows-Komponenten-STIGS.

Änderungen im vierten Quartal 2021 – 20.12.2021:

Die STIG-Versionen wurden aktualisiert und STIGS für die Version des vierten Quartals 2021 angewendet:

Windows STIG Low (Kategorie III)

- Windows Server 2019 STIG Version 2 Release 3
- Windows Server 2016 STIG Version 2 Release 3
- Windows Server 2012 R2 MS STIG Version 3 Release 3
- Microsoft .NET Framework 4.0 STIG Version 2 Release 1
- Windows Firewall STIG Version 2 Release 1
- Internet Explorer 11 STIG Version 1 Release 19

Windows STIG Medium (Kategorie II)

- Windows Server 2019 STIG Version 2 Release 3
- Windows Server 2016 STIG Version 2 Release 3

- Windows Server 2012 R2 MS STIG Version 3 Release 3
- Microsoft .NET Framework 4.0 STIG Version 2 Release 1
- Windows Firewall STIG Version 2 Release 1
- Internet Explorer 11 STIG Version 1 Release 19

Windows STIG High (Kategorie I)

- Windows Server 2019 STIG Version 2 Release 3
- Windows Server 2016 STIG Version 2 Release 3
- Windows Server 2012 R2 MS STIG Version 3 Release 3
- Microsoft .NET Framework 4.0 STIG Version 2 Release 1
- Windows Firewall STIG Version 2 Release 1
- Internet Explorer 11 STIG Version 1 Release 19

Änderungen im dritten Quartal 2021 – 30.09.2021:

Die STIG-Versionen wurden aktualisiert und STIGS für die Version des dritten Quartals 2021 angewendet.

Windows STIG Low (Kategorie III)

- Windows Server 2019 STIG Version 2 Release 2
- Windows Server 2016 STIG Version 2 Release 2
- Windows Server 2012 R2 MS STIG Version 3 Release 2
- Microsoft .NET Framework 4.0 STIG Version 2 Release 1
- Windows Firewall STIG Version 1 Release 7
- Internet Explorer 11 STIG Version 1 Release 19

Windows STIG Medium (Kategorie II)

- Windows Server 2019 STIG Version 2 Release 2
- Windows Server 2016 STIG Version 2 Release 2
- Windows Server 2012 R2 MS STIG Version 3 Release 2
- Microsoft .NET Framework 4.0 STIG Version 2 Release 1

- Windows Firewall STIG Version 1 Release 7
- Internet Explorer 11 STIG Version 1 Release 19

Windows STIG High (Kategorie I)

- Windows Server 2019 STIG Version 2 Release 2
- Windows Server 2016 STIG Version 2 Release 2
- Windows Server 2012 R2 MS STIG Version 3 Release 2
- Microsoft .NET Framework 4.0 STIG Version 2 Release 1
- Windows Firewall STIG Version 1 Release 7
- Internet Explorer 11 STIG Version 1 Release 19

AWS Systems Manager verwenden, um STIG-Einstellungen auf Ihre Instance anzuwenden

Sie können das Systems-Manager-Befehlsdokument `AWSEC2-ConfigureSTIG` verwenden, um STIG-Einstellungen auf eine bestehende EC2-Instance anzuwenden. Sie müssen das Befehlsdokument von der Instance aus ausführen, die es aktualisiert. Das Befehlsdokument wendet die entsprechenden Einstellungen an, die auf dem Betriebssystem und der Konfiguration der Instance basieren, auf der es ausgeführt wird.

Diese Seite enthält Details zum `AWSEC2-ConfigureSTIG`-Befehlsdokument, einschließlich Eingabeparametern und wie es in der Systems-Manager-Konsole oder mit `send-command` in der AWS CLI ausgeführt wird.

AWSEC2-ConfigureSTIG-Eingabeparameter

Sie können die folgenden Eingabeparameter angeben, um anzugeben, wie das Befehlsdokument die STIG-Einstellungen auf Ihre Instance anwenden soll.

Stufe (Zeichenfolge, erforderlich)

Geben Sie den anzuwendenden STIG-Schweregrad an. Gültige Werte sind unter anderem:

- Hoch
- Mittelschwer
- Niedrig

Wenn Sie keinen Wert angeben, verwendet das System standardmäßig den Wert `High`.

InstallPackages (Zeichenfolge, optional – nur Linux)

Wenn der Wert `No` ist, installiert das Skript keine zusätzlichen Softwarepakete. Wenn der Wert `Yes` ist, installiert das Skript zusätzliche Softwarepakete, die für maximale Compliance erforderlich sind. Der Standardwert ist `No`.

SetDoDConsentBanner (Zeichenfolge, optional – nur Linux)

Wenn der Wert `No` ist, wird das DoD-Zustimmungsbanner nicht angezeigt, wenn Sie eine Verbindung zu einer Instance herstellen, auf der ein Linux-STIG-Skript installiert ist. Wenn der Wert `Yes` ist, wird das DoD-Zustimmungsbanner vor der Anmeldung angezeigt, wenn Sie eine Verbindung zu einer Instance herstellen, auf der ein Linux-STIG-Skript installiert ist. Sie müssen das Banner bestätigen, bevor Sie sich anmelden können. Der Standardwert ist `No`.

Ein Beispiel für das Einwilligungsbanner ist der Haftungsausschluss, Datenschutz- und Einwilligungserklärung des Department of Defence, der angezeigt wird, wenn Sie auf die Website von DLA Document Services zugreifen.

Das AWSEC2-ConfigureSTIG-Befehlsdokument ausführen

Folgen Sie den Schritten für Ihre bevorzugte Umgebung, um das Dokument `AWSEC2-ConfigureSTIG` auszuführen.

Console

1. Öffnen Sie die AWS Systems Manager-Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich Befehl ausführen. Hier wird gegebenenfalls eine Liste der Befehle angezeigt, die derzeit in Ihrem Konto ausgeführt werden.
3. Wählen Sie Befehl ausführen aus. Dadurch wird das Dialogfeld Befehl ausführen geöffnet und eine Liste von Befehlsdokumenten angezeigt, auf die Sie Zugriff haben.
4. Wählen Sie `AWSEC2-ConfigureSTIG` aus der Liste der Befehlsdokumente aus. Um die Ergebnisse zu optimieren, können Sie den Dokumentnamen ganz oder teilweise eingeben. Sie können auch nach dem Eigentümer, nach Plattformtypen oder nach Tags filtern.

   Wenn Sie ein Befehlsdokument auswählen, werden die Details unter der Liste angezeigt.
5. Wählen Sie `Default version at runtime` aus der Liste der Dokumentversionen.

6. Konfigurieren Sie die Befehlsparameter, um zu definieren, wie `AWSEC2-ConfigureSTIG` das Skriptpaket installiert und ausführt, um Ihre Instance zu aktualisieren. Einzelheiten zu den Parametern finden Sie unter AWSEC2-ConfigureSTIG-Eingabeparameter.
7. Geben Sie für Zielauswahl Tags an oder wählen Sie Instances manuell, um die Instances zu identifizieren, in denen Sie diesen Vorgang ausführen möchten.

   > **Note**
   >
   > Wenn Sie entscheiden, Instances manuell auszuwählen, und eine von Ihnen erwartete Instance nicht in der Liste enthalten ist, finden Sie Tipps zur Fehlersuche unter Wo sind meine Instances?.

8. Für zusätzliche Parameter zur Definition des Verhaltens von Systems Manager Run Command, wie z. B. die Ratensteuerung, geben Sie Werte ein, wie unter Befehle von der Konsole ausführen beschrieben.
9. Klicken Sie auf Ausführen.

   Bei Erfolg installiert das Befehlsdokument das Skript und konfiguriert Ihre Instance. Wenn die Befehlsausführung fehlgeschlagen ist, zeigen Sie die Systems Manager-Befehlsausgabe an, um nähere Informationen zum Grund hierfür zu erfahren.

AWS CLI

Beispiel 1: Mit Standardwerten ausführen

Führen Sie den folgenden Befehl aus, um das STIG-Skript zu installieren und mit Standardwerten auszuführen. Weitere Informationen über die Eingabeparameter finden Sie unter AWSEC2-ConfigureSTIG-Eingabeparameter.

```
aws ssm send-command \
 --document-name "AWSEC2-ConfigureSTIG" \
 --instance-ids "i-1234567890abcdef0"'
```

Beispiel 2: Konfigurieren Sie die STIG-Einstellungen auf mittlerer Ebene auf Ihrer Instance

Führen Sie den folgenden Befehl aus, um das STIG-Skript zu installieren, und führen Sie es mit dem `Level`-Eingabeparameter auf `Medium` gesetzt aus. Weitere Informationen über die Eingabeparameter finden Sie unter AWSEC2-ConfigureSTIG-Eingabeparameter.

```
aws ssm send-command \
 --document-name "AWSEC2-ConfigureSTIG" \
 --instance-ids "i-1234567890abcdef0"
 --parameters '{"Level":"Medium"}'
```

Bei Erfolg installiert das Befehlsdokument das Skript und konfiguriert Ihre Instance. Wenn die Befehlsausführung fehlgeschlagen ist, zeigen Sie die -Befehlsausgabe an, um nähere Informationen zum Grund hierfür zu erfahren.

PowerShell

Beispiel 1: Mit Standardwerten ausführen

Führen Sie den folgenden Befehl aus, um das STIG-Skript zu installieren und mit Standardwerten auszuführen. Weitere Informationen über die Eingabeparameter finden Sie unter AWSEC2-ConfigureSTIG-Eingabeparameter.

```
Send-SSMCommand -DocumentName "AWSEC2-ConfigureSTIG" -InstanceId
 "i-1234567890abcdef0"}
```

Beispiel 2: Konfigurieren Sie die STIG-Einstellungen auf mittlerer Ebene auf Ihrer Instance

Führen Sie den folgenden Befehl aus, um das STIG-Skript zu installieren, und führen Sie es mit dem `Level`-Eingabeparameter auf `Medium` gesetzt aus. Weitere Informationen über die Eingabeparameter finden Sie unter AWSEC2-ConfigureSTIG-Eingabeparameter.

```
Send-SSMCommand -DocumentName "AWSEC2-ConfigureSTIG" -InstanceId
 "i-1234567890abcdef0" -Parameter @{'Level'='Medium'}
```

Bei Erfolg installiert das Befehlsdokument das Skript und konfiguriert Ihre Instance. Wenn die Befehlsausführung fehlgeschlagen ist, zeigen Sie die -Befehlsausgabe an, um nähere Informationen zum Grund hierfür zu erfahren.

Präzise Uhr- und Zeitsynchronisierung auf Ihrer EC2-Instance

Eine konsistente und korrekte Zeitreferenz in Ihrer Amazon-EC2-Instance ist für viele Serveraufgaben und -prozesse unerlässlich. Zeitstempel in Systemprotokollen sind wichtig, um den Zeitpunkt, zu dem Probleme aufgetreten sind, sowie die chronologische Reihenfolge von Ereignissen zu ermitteln. Wenn Sie die AWS CLI oder ein AWS SDK verwenden, um Anforderungen an Ihre Instance zu

senden, signieren diese Tools die Anforderungen für Sie. Stellen Sie sicher, dass die Datums- und Uhrzeiteinstellungen der Instance korrekt sind. Andernfalls kann es zu einer Diskrepanz zwischen dem Datum in der Signatur und dem Datum der Anforderung kommen, was zur Folge hat, dass die Anforderung von AWS abgelehnt wird.

Für diesen wichtigen Aspekt stellt Amazon den Amazon Time Sync Service bereit, der über alle EC2-Instances zugänglich ist und von verschiedenen AWS-Services verwendet. Dieser Service nutzt eine Flotte aus mit Satelliten verbundenen und atomaren Referenzuhren in jeder AWS-Region, um präzise und aktuelle Zeitangaben des globalen Standards der koordinierten Weltzeit (UTC) bereitzustellen.

Für eine optimale Leistung empfehlen wir, den lokalen Amazon Time Sync Service auf Ihren EC2-Instances zu verwenden. Für eine Sicherung des lokalen Amazon Time Sync Service auf Ihren Instances oder um Ressourcen außerhalb von Amazon EC2 mit dem Amazon Time Sync Service zu verbinden, können Sie den öffentlichen Amazon Time Sync Service verwenden, der sich unter `time.aws.com` befindet. Der öffentliche Amazon Time Sync Service teilt genau wie der lokale Amazon Time Sync Service automatisch alle Schaltsekunden auf, die der UTC hinzugefügt werden. Der öffentliche Amazon Time Sync Service wird weltweit von unserer Flotte aus mit Satelliten verbundenen und atomaren Referenzuhren in jeder unterstützt AWS-Region.

Hardware-Paket-Zeitstempel

Sie können Hardware-Paket-Zeitstempel auf der Instance aktivieren, um jedem eingehenden Netzwerkpaket einen 64-Bit-Zeitstempel mit einer Genauigkeit von Nanosekunden hinzuzufügen. Da der Zeitstempel für Hardwarepakete auf Hardwareebene erfolgt, also bevor das Paket den Kernel, den Socket oder die Anwendungsschicht erreicht, umgehen Sie alle Verzögerungen, die durch Software-Zeitstempel entstehen. Die zugrunde liegende Referenzuhr für Hardware-Zeitstempel ist die PTP-Hardware-Uhr von Amazon Time Sync Service.

Vorteile

Hardware-Paket-Zeitstempel bieten die folgenden Vorteile:

- Verbessert die Reihenfolge der Ereignisse, anhand derer auch die tatsächliche Reihenfolge bestimmt werden kann, in der Pakete bei Ihrer EC2-Instance ankommen, wodurch eine faire Paketverarbeitung gewährleistet wird.
- Misst die unidirektionale Netzwerklatenz.
- Erhöht die Geschwindigkeit verteilter Transaktionen mit höherer Präzision und Genauigkeit im Vergleich zu den meisten On-Premises-Lösungen.

Voraussetzungen und Konfiguration

Um Hardware-Paket-Zeitstempel zu aktivieren, muss die Instance die folgenden Voraussetzungen erfüllen:

- Es muss eine Linux-Instance sein.
- Sie muss die Anforderungen zur Unterstützung der PTP-Hardware-Uhr erfüllen.

Anweisungen zur Konfiguration finden Sie unter Hardware-Paket-Zeitstempel auf der Seite Linux-Kerneltreiber für die Elastic Network Adapter (ENA)-Familie auf GitHub.

Schaltsekunden

Schaltsekunden wurden 1972 eingeführt. Sie sind gelegentliche einsekündige Anpassungen der UTC-Zeit, um Unregelmäßigkeiten bei der Erdrotation sowie Abweichungen zwischen der Internationalen Atomzeit (TAI) und der Sonnenzeit (Ut1) Rechnung zu tragen. Um Schaltsekunden für unsere Kunden zu verwalten, haben wir die Schaltsekundenaufteilung im Rahmen des Amazon Time Sync Service entwickelt. Weitere Informationen finden Sie unter Augen auf bei der Verwendung von Schaltsekunden: Die nächste Schaltsekunde und AWS.

Schaltsekunden werden abgeschafft und wir stehen voll und ganz hinter der bei der 27. General Conference on Weights and Measures getroffenen Entscheidung, Schaltsekunden bis spätestens 2035 abzuschaffen.

Um diese Umstellung zu unterstützen, planen wir, während eines Schaltsekundenereignisses weiterhin Time Smearing einzusetzen, wenn auf den Amazon Time Sync Service über die lokale NTP-Verbindung oder über unsere öffentlichen NTP-Pools (`time.aws.com`) zugegriffen wird. Die PTP-Hardware-Uhr bietet jedoch keine Time Smearing-Option. Im Falle einer Schaltsekunde fügt die PTP-Hardware-Uhr die Schaltsekunde gemäß den UTC-Standards hinzu. Zeitquellen mit Leap Smearing und Zeitquellen mit Schaltsekunden sind in den meisten Fällen gleich. Da sie sich jedoch während eines Schaltsekundenereignisses unterscheiden, raten wir davon ab, während eines Schaltsekundenereignisses sowohl Zeitquellen mit Time Smearing als auch Zeitquellen ohne Time Smearing in Ihrer Zeit-Client-Konfiguration zu verwenden.

Themen

- Die Zeitreferenz auf Ihrer EC2 Instance so einstellen, dass der lokale Amazon Time Sync Service verwendet wird

- Die Zeitreferenz auf Ihrer EC2-Instance oder einem beliebigen Gerät mit Internetanschluss so definieren, dass der öffentliche Amazon Time Sync Service verwendet wird
- Vergleichen von Zeitstempeln für Ihre Linux-Instances
- Ändern der Zeitzone für Ihre Instance

Zugehörige Ressourcen

- AWS-Compute-Blog: Es ist an der Zeit: Mikrosekundengenaue Uhren auf Amazon-EC2-Instances
- AWS-Cloud-Operations- und Migrations-Blog: Verwalten der Zeitgenauigkeit von Amazon-EC2-Instances mithilfe von Amazon Time Sync Service und Amazon CloudWatch – Teil 1
- (Linux) https://chrony-project.org/

Die Zeitreferenz auf Ihrer EC2 Instance so einstellen, dass der lokale Amazon Time Sync Service verwendet wird

Der lokale Amazon Time Sync Service verwendet entweder das Network Time Protocol (NTP) oder stellt in unterstützten Instances eine lokale Precision Time Protocol (PTP)-Hardware-Uhr bereit. Die PTP-Hardware-Uhr unterstützt entweder eine NTP-Verbindung (Linux- und Windows-Instances) oder eine direkte PTP-Verbindung (nur Linux-Instances). Die NTP-Verbindung und die direkte PTP-Verbindung verwenden zwar die gleiche hochpräzise Zeitquelle, die direkte PTP-Verbindung ist jedoch genauer als die NTP-Verbindung. Die NTP-Verbindung mit dem Amazon Time Sync Service unterstützt „Leap Smearing“ (Aufteilung von Schaltsekunden). Bei der PTP-Verbindung mit der PTP-Hardware-Uhr gibt es dagegen keine zeitliche Verwischung. Weitere Informationen finden Sie unter Schaltsekunden.

Ihre Instances können wie folgt auf den lokalen Amazon Time Sync Service zugreifen:

- Über NTP an folgenden IP-Adressendpunkten:
  - IPv4: `169.254.169.123`
  - IPv6: `fd00:ec2::123` (Nur auf Nitro-basierten Instances zugänglich.)
- (Nur Linux) Über eine direkte PTP-Verbindung, um eine Verbindung mit einer lokalen PTP-Hardware-Uhr herzustellen:
  - `PHC0`

Amazon-Linux-AMIs, Windows-AMIs und die meisten Partner-AMIs konfigurieren Ihre Instance so, dass sie standardmäßig den NTP-IPv4-Endpunkt verwendet. Dies ist die empfohlene Einstellung für die meisten Kunden-Workloads. Für Instances, die von diesen AMIs aus gestartet werden, ist keine weitere Konfiguration erforderlich, es sei denn, Sie möchten den IPv6-Endpunkt verwenden oder eine direkte Verbindung mit der PTP-Hardware-Uhr herstellen.

Für NTP- und PTP-Verbindungen müssen keine VPC-Konfigurationsänderungen vorgenommen werden und Ihre Instance benötigt keinen Zugriff auf das Internet.

Überlegungen

- Für Services, die Link-Local-Adressen verwenden, gilt eine Obergrenze von 1 024 Paketen pro Sekunde (PPS). Dieses Limit umfasst die Summe von Route-53-Resolver-DNS-Abfragen, Instance Metadata Service (IMDS)-Anfragen, Amazon Time Service Network Time Protocol (NTP)-Anfragen und Windows Licensing Service-Anfragen (für Microsoft Windows-basierte Instances).
- Nur Linux-Instances können sich über eine direkte PTP-Verbindung mit der lokalen PTP-Hardware-Uhr verbinden. Windows-Instances verwenden NTP, um eine Verbindung zur lokalen PTP-Hardwareuhr herzustellen.

Inhalt

- Eine Verbindung mit dem IPv4-Endpunkt des Amazon Time Sync Service herstellen
- Herstellen einer Verbindung mit dem IPv6-Endpunkt des Amazon Time Sync Service
- Herstellen einer Verbindung mit der PTP-Hardware-Uhr

Eine Verbindung mit dem IPv4-Endpunkt des Amazon Time Sync Service herstellen

Ihr AMI hat den Amazon Time Sync Service möglicherweise bereits standardmäßig konfiguriert. Andernfalls verwenden Sie die folgenden Verfahren, um Ihre Instance für die Verwendung des lokalen Amazon Time Sync Service über den IPv4-Endpunkt zu konfigurieren.

Hilfe zur Behebung von Problemen finden Sie unter Fehlerbehebung bei NTP-Synchronisierungsproblemen auf Linux-Instances oder Fehlerbehebung bei Zeitproblemen auf Windows-Instances.

Amazon Linux

AL2023 und die neuesten Versionen von Amazon Linux 2 sind so konfiguriert, dass sie standardmäßig den IPv4-Endpunkt des Amazon Time Sync Service verwenden. Wenn Sie

bestätigen, dass Ihre Instance bereits konfiguriert ist, können Sie das folgende Verfahren überspringen.

So überprüfen Sie, ob chrony für die Verwendung des IPv4-Endpunkts konfiguriert ist

Führen Sie den folgenden Befehl aus. In der Ausgabe, zeigt die Zeile, die mit ^* beginnt, die bevorzugte Zeitquelle.

```
chronyc sources -v | grep -F ^*
^* 169.254.169.123               3   4   377    14    +12us[+9653ns] +/-  290us
```

So konfigurieren Sie chrony für die Verbindung mit dem IPv4-Endpunkt auf älteren Versionen von Amazon Linux 2

1. Stellen Sie eine Verbindung mit Ihrer Instance her und deinstallieren Sie den NTP-Service.

   ```
   [ec2-user ~]$ sudo yum erase 'ntp*'
   ```

2. Installieren Sie das Paket `chrony`.

   ```
   [ec2-user ~]$ sudo yum install chrony
   ```

3. Öffnen Sie die Datei `/etc/chrony.conf` mit einem Texteditor Ihrer Wahl, z. B. vim oder nano. Fügen Sie die folgende Zeile vor beliebigen anderen `server`- oder `pool`-Anweisungen ein, die bereits in der Datei vorhanden sind, und speichern Sie Ihre Änderungen:

   ```
   server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
   ```

4. Starten Sie den `chrony`-Daemon (`chronyd`) neu.

   ```
   [ec2-user ~]$ sudo service chronyd restart
   ```

   ```
   Starting chronyd:                                          [  OK  ]
   ```

   > **Note**
   >
   > Auf RHEL und CentOS (bis zu Version 6) lautet der Servicename `chrony` anstatt `chronyd`.

5. Mithilfe des Befehls `chkconfig` können Sie konfigurieren, dass `chronyd` bei jedem Systemstart gestartet werden soll.

```
[ec2-user ~]$ sudo chkconfig chronyd on
```

6. Vergewissern Sie sich, dass `chrony` den IPv4-Endpunkt `169.254.169.123` für die Zeitsynchronisierung verwendet.

```
[ec2-user ~]$ chronyc sources -v | grep -F ^*
```

In der Ausgabe gibt `^*` die bevorzugte Zeitquelle an.

```
^* 169.254.169.123               3   6    17    43    -30us[ -226us] +/-  287us
```

7. Überprüfen Sie die von gemeldeten Zeitsynchronisierungsmetrike `chrony`.

```
[ec2-user ~]$ chronyc tracking
```

```
Reference ID    : A9FEA97B (169.254.169.123)
Stratum         : 4
Ref time (UTC)  : Wed Nov 22 13:18:34 2017
System time     : 0.000000626 seconds slow of NTP time
Last offset     : +0.002852759 seconds
RMS offset      : 0.002852759 seconds
Frequency       : 1.187 ppm fast
Residual freq   : +0.020 ppm
Skew            : 24.388 ppm
Root delay      : 0.000504752 seconds
Root dispersion : 0.001112565 seconds
Update interval : 64.4 seconds
Leap status     : Normal
```

Ubuntu

So konfigurieren Sie chrony für die Verbindung mit dem IPv4-Endpunkt unter Ubuntu

1. Stellen Sie eine Verbindung mit Ihrer Instance her und installieren Sie mit `apt` das `chrony`-Paket.

```
ubuntu:~$ sudo apt install chrony
```

> **Note**
>
> Sofern erforderlich, aktualisieren Sie Ihre Instance, indem Sie zuerst ausführe `sudo apt update`.

2. Öffnen Sie die Datei `/etc/chrony/chrony.conf` mit einem Texteditor Ihrer Wahl, z. B. vim oder nano. Fügen Sie die folgende Zeile vor beliebigen anderen `server`- oder `pool`-Anweisungen ein, die bereits in der Datei vorhanden sind. Speichern Sie dann Ihre Änderungen:

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

3. Den Service `chrony` neu starten.

```
ubuntu:~$ sudo /etc/init.d/chrony restart
```

```
Restarting chrony (via systemctl): chrony.service.
```

4. Vergewissern Sie sich, dass `chrony` den IPv4-Endpunkt `169.254.169.123` für die Zeitsynchronisierung verwendet.

```
ubuntu:~$ chronyc sources -v | grep -F ^*
```

In der Ausgabe, zeigt die Zeile, die mit `^*` beginnt, die bevorzugte Zeitquelle.

```
^* 169.254.169.123               3   6    17    12    +15us[  +57us] +/-  320us
```

5. Überprüfen Sie die von gemeldeten Zeitsynchronisierungsmetrike `chrony`.

```
ubuntu:~$ chronyc tracking
```

```
Reference ID    : 169.254.169.123 (169.254.169.123)
Stratum         : 4
Ref time (UTC)  : Wed Nov 29 07:41:57 2017
System time     : 0.000000011 seconds slow of NTP time
```

```
Last offset     : +0.000041659 seconds
RMS offset      : 0.000041659 seconds
Frequency       : 10.141 ppm slow
Residual freq   : +7.557 ppm
Skew            : 2.329 ppm
Root delay      : 0.000544 seconds
Root dispersion : 0.000631 seconds
Update interval : 2.0 seconds
Leap status     : Normal
```

SUSE Linux

Ab SUSE Linux Enterprise Server 15 ist `chrony` die Standardimplementierung von NTP.

So konfigurieren Sie chrony für die Verbindung mit dem IPv4-Endpunkt unter SUSE Linux

1. Öffnen Sie die Datei `/etc/chrony.conf` mit einem Texteditor Ihrer Wahl, z. B. vim oder nano.
2. Überprüfen Sie, ob die Datei die folgende Zeile enthält:

   ```
   server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
   ```

   Wenn diese Zeile nicht vorhanden ist, fügen Sie sie hinzu.
3. Kommentieren Sie alle anderen Server- oder Pool-Zeilen aus.
4. Öffnen Sie YaST und aktivieren Sie den chrony-Service.

Windows

Aber der Version von August 2018 nutzen Windows-AMIs den Amazon Time Sync Service standardmäßig. Für Instances, die von diesen AMIs aus gestartet werden, ist keine weitere Konfiguration erforderlich und Sie können die folgenden Verfahren überspringen.

Überprüfen Sie zunächst Ihre aktuelle NTP-Konfiguration, wenn Sie eine AMI verwenden, für die der Amazon Time Sync Service nicht standardmäßig konfiguriert ist. Wenn Ihre Instance bereits den IPv4-Endpunkt des Amazon Time Sync Service verwendet, ist keine weitere Konfiguration erforderlich. Wenn Ihre Instance den Amazon Time Sync Service nicht verwendet, schließen Sie das Verfahren ab, um den NTP-Server so zu ändern, dass er den Amazon Time Sync Service verwendet.

So überprüfen Sie die NTP-Konfiguration

1. Öffnen Sie in Ihrer Instance ein Eingabeaufforderungsfenster.
2. Mit folgendem Befehl zeigen Sie die derzeitige NTP-Konfiguration an:

   ```
   w32tm /query /configuration
   ```

   Dieser Befehl gibt die aktuellen Konfigurationseinstellungen für die Windows-Instance zurück und zeigt, ob eine Verbindung mit dem Amazon Time Sync Service besteht.
3. Mit folgendem Befehl wird der Status der derzeitigen Konfiguration angezeigt (optional):

   ```
   w32tm /query /status
   ```

   Dieser Befehl gibt Informationen wie den Zeitpunkt der letzten Synchronisierung der Instance mit dem NTP-Server und das Abrufintervall zurück.

So stellen Sie den NTP-Server auf die Verwendung des Amazon Time Sync Service ein

1. Führen Sie über das Eingabeaufforderungsfenster den folgenden Befehl aus:

   ```
   w32tm /config /manualpeerlist:169.254.169.123 /syncfromflags:manual /update
   ```
2. Mit folgendem Befehl überprüfen Sie Ihre neuen Einstellungen:

   ```
   w32tm /query /configuration
   ```

   Vergewissern Sie sich in der zurückgegebenen Ausgabe, dass für `NtpServer` der IPv4-Endpunkt `169.254.169.123` angezeigt wird.

Standardmäßige NTP-Einstellungen für Amazon-Windows-AMIs

Amazon Machine Images (AMIs) entsprechen in der Regel den werksseitigen Standards, es sei denn, Änderungen an der Funktion der EC2-Infrastruktur sind erforderlich. Die folgenden Einstellungen funktionieren in einer virtualisierten Umgebung erwiesenermaßen gut. Zudem weicht die Uhrzeit nie um mehr als eine Sekunde ab:

- Aktualisierungsintervall: regelt, wie häufig der Zeit-Service die Genauigkeit der Systemzeit anpasst. AWS konfiguriert das Aktualisierungsintervall so, dass es alle zwei Minuten eintritt.
- NTP-Server: Ab dem Release vom August 2018 verwenden AMIs standardmäßig den Amazon Time Sync Service. Dieser Zeit-Service ist in jeder AWS-Region am IPv4-Endpunkt 169.254.169.123 verfügbar. Zudem gibt das Flag 0x9 an, dass der Zeitdienst als Client fungiert und dass `SpecialPollInterval` verwendet werden soll, um zu ermitteln, wie häufig der Abgleich mit dem konfigurierten Zeitserver erfolgen soll.
- Typ – „NTP“ bedeutet, dass der Service als eigenständiger NTP-Client und nicht als Teil einer Domain fungiert.
- Aktiviert und InputProvider – Der Zeit-Service ist aktiviert und stellt dem Betriebssystem die Uhrzeit bereit.
- Spezielles Abrufintervall – Fragt den konfigurierten NTP-Server alle 900 Sekunden (15 Minuten) ab.

Registry-Pfad	Tastenname	Daten
HKLM:\System\CurrentControlSet\services\w32time\Config	UpdateInterval	120
HKLM:\System\CurrentControlSet\services\w32time\Parameters	NtpServer	169.254.169.123,0x9
HKLM:\System\CurrentControlSet\services\w32time\Parameters	Typ	NTP
HKLM:\System\CurrentControlSet\services\w32time\TimeProviders\NtpClient	Enabled	1
HKLM:\System\CurrentControlSet\services\w32time\TimeProviders\NtpClient	InputProvider	1

Registry-Pfad	Tastenname	Daten
HKLM:\System\CurrentControlSet\services\w32time\TimeProviders\NtpClient	SpecialPollInterval	900

Herstellen einer Verbindung mit dem IPv6-Endpunkt des Amazon Time Sync Service

In diesem Abschnitt erfahren Sie, inwiefern sich die unter Eine Verbindung mit dem IPv4-Endpunkt des Amazon Time Sync Service herstellen beschriebenen Schritte unterscheiden, wenn Sie Ihre Instance für die Verwendung des lokalen Amazon Time Sync Service über den IPv6-Endpunkt konfigurieren. Es wird nicht der gesamte Konfigurationsprozess des Amazon Time Sync Service erklärt.

Auf den IPv6-Endpunkt kann nur in Nitro-basierten Instances zugegriffen werden.

Es wird nicht empfohlen, die IPv4- und IPv6-Endpunkteinträge zusammen zu verwenden. Die IPv4- und IPv6-NTP-Pakete stammen von demselben lokalen Server für Ihre Instance. Das gleichzeitige Konfigurieren von IPv4- und IPv6-Endpunkten ist unnötig und führt nicht zu einer höheren Zeitgenauigkeit in Ihrer Instance.

Linux

Je nach der Linux-Distribution verwenden Sie, wenn Sie den Schritt zum Bearbeiten der `chrony.conf`-Datei erreichen, den IPv6-Endpunkt des Amazon Time Sync Service (`fd00:ec2::123`) anstelle des IPv4-Endpunkts (`169.254.169.123`):

```
server fd00:ec2::123 prefer iburst minpoll 4 maxpoll 4
```

Speichern Sie die Datei und vergewissern Sie sich, dass chrony den IPv6-Endpunkt `fd00:ec2::123` für die Zeitsynchronisierung verwendet:

```
[ec2-user ~]$ chronyc sources -v
```

Wenn die Ausgabe den IPv6-Endpunkt `fd00:ec2::123` enthält, ist die Konfiguration abgeschlossen.

Windows

Wenn Sie den Schritt erreichen, den NTP-Server für die Verwendung des Amazon Time Sync Service zu ändern, verwenden Sie den IPv6-Endpunkt des Amazon Time Sync Service (`fd00:ec2::123`) anstelle des IPv4-Endpunkts (`169.254.169.123`):

```
w32tm /config /manualpeerlist:fd00:ec2::123 /syncfromflags:manual /update
```

Stellen Sie sicher, dass Ihre neuen Einstellungen den `fd00:ec2::123`-IPv6-Endpunkt zur Zeitsynchronisierung verwenden:

```
w32tm /query /configuration
```

Vergewissern Sie sich in der Ausgabe, dass `NtpServer` den `fd00:ec2::123`-IPv6-Endpunkt anzeigt.

Herstellen einer Verbindung mit der PTP-Hardware-Uhr

Die PTP-Hardware-Uhr ist Teil von AWS Nitro System. Daher kann in unterstützten Bare-Metal- und virtualisierten EC2-Instances direkt darauf zugegriffen werden, ohne Kundenressourcen zu beanspruchen.

Die NTP-Endpunkte für die PTP-Hardware-Uhr sind die gleichen wie für den regulären Amazon Time Sync Service. Wenn Ihre Instance über eine PTP-Hardware-Uhr verfügt und Sie die NTP-Verbindung (entweder mit dem IPv4- oder mit dem IPv6-Endpunkt) konfiguriert haben, wird Ihre Instance-Zeit automatisch von der PTP-Hardware-Uhr über NTP abgerufen.

Für Linux-Instances können Sie eine direkte PTP-Verbindung konfigurieren, um eine präzisere Uhrzeit zu erhalten als bei der NTP-Verbindung. Windows-Instances unterstützen nur eine NTP-Verbindung zur PTP-Hardware-Uhr.

Voraussetzungen

Die PTP-Hardware-Uhr ist in einer Instance verfügbar, wenn die folgenden Anforderungen erfüllt sind:

- Unterstützte AWS-Regionen: USA Ost (Nord-Virginia), USA Ost (Ohio), Asien-Pazifik (Malaysia), Asien-Pazifik (Thailand), Asien-Pazifik (Tokio) und Europa (Stockholm)
- Unterstützte Local Zones: USA Ost (New York City)
- Unterstützte Instance-Familien:

  - Allzweck: M7a, M7g, M7i
  - Arbeitsspeicheroptimiert: R7a, R7g, R7i
  - Speicheroptimiert: I8g, I8ge
- (Nur Linux) Installation der ENA-Treiberversion 2.10.0 oder höher für ein unterstütztes Betriebssystem. Weitere Informationen zu unterstützten Betriebssystemen finden Sie auf GitHub in den treiberspezifischen Voraussetzungen.

(Nur Linux) Eine direkte PTP-Verbindung mit der PTP-Hardware-Uhr konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie Ihre Linux-Instance für die Verwendung des lokalen Amazon Time Sync Service über die PTP-Hardware-Uhr konfigurieren und dabei eine direkte PTP-Verbindung verwenden. Dafür muss der `chrony`-Konfigurationsdatei ein Servereintrag für die PTP-Hardware-Uhr hinzugefügt werden.

Eine direkte PTP-Verbindung mit der PTP-Hardware-Uhr konfigurieren (nur Linux-Instances)

1. Voraussetzungen für die Installation

   Stellen Sie eine Verbindung zur Ihrer Linux-Instance her und führen Sie die folgenden Schritte aus:

   a. Installieren Sie den Linux-Kernel-Treiber für die Elastic Network Adapter (ENA)-Version 2.10.0 oder höher.
   b. Aktivieren Sie die PTP-Hardware-Uhr.

   Die Installationsanleitung finden Sie auf GitHub unter Linux-Kernel-Treiber für die Elastic Network Adapter (ENA)-Familie.
2. ENA-PTP-Gerät überprüfen

   Vergewissern Sie sich, dass das ENA-PTP-Hardware-Uhr-Gerät in Ihrer Instance angezeigt wird.

   ```
   [ec2-user ~]$ for file in /sys/class/ptp/*; do echo -n "$file: "; cat "$file/
   clock_name"; done
   ```

   Erwartete Ausgabe

   ```
   /sys/class/ptp/ptp<index>: ena-ptp-<PCI slot>
   ```

Wobei Folgendes gilt:

- *index* ist der im Kernel registrierte Index für die PTP-Hardware-Uhr.
- *PCI slot* ist der PCI-Steckplatz des ENA-Ethernet-Controllers. Dies ist derselbe Steckplatz wie unter `lspci | grep ENA` gezeigt.

Beispielausgabe

```
/sys/class/ptp/ptp0: ena-ptp-05
```

Sollte `ena-ptp-<PCI slot>` nicht in der Ausgabe enthalten sein, wurde der ENA-Treiber nicht korrekt installiert. Informationen zum Installieren des Treibers finden Sie in Schritt 1 dieses Verfahrens.

3. PTP-Symlink konfigurieren

   PTP-Geräte werden normalerweise `/dev/ptp0`, `/dev/ptp1` usw. benannt, wobei ihr Index von der Reihenfolge der Hardware-Initialisierung abhängt. Durch das Erstellen eines Symlinks wird sichergestellt, dass Anwendungen wie chrony unabhängig von Indexänderungen konsistent auf das richtige Gerät verweisen.

   Die neuesten AMIs von Amazon Linux 2023 enthalten eine `udev`-Regel, die den Symlink `/dev/ptp_ena` erstellt und auf den richtigen `/dev/ptp`-Eintrag verweist, der dem ENA-Host zugeordnet ist.

   Überprüfen Sie zunächst, ob der Symlink vorhanden ist, indem Sie den folgenden Befehl ausführen.

```
[ec2-user ~]$ ls -l /dev/ptp*
```

   Beispielausgabe

```
crw------- 1 root root 245, 0 Jan 31 2025 /dev/ptp0
lrwxrwxrwx 1 root root      4 Jan 31 2025 /dev/ptp_ena -> ptp0
```

   Wobei Folgendes gilt:

   - `/dev/ptp<index>` ist der Pfad zum PTP-Gerät.

- `/dev/ptp_ena` ist der konstante Symlink, der auf dasselbe PTP-Gerät zeigt.

Wenn der Symlink `/dev/ptp_ena` vorhanden ist, fahren Sie mit Schritt 4 dieses Verfahrens fort. Falls es fehlt, gehen Sie wie folgt vor:

a. Fügen Sie die folgende `udev`-Regel hinzu.

```
[ec2-user ~]$ echo "SUBSYSTEM==\"ptp\", ATTR{clock_name}==\"ena-ptp-*\",
 SYMLINK += \"ptp_ena\"" | sudo tee -a /etc/udev/rules.d/53-ec2-network-
interfaces.rules
```

b. Laden Sie die `udev`-Regel neu, indem Sie entweder die Instance neu starten oder den folgenden Befehl ausführen.

```
[ec2-user ~]$ sudo udevadm control --reload-rules && udevadm trigger
```

4. Chrony konfigurieren

Chrony muss so konfiguriert werden, dass der Symlink `/dev/ptp_ena` verwendet wird, anstatt direkt auf /dev/ptp*<index>* zu verweisen.

a. Bearbeiten Sie `/etc/chrony.conf` mithilfe eines Text-Editors und fügen Sie an einer beliebigen Stelle in der Datei die folgende Zeile hinzu.

```
refclock PHC /dev/ptp_ena poll 0 delay 0.000010 prefer
```

b. Starten Sie chrony erneut.

```
[ec2-user ~]$ sudo systemctl restart chronyd
```

5. Chrony-Konfiguration überprüfen

Vergewissern Sie sich, dass chrony die PTP-Hardware-Uhr für die Zeitsynchronisierung in dieser Instance verwendet.

```
[ec2-user ~]$ chronyc sources
```

Erwartete Ausgabe

```
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
#* PHC0                          0   0    377    1   +2ns[ +1ns] +/-   5031ns
```

In der zurückgegebenen Ausgabe gibt * die bevorzugte Zeitquelle an. PHC0 entspricht der PTP-Hardware-Uhr. Nach dem Neustart von chrony dauert es möglicherweise einige Sekunden, bis das Sternchen angezeigt wird.

Die Zeitreferenz auf Ihrer EC2-Instance oder einem beliebigen Gerät mit Internetanschluss so definieren, dass der öffentliche Amazon Time Sync Service verwendet wird

Sie können Ihre Instance oder ein beliebiges Gerät mit Internetverbindung (etwa Ihren lokalen Computer oder einen On-Premises-Server) für die Verwendung des öffentlichen Amazon Time Sync Service konfigurieren, der im Internet unter `time.aws.com` zur Verfügung steht. Sie können den öffentlichen Amazon Time Sync Service als Ausweichlösung für den lokalen Amazon Time Sync Service verwenden sowie dazu, Ressourcen außerhalb von AWS mit dem Amazon Time Sync Service zu verbinden.

> **Note**
>
> Für eine optimale Leistung empfehlen wir, den lokalen Amazon Time Sync Service auf Ihren Instances zu verwenden und den öffentlichen Amazon Time Sync Service nur als Backup zu verwenden.

Verwenden Sie die Anleitung für das Betriebssystem Ihrer Instance oder Ihres Gerätes.

Linux

So konfigurieren Sie Ihre Linux-Instance oder Ihr Linux-Gerät mithilfe von chrony oder ntpd für die Verwendung des öffentlichen Amazon Time Sync Service

1. Bearbeiten Sie `/etc/chrony.conf` (bei Verwendung von chrony) oder `/etc/ntp.conf` (bei Verwendung von ntpd) mithilfe eines Text-Editors wie folgt:

a. Entfernen Sie Zeilen, die mit `server` beginnen, oder kommentieren Sie sie aus (mit Ausnahme ggf. vorhandener Verbindungen mit dem lokalen Amazon Time Sync Service), damit Ihre Instance oder Ihr Gerät nicht versucht, Server mit und ohne Time Smearing gemeinsam zu verwenden.

> **Important**
>
> Wenn Sie Ihre EC2-Instance so konfigurieren, dass sie eine Verbindung mit dem öffentlichen Amazon Time Sync Service herstellt, darf die folgende Zeile, die Ihre Instance für die Verbindungsherstellung mit dem lokalen Amazon Time Sync Service konfiguriert, nicht entfernt werden. Der lokale Amazon Time Sync Service stellt eine direktere Verbindung dar und bietet eine höhere Zeitgenauigkeit. Der öffentliche Amazon Time Sync Service sollte nur als Ausweichlösung verwendet werden.
>
> ```
> server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
> ```

b. Fügen Sie die folgende Zeile hinzu, um eine Verbindung mit dem öffentlichen Amazon Time Sync Service herzustellen.

```
pool time.aws.com iburst
```

2. Starten Sie den Daemon mithilfe eines der folgenden Befehle neu.

   - chrony

     ```
     sudo service chronyd force-reload
     ```

   - ntpd

     ```
     sudo service ntp reload
     ```

macOS

So konfigurieren Sie Ihre macOS-Instance oder Ihr macOS-Gerät für die Verwendung des öffentlichen Amazon Time Sync Service

1. Öffnen Sie Systemeinstellungen.

2. Wählen Sie Date & Time (Datum und Uhrzeit) und dann die Registerkarte Date & Time (Datum und Uhrzeit).
3. Um Änderungen vorzunehmen, wählen Sie das Schlosssymbol und geben Sie Ihr Passwort ein, wenn Sie dazu aufgefordert werden.
4. Geben Sie für Datum und Uhrzeit automatisch festlegen den Wert **`time.aws.com`** ein.

Windows

So konfigurieren Sie Ihre Windows-Instance oder Ihr Windows-Gerät für die Verwendung des öffentlichen Amazon Time Sync Service

1. Öffnen Sie das Control Panel (Bedienfeld).
2. Wählen Sie das Symbol für Date and Time (Datum und Uhrzeit).
3. Wählen Sie die Registerkarte Internet Time (Internetzeit). Diese Registerkarte ist nicht verfügbar, wenn Ihr PC in eine Domain eingebunden ist. In diesem Fall synchronisiert er die Zeit mit dem Domain-Controller. Sie können den Controller für die Verwendung des öffentlichen Amazon Time Sync Service konfigurieren.
4. Wählen Sie Change settings (Einstellungen ändern).
5. Aktivieren Sie das Kontrollkästchen für Mit einem Internet-Zeitserver synchronisieren.
6. Geben Sie neben Server den Wert **`time.aws.com`** ein.

So konfigurieren Sie Ihre Windows Server-Instance oder Ihr Windows Server-Gerät für die Verwendung des öffentlichen Amazon Time Sync Service

- Folgen Sie den Anweisungen von Microsoft, um Ihre Registry zu aktualisieren.

Vergleichen von Zeitstempeln für Ihre Linux-Instances

Wenn Sie den Amazon Time Sync Service verwenden, können Sie die Zeitstempel Ihrer Amazon-EC2-Linux-Instances mit ClockBound vergleichen, um den tatsächlichen Zeitpunkt eines Ereignisses zu ermitteln. ClockBound misst die Taktgenauigkeit Ihrer EC2-Instance und ermöglicht es Ihnen zu überprüfen, ob sich ein bestimmter Zeitstempel in Bezug auf die aktuelle Uhr Ihrer Instance in der Vergangenheit oder Zukunft befindet. Diese Informationen sind wertvoll, um die Reihenfolge und Konsistenz von Ereignissen und Transaktionen über EC2-Instances hinweg unabhängig vom geografischen Standort jeder Instance zu bestimmen.

ClockBound ist ein Daemon und eine Bibliothek auf Open-Source-Basis. Weitere Informationen über ClockBound, einschließlich Installationsanweisungen, finden Sie unter ClockBound auf GitHub.

ClockBound wird nur für Linux-Instances unterstützt.

Bei Verwendung der direkten PTP-Verbindung mit der PTP-Hardware-Uhr unterschätzt Ihr Zeit-Daemon (beispielsweise chrony) die Zeitfehlergrenze. Das liegt daran, dass eine PTP-Hardware-Uhr im Gegensatz zu NTP nicht die richtigen Informationen zur Fehlergrenze an chrony übergibt. Folglich geht Ihr Daemon für die Zeitsynchronisierung davon aus, dass die UTC-Zeit der Uhr korrekt ist, und verwendet daher eine Fehlergrenze von `0`. Zur Messung der gesamten Fehlergrenze berechnet das Nitro-System die Fehlergrenze der PTP-Hardware-Uhr und macht sie über das ENA-Treiberdateisystem `sysfs` für Ihre EC2-Instance verfügbar. Dies ist direkt als Wert in Nanosekunden lesbar.

De PTP-Hardware-Uhr abrufen

1. Rufen Sie zunächst mithilfe eines der folgenden Befehle den korrekten Standort der PTP-Hardware-Uhr ab. Der Pfad im Befehl unterscheidet sich je nach AMI, das zum Starten der Instance verwendet wird.

   - Für Amazon Linux 2:

     ```
     cat /sys/class/net/eth0/device/uevent | grep PCI_SLOT_NAME
     ```

   - Für Amazon Linux 2023:

     ```
     cat /sys/class/net/ens5/device/uevent | grep PCI_SLOT_NAME
     ```

   Die Ausgabe gibt den PCI-Steckplatz an, an dem sich die PTP-Hardware-Uhr befindet. In diesem Beispiel ist der Speicherort `0000:00:03.0`.

   ```
   PCI_SLOT_NAME=0000:00:03.0
   ```

2. Führen Sie den folgenden Befehl aus, um den PTP-Hardware-Zeitfehler abzurufen. Geben Sie den PCI-Steckplatznamen aus dem vorherigen Schritt an.

   ```
   cat /sys/bus/pci/devices/0000:00:03.0/phc_error_bound
   ```

   Die Ausgabe gibt die Zeitfehlergrenze der PTP-Hardware-Uhr in Nanosekunden an.

Um bei Verwendung der direkten PTP-Verbindung mit der PTP-Hardware-Uhr die korrekte Zeitfehlergrenze für einen bestimmten Zeitpunkt zu berechnen, müssen Sie die Zeitfehlergrenze von chrony oder von ClockBound zu dem Zeitpunkt, zu dem chrony die PTP-Hardware-Uhr abfragt, addieren. Weitere Informationen zur Messung und Überwachung der Zeitgenauigkeit finden Sie unter Verwalten der Zeitgenauigkeit von Amazon-EC2-Instances mithilfe von Amazon Time Sync Service und Amazon CloudWatch – Teil 1.

Ändern der Zeitzone für Ihre Instance

Amazon-EC2-Instances werden standardmäßig auf die Zeitzone UTC (Coordinated Universal Time) festgelegt. Sie können die Zeit für eine Instance auf die lokale Zeitzone oder auf eine andere Zeitzone in Ihrem Netzwerk festlegen.

Verwenden Sie die Anleitung für das Betriebssystem Ihrer Instance.

Linux

> **Important**
>
> Diese Informationen gelten für Amazon Linux. Weitere Informationen zu anderen Verteilungen finden Sie in der jeweiligen Dokumentation.

So ändern Sie die Zeitzone in Amazon Linux

1. Zeigen Sie die aktuelle Zeitzoneneinstellung des Systems an.

   ```
   [ec2-user ~]$ timedatectl
   ```

2. Listen Sie die verfügbaren Zeitzonen auf.

   ```
   [ec2-user ~]$ timedatectl list-timezones
   ```

3. Legen Sie die ausgewählte Zeitzone fest.

   ```
   [ec2-user ~]$ sudo timedatectl set-timezone America/Vancouver
   ```

4. (Optional) Bestätigen Sie durch erneutes Ausführen des Befehls timedatectl, dass die aktuelle Zeitzone auf die neue Zeitzone geändert wird.

```
[ec2-user ~]$ timedatectl
```

Windows

So ändern Sie die Zeitzone für eine Windows-Instance

1. Öffnen Sie in Ihrer Instance ein Eingabeaufforderungsfenster.
2. Ermitteln Sie die Zeitzone, die in Ihrer Instance verwendet wird. Mit dem folgenden Befehl zeigen Sie eine Liste aller Zeitzonen an:

   ```
   tzutil /l
   ```

   Dieser Befehl gibt eine Liste mit allen verfügbaren Zeitzonen im folgenden Format zurück:

   ```
   display name
   time zone ID
   ```
3. Ermitteln Sie die ID der Zeitzone, die Sie der Instance zuordnen möchten.
4. Beispiel: Die UTC-Zeitzone zuweisen:

   ```
   tzutil /s "UTC"
   ```

   Beispiel: Pazifische Standardzeit zuweisen:

   ```
   tzutil /s "Pacific Standard Time"
   ```

Wenn Sie die Zeitzone für eine Windows-Instance ändern, müssen Sie sicherstellen, dass die Zeitzone bei Systemneustarts erhalten bleibt. Andernfalls ändert sich die Zeit beim Neustart einer Instance wieder in UTC. Sie können Ihre Zeitzoneneinstellung beibehalten, indem Sie einen RealTimeIsUniversal-Registrierungsschlüssel hinzufügen. Dieser Schlüssel wird standardmäßig für alle Instances der aktuellen Generation festgelegt. Informationen zum Überprüfen, ob der Registrierungsschlüssel RealTimeIsUniversal festgelegt ist, finden Sie im folgenden Verfahren unter Schritt 3. Ist der Schlüssel nicht festgelegt, führen Sie die folgenden Schritte von Anfang an aus.

So legen Sie den RealTimeIsUniversal-Registrierungsschlüssel fest

1. Öffnen Sie in der Instance ein Eingabeaufforderungsfenster.
2. Verwenden Sie den folgenden Befehl, um den Registrierungsschlüssel hinzuzufügen:

```
reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation" /
v RealTimeIsUniversal /d 1 /t REG_DWORD /f
```

3. Stellen Sie sicher, dass die Instance den Schlüssel erfolgreich gespeichert hat, bevor Sie folgenden Befehl ausführen (optional):

```
reg query "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control
\TimeZoneInformation" /s
```

Dieser Befehl gibt die Unterschlüssel für den Registrierungsschlüssel TimeZoneInformation zurück. Die Ausgabe des RealTimeIsUniversal-Schlüssels am Ende der Liste sollte ähnlich dem folgenden Beispiel aussehen:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation
    Bias                            REG_DWORD     0x1e0
    DaylightBias                    REG_DWORD     0xfffffc4
    DaylightName                    REG_SZ        @tzres.dll,-211
    DaylightStart                   REG_BINARY    00000300020002000000000000000000
    StandardBias                    REG_DWORD     0x0
    StandardName                    REG_SZ        @tzres.dll,-212
    StandardStart                   REG_BINARY    00000B0001000200000000000000000
    TimeZoneKeyName                 REG_SZ        Pacific Standard Time
    DynamicDaylightTimeDisabled     REG_DWORD     0x0
    ActiveTimeBias                  REG_DWORD     0x1a4
    RealTimeIsUniversal             REG_DWORD     0x1
```

EC2 Capacity Manager

Mit Amazon EC2 Capacity Manager können Sie Ihre Kapazitätsnutzung für On-Demand-Instances, Spot Instances und Kapazitätsreservierungen von einem einzigen Standort aus überwachen, analysieren und verwalten. Capacity Manager vereinfacht die Kapazitätsverfolgung durch ein einheitliches Dashboard, das Ihre Nutzungsdaten mit stündlichen Aktualisierungen und Optimierungsmöglichkeiten zusammenfasst.

Capacity Manager wurde für große Unternehmen und Organisationen mit mehreren Konten entwickelt und macht die manuelle Datenerfassung aus mehreren Quellen überflüssig. Das Tool bietet tiefe Einblicke in Ihre AWS-Regionen. Sie können detaillierte Kapazitätsmetriken einsehen und sofort Maßnahmen zur Optimierung Ihrer Cloud-Ressourcen ergreifen.

Wenn Sie die Integration mit AWS Organizations aktivieren, können Sie die Kapazitätsdaten aller Mitgliedskonten in Ihrer Organisation von einem einzigen Dashboard aus anzeigen und analysieren. Ohne Organizations-Integration überwacht Capacity Manager nur Ressourcen innerhalb des einzelnen AWS-Konto, für das er aktiviert ist.

> **Note**
>
> - Sie können Capacity Manager nur in einer AWS-Region pro Konto aktivieren.
> - Bei allen in Capacity Manager angezeigten Kosten handelt es sich um geschätzte Kosten, die auf veröffentlichten On-Demand-Preisen basieren. Diese Schätzungen beinhalten keine Rabatte wie Savings Plans oder Reserved Instances. Die aktuellen Kosten unterscheiden sich möglicherweise von dieser Schätzung.

Wichtigste Funktionen

- Zentralisiertes Dashboard: Zeigen Sie die Kapazitätsnutzung in allen Konten und Regionen an, wobei stündlich neue Datenpunkte aktualisiert werden
- Kontoübergreifende Sichtbarkeit: Ansicht für Administratorkonten auf Organisationsebene
- Datenexporte: Exportieren von Kapazitätsdaten nach Amazon S3
- APIs: Programmgesteuerter Zugriff auf Kapazitätsmetriken und -daten
- Flexible Analyse: Dynamische Datumsauswahl zur Untersuchung der Kapazitätsnutzung in verschiedenen Zeiträumen der letzten 90 Tage
- Umfassende Metriken und Dimensionen: Zugriff auf mehr als 30 Metriken für mehrere Messeinheiten (vCPUs, Instances, geschätzte Kosten) mit umfangreichen Filterfunktionen, darunter Konto-ID, Region, Instance-Familie, Availability Zone, Instance-Typ, Plattform, Tenancy und reservierungsspezifische Dimensionen

EC2 Capacity Manager aktivieren

Capacity Manager kann je nach Ihren Anforderungen auf zwei verschiedenen Ebenen aktiviert werden. Sie können den Service für ein einzelnes AWS-Konto aktivieren, um nur Ressourcen innerhalb dieses Kontos zu überwachen, oder ihn in AWS Organizations integrieren, um einen zentralen Überblick über alle Mitgliedskonten in Ihrer Organisation zu erhalten.

- Organisationsebene: Sehen und analysieren Sie die Kapazitätsdaten aller Mitgliedskonten in Ihrer Organisation von einem einzigen Dashboard aus.
- Kontoebene: Überwachen Sie die Kapazitätsnutzung innerhalb eines einzelnen AWS-Konto.

Themen

- EC2 Capacity Manager mit AWS Organizations aktivieren
- EC2 Capacity Manager auf Kontoebene aktivieren
- Registrieren eines delegierten Administrators
- Verwenden von serviceverknüpften Rollen für EC2 Capacity Manager

EC2 Capacity Manager mit AWS Organizations aktivieren

Sie können EC2 Capacity Manager with AWS Organizations aktivieren, um Ihre Kapazität auf Organisationsebene für alle Mitgliedskonten sichtbar zu machen und zu verwalten. Diese Integration ermöglicht es Ihnen, die Kapazitätsnutzung von einem zentralen Ort aus zu überwachen, zu analysieren und zu verwalten.

Das Verwaltungskonto ist dafür verantwortlich, den Zugriff auf Organisationsebene zu ermöglichen und die Kapazität in der gesamten Organisation zu verwalten.

Die Aktivierung von Capacity Manager mit AWS Organizations bietet die folgenden Vorteile:

- Zentralisierte Kapazitätstransparenz – Zeigen Sie die Kapazitätsnutzung aller Mitgliedskonten in Ihrer Organisation über ein einziges Dashboard mit konto- und regionsübergreifender Aggregation an.
- Organisationsweite Optimierung – Identifizieren Sie ungenutzte Kapazitätsreservierungen und Optimierungsmöglichkeiten für alle Konten in Ihrer Organisation.
- Delegierter Administrator – Erlauben Sie bestimmten Mitgliedskonten die Verwaltung des Capacity Managers für eine Organisation und behalten Sie gleichzeitig die richtigen Zugriffskontrollen bei.

Wenn Sie die Integration mit AWS Organizations nicht aktivieren, können Sie nur die Ressourcen des einzelnen AWS-Konto überwachen, für das Sie Capacity Manager aktiviert haben.

Voraussetzungen

- Sie müssen über eine AWS-Organizations-Einrichtung mit einem Verwaltungskonto und einem oder mehreren Mitgliedskonten verfügen. Weitere Informationen zu den verschiedenen Kontotypen finden Sie unter Terminologie und Konzepte im Benutzerhandbuch zu AWS Organizations.
- Das Verwaltungskonto muss über Berechtigungen für die folgenden IAM-Aktionen verfügen:
  - `organizations:EnableAwsServiceAccess`
  - `organizations:RegisterDelegatedAdministrator` (bei Verwendung der delegierten Administration)
  - `iam:CreateServiceLinkedRole`
- Sie müssen eine serviceverknüpfte Rolle mit dem Anwendungsfall AWSEC2CapacityManagerServiceRolePolicy erstellen, um AWS Organizations Zugriff zu gewähren. Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle für Capacity Manager.

Capacity Manager mit AWS Organizations aktivieren

Ermöglichen Sie mithilfe des Verwaltungskontos den Organisationszugriff in Capacity Manager.

Console

So ermöglichen Sie den Organisationszugriff in Capacity Manager

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Capacity Manager aus.
3. Wählen Sie die Registerkarte Einstellungen.
4. Wählen Sie im Abschnitt Vertrauenswürdiger Zugriff die Option Vertrauenswürdigen Zugriff verwalten aus.
5. Wählen Sie in dem daraufhin angezeigten Prompt die Option Vertrauenswürdigen Zugriff aktivieren aus. Wählen Sie dann Save (Speichern) aus.

AWS CLI

So ermöglichen Sie den Organisationszugriff in Capacity Manager

1. Erstellen einer serviceverknüpften Rolle

```
aws iam create-service-linked-role --aws-service-name
 ec2.capacitymanager.amazonaws.com
```

2. Zugriff für AWS Organizations ermöglichen

```
aws organizations enable-aws-service-access --service-principal
 ec2.capacitymanager.amazonaws.com
```

3. Capacity Manager mit AWS Organizations aktivieren

```
aws ec2 enable-capacity-manager --organizations-access
```

Führen Sie zum Aktualisieren des Organisationszugriffs für einen vorhandenen Capacity Manager den folgenden Befehl aus:

```
aws ec2 update-capacity-manager-organizations-access --organizations-access
```

Überprüfen, ob Capacity Manager in Ihrer Organisation aktiviert ist

Console

So überprüfen Sie, ob Capacity Manager in Ihrer Organisation aktiviert ist

1. Wählen Sie in der Capacity-Manager-Konsole Einstellungen aus.

2. Vergewissern Sie sich, dass im Abschnitt Vertrauenswürdiger Zugriff die Option Organisationszugriff als Aktiviert angezeigt wird.
3. Vergewissern Sie sich, dass in der Organisations-ID die ID Ihrer Organisation angezeigt wird.

AWS CLI

So überprüfen Sie, ob Capacity Manager in Ihrer Organisation aktiviert ist

Führen Sie den folgenden Befehl aus:

```
aws ec2 get-capacity-manager-attributes
```

Die Ausgabe sollte folgendes anzeigen:

```
{
    "CapacityManagerStatus": "enabled",
    "OrganizationsAccess": true,
    "IngestionStatus": "initial-ingestion-pending",
    "IngestionStatusMessage": "Capacity Manager is collecting historical data from
 2025-10-01T00:00:00Z. Data collection is in progress and may take several hours to
 complete."
}
```

Überlegungen

- Erstellung von serviceverknüpften Rollen: Wenn Sie den Organisationszugriff über die Konsole ermöglichen, erstellt Capacity Manager automatisch die serviceverknüpfte AWSServiceRoleForEC2CapacityManager-Rolle in allen Mitgliedskonten. Wenn Sie die Aktivierung über die AWS CLI vornehmen, müssen Sie `createServiceLinkedRole` manuell aufrufen.
- Datenaggregation: Nachdem der Organisationszugriff aktiviert wurde, füllt Capacity Manager historische Daten von 14 Tagen aus allen Mitgliedskonten wieder auf. Dieser Prozess dauert in der Regel einige Minuten, um den Vorgang abzuschließen.
- Regionale Einschränkungen: Sie können Capacity Manager nur in einer Region pro Organisation aktivieren, es werden jedoch Daten aus allen kommerziellen Regionen aggregiert.

- Berechtigungen: Mitgliedskonten müssen keine Aktion durchführen. Capacity Manager verwendet die serviceverknüpfte Rolle, um Ressourcen in allen Konten automatisch zu ermitteln.

EC2 Capacity Manager auf Kontoebene aktivieren

Aktivieren Sie Capacity Manager auf Kontoebene, um Ihre EC2-Kapazitätsnutzung innerhalb eines einzelnen AWS-Kontos zu überwachen und zu analysieren. Nach der Aktivierung sammelt Capacity Manager Daten über Ihre On-Demand-Instances, Spot Instances und Kapazitätsreservierungen, um Sie bei der Identifizierung von Optimierungsmöglichkeiten und der Nachverfolgung von Nutzungsmustern zu unterstützen.

Capacity Manager auf Kontoebene aktivieren

Console

So aktivieren Sie Capacity Manager für Ihr Konto

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Capacity Manager aus.
3. Wählen Sie auf der Capacity-Manager-Seite die Option In Region aktivieren aus.

AWS CLI

So aktivieren Sie Capacity Manager für Ihr Konto

Führen Sie den folgenden Befehl aus:

```
aws ec2 enable-capacity-manager
```

Note

- Nachdem Sie Capacity Manager aktiviert haben, sammelt und aggregiert Capacity Manager historische Daten aus 14 Tagen. Dieser Vorgang kann einige Stunden dauern.
- Während der Erfassung Ihrer historischen Daten wird ein `initial-ingestion-in-progress`-Status angezeigt. Während dieses Erfassungszeitraums können Sie Lücken in

Ihren historischen Daten feststellen. Sobald die Datenerfassung abgeschlossen ist, wird ein `ingestion-complete`-Status angezeigt.

Registrieren eines delegierten Administrators

Sie können einen delegierten Administrator für Capacity Manager registrieren. Auf diese Weise kann ein Mitgliedskonto Capacity Manager für Ihre AWS-Organisation verwalten. Nur das Verwaltungskonto kann einen delegierten Administrator in Ihrer Organisation registrieren oder entfernen.

> **Note**
>
> Sie können Capacity Manager für Ihre Organisation nicht deaktivieren, solange es einen registrierten delegierten Administrator gibt.

Themen

- Voraussetzungen
- Einen delegierten Administrator registrieren
- Einen delegierten Administrator entfernen

Voraussetzungen

Ihr Verwaltungskonto muss Capacity Manager with AWS Organizations aktiviert haben. Weitere Informationen finden Sie unter EC2 Capacity Manager mit AWS Organizations aktivieren.

Einen delegierten Administrator registrieren

Sie können einen delegierten Administrator über die Amazon-EC2-Konsole oder die AWS CLI registrieren.

Console

Registrieren Sie einen delegierten Administrator wie folgt

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Capacity Manager aus.

3. Wählen Sie die Registerkarte Einstellungen.
4. Wählen Sie im Bereich Delegierter Administrator die Option Hinzufügen aus.
5. Geben Sie im angezeigten Prompt die Konto-ID des Organisationsmitglieds ein, das Sie als delegierten Administrator hinzufügen möchten.
6. Wählen Sie Add delegated administrator (Delegierten Administrator hinzufügen).

AWS CLI

Registrieren Sie einen delegierten Administrator wie folgt

Führen Sie den folgenden Befehl aus:

```
aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal ec2.capacitymanager.amazonaws.com
```

Einen delegierten Administrator entfernen

Sie können einen delegierten Administrator mit der Amazon-EC2-Konsole oder der AWS CLI entfernen.

Console

So entfernen Sie einen delegierten Administrator

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Capacity Manager aus.
3. Wählen Sie die Registerkarte Einstellungen.
4. Wählen Sie im Bereich Delegierter Administrator die Option Verwalten aus.
5. Wählen Sie im angezeigten Prompt Delegierten Administrator entfernen aus.

AWS CLI

So entfernen Sie einen delegierten Administrator

Führen Sie den folgenden Befehl aus:

```
aws organizations deregister-delegated-administrator \
    --account-id 123456789012 \
    --service-principal ec2.capacitymanager.amazonaws.com
```

Verwenden von serviceverknüpften Rollen für EC2 Capacity Manager

EC2 Capacity Manager verwendet serviceverknüpfte Rollen von AWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit Capacity Manager verknüpft ist. Serviceverknüpfte Rollen werden von Capacity Manager vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer AWS-Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle macht die Einrichtung von Capacity Manager einfacher, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Capacity Manager definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, kann nur Capacity Manager die Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre Capacity-Manager-Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für Capacity Manager

Capacity Manager verwendet die serviceverknüpfte Rolle mit dem Namen AWSServiceRoleForEC2CapacityManager, um Kapazitätsressourcen zu verwalten und die Integration mit AWS Organizations in Ihrem Namen zu ermöglichen.

Die serviceverknüpfte Rolle AWSServiceRoleForEC2CapacityManager vertraut den folgenden Services, die Rolle zu übernehmen:

- `ec2.capacitymanager.amazonaws.com`

Die Rollenberechtigungsrichtlinie mit dem Namen AWSEC2CapacityManagerServiceRolePolicy erlaubt es Capacity Manager, die folgenden Aktionen auszuführen:

- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListChildren`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListDelegatedAdministrators`

Sie müssen Berechtigungen konfigurieren, damit eine Benutzer, Gruppen oder Rollen eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen können. Weitere Informationen finden Sie unter serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen einer serviceverknüpften Rolle für Capacity Manager

Sie können die IAM-Konsole verwenden, um eine serviceverknüpfte Rolle mit dem Anwendungsfall AWSEC2CapacityManagerServiceRolePolicy zu erstellen. Erstellen Sie in der AWS CLI oder der AWS-API eine serviceverknüpfte Rolle mit dem Servicenamen `ec2.capacitymanager.amazonaws.com`. Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpften Rolle für Capacity Manager

Capacity Manager erlaubt es Ihnen nicht, die serviceverknüpfte Rolle AWSServiceRoleForEC2CapacityManager zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Capacity Manager

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte

juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpften Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

> **Note**
>
> Wenn der Capacity-Manager-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

So entfernen Sie Capacity-Manager-Ressourcen, die von AWSServiceRoleForEC2CapacityManager verwendet werden

1. Alle delegierten Administratoren müssen ihren Capacity Manager deaktiviert haben, bevor sie Organisationen den Zugriff entziehen können.
2. Sie müssen alle aktiven Datenexporte löschen, bevor Sie einen Kapazitätsmanager deaktivieren können.

So löschen Sie die -servicegebundene Rolle mit IAM

Verwenden Sie die IAM-Konsole, die AWS CLI oder die AWS-API, um die serviceverknüpfte Rolle AWSServiceRoleForEC2CapacityManager zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte Capacity-Manager-Rollen

Capacity Manager unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen erhalten Sie unter AWS-Regionen und Endpunkte.

Capacity Manager unterstützt die Verwendung von serviceverknüpften Rollen nicht in allen Regionen, in denen der Service verfügbar ist. Sie können die Rolle AWSServiceRoleForEC2CapacityManager in den folgenden Regionen verwenden.

Name der Region	Regions-ID	Support in Capacity Manager
USA Ost (Nord-Virginia)	us-east-1	Ja

Name der Region	Regions-ID	Support in Capacity Manager
USA Ost (Ohio)	us-east-2	Ja
USA West (Nordkalifornien)	us-west-1	Ja
USA West (Oregon)	us-west-2	Ja
Afrika (Kapstadt)	af-south-1	Nein
Asien-Pazifik (Hongkong)	ap-east-1	Nein
Asien-Pazifik (Jakarta)	ap-southeast-3	Nein
Asien-Pazifik (Mumbai)	ap-south-1	Ja
Asien-Pazifik (Osaka)	ap-northeast-3	Ja
Asien-Pazifik (Seoul)	ap-northeast-2	Ja
Asien-Pazifik (Singapore)	ap-southeast-1	Ja
Asien-Pazifik (Sydney)	ap-southeast-2	Ja
Asien-Pazifik (Tokyo)	ap-northeast-1	Ja
Kanada (Zentral)	ca-central-1	Ja
Europa (Frankfurt)	eu-central-1	Ja
Europa (Ireland)	eu-west-1	Ja
Europa (London)	eu-west-2	Ja
Europa (Mailand)	eu-south-1	Nein
Europa (Paris)	eu-west-3	Ja
Europa (Stockholm)	eu-north-1	Ja
Naher Osten (Bahrain)	me-south-1	Nein

Name der Region	Regions-ID	Support in Capacity Manager
Naher Osten (VAE)	me-central-1	Nein
Südamerika (São Paulo)	sa-east-1	Ja
AWS GovCloud (USA-Ost)	us-gov-east-1	Nein
AWS GovCloud (USA-West)	us-gov-west-1	Nein

Ihre Daten in Capacity Manager organisieren

Capacity Manager verwendet eine Kombination aus Metriken, Datenpunkten, Dimensionen, Datumsbereichen und Zeiträumen, um Ihre Kapazitätsdaten zu organisieren. Dies kann Ihnen helfen, Nutzungsmuster zu analysieren und fundierte Entscheidungen über Ihre Ressourcen zu treffen.

Metriken und Datenpunkte

Eine Metrik ist ein chronologisch sortierter Satz von Datenpunkten. Wenn Sie beispielsweise die Spot-Nutzung in vCPUs überwachen möchten, verwenden Sie die Metrik `SpotTotalUsageHrsVcpu`.

Jede Stunde generiert die Metrik einen Datenpunkt mit Zeitstempel und der Spot-Nutzung in vCPU-Stunden. Wenn Sie beispielsweise 100 vCPUs in der Stunde von 10:00 Uhr verwendet haben, erstellt Capacity Manager einen Datenpunkt mit einem Zeitstempel von 10:00 Uhr und einem Wert von 100.

Eine vollständige Liste der Metriken, die Capacity Manager analysiert, finden Sie unter Metriken von EC2 Capacity Manager.

Dimensionen

Dimensionen sind Name-Wert-Paare, die Ihnen helfen, verschiedene Aspekte einer Metrik zu kategorisieren und zu identifizieren. Beispielsweise lautet der Name einer Dimension in Capacity Manager AccountID, wobei der Wert die tatsächliche Konto-ID ist. Capacity Manager bietet Dimensionen zum Segmentieren und Gruppieren Ihrer Daten wie Instance-Familie, Reservierungs-ARN, Reservierungstyp und Tenancy.

Eine vollständige Liste der Dimensionen finden Sie unter Metriken von EC2 Capacity Manager.

Datumsbereich und Zeitraum

Der Datumsbereich gibt an, wie viel Zeit Sie analysieren möchten, von einer Stunde bis zu 90 Tagen. Der Zeitraum bestimmt, wie Capacity Manager Ihre Daten im Laufe der Zeit aggregiert und wie viele Datenpunkte zurückgegeben werden. Wenn Ihr Datumsbereich beispielsweise eine Woche und Ihr Zeitraum 1 Tag beträgt, gibt Capacity Manager 7 Datenpunkte zurück. Jeder Datenpunkt steht für einen Tag mit aggregierten Daten. Der Zeitraum muss ein Intervall von einer Stunde sein und gleichmäßig in den Datumsbereich aufgeteilt werden.

Themen

- Metriken von EC2 Capacity Manager
- Daten gruppieren und filtern

Metriken von EC2 Capacity Manager

Capacity Manager bietet eine umfassende Auswahl an Metriken zur Erfassung Ihrer Kapazität über verschiedene Ressourcentypen hinweg. Metriken können je nach Ihren Analyseanforderungen mit unterschiedlichen Einheiten gemessen werden.

Die Metriknamen in Capacity Manager verwenden vier verschiedene Präfixe, um die Art der gemessenen Kapazität zu kategorisieren:

- `Reservation` – Die Kapazitätsreservierungen selbst, einschließlich der gesamten reservierten Kapazität, der Nutzungsraten, der ungenutzten Kapazität und der Anzahl der Reservierungen.
- `Reserved` – Nutzung von On-Demand-Instances, die durch Ihre Kapazitätsreservierungen abgedeckt ist.
- `Unreserved` – Nutzung von On-Demand-Instances, die nicht von Kapazitätsreservierungen abgedeckt ist.
- `Spot` – Speziell für die Nutzung von Spot Instances, einschließlich Laufzeit und geschätzter Kosten. Diese Metriken sind unabhängig von der reservierungsbasierten Kapazität.

Die folgende Tabelle enthält auch die verfügbaren Dimensionen für jede Metrik. Die Dimensionskategorien werden wie folgt aufgeschlüsselt:

- Allgemeine Kapazitätsdimensionen – Konto-ID, Region, Instance-Familie, Availability Zone, Instance-Typ, Plattform und Tenancy
- Dimensionen der Kapazitätsreservierung – Reservierungs-ID (Kapazitätsreservierungs-ID), Reservierungs-ARN, ungenutzter finanzieller Eigentümer, Reservierungstyp (ODCR/

Kapazitätsblock), Erstellungszeitstempel, Startzeitstempel, Endzeitstempel, Status und Instance entsprechen den Kriterien.

- Dimensionen für reservierte Nutzung – Reservierungs-ID (CRID), Reservierungs-ARN, Reservierungstyp

Metrik	Beschreibung	Verfügbare Dimensionen	Verfügbare Einheiten
`ReservationTotalCapacityHrs`	Gesamtkapazität, die Sie im ausgewählten Zeitraum über Kapazitätsreservierungen reserviert haben.	Allgemeine Dimensionen für Kapazität und Kapazitätsreservierung	vCPU, Instance
`ReservationTotalEstimatedCost`	Geschätzte Kosten der Gesamtkapazitätsstunden, die im gewählten Zeitraum reserviert wurden.	Allgemeine Dimensionen für Kapazität und Kapazitätsreservierung	
`ReservationMaxSize`	Die maximale Größe, die Ihre Kapazitätsreservierung zu einem beliebigen Zeitpunkt im ausgewählten Zeitraum erreicht hat. Reservierungs-ID erforderlich.	Allgemeine Dimensionen für Kapazität und Kapazitätsreservierung	vCPU, Instance
`ReservationMinSize`	Die Mindestgröße, die Ihre Kapazitätsreservierung zu einem beliebigen Zeitpunkt im ausgewählten Zeitraum erreicht hat. Reservierungs-ID erforderlich.	Allgemeine Dimensionen für Kapazität und Kapazitätsreservierung	vCPU, Instance
`ReservationUnusedT`	Gesamtmenge der reservierten Kapazität, die Sie im ausgewähl	Allgemeine Dimensionen für Kapazität	vCPU, Instance

Metrik	Beschreibung	Verfügbare Dimensionen	Verfügbare Einheiten
`otalCapacityHrs`	ten Zeitraum hatten, aber nicht genutzt haben.	und Kapazitätsreservierung	
`ReservationUnusedTotalEstimatedCost`	Geschätzte Kosten der reservierten Kapazität, die Sie im ausgewählten Zeitraum hatten, aber nicht genutzt haben (berechnet anhand von On-Demand-Tarifen).	Allgemeine Dimensionen für Kapazität und Kapazitätsreservierung	
`ReservationMaxUnusedSize`	Die maximale Menge an ungenutzter Kapazität in Ihrer Kapazitätsreservierung zu einem beliebigen Zeitpunkt während des ausgewählten Zeitraums. Reservierungs-ID erforderlich.	Allgemeine Dimensionen für Kapazität und Kapazitätsreservierung	vCPU, Instance
`ReservationMinUnusedSize`	Die Mindestmenge an ungenutzter Kapazität in Ihrer Kapazitätsreservierung zu einem beliebigen Zeitpunkt während des ausgewählten Zeitraums. Reservierungs-ID erforderlich.	Allgemeine Dimensionen für Kapazität und Kapazitätsreservierung	vCPU, Instance
`ReservationMaxUtilization`	Der maximale Nutzungsprozentsatz, den Ihre Kapazitätsreservierung zu einem beliebigen Zeitpunkt im ausgewählten Zeitraum erreicht hat. Reservierungs-ID erforderlich.	Allgemeine Dimensionen für Kapazität und Kapazitätsreservierung	

Metrik	Beschreibung	Verfügbare Dimensionen	Verfügbare Einheiten
`ReservationMinUtilization`	Die prozentuale Mindestauslastung, die Ihre Kapazitätsreservierung zu einem beliebigen Zeitpunkt im ausgewählten Zeitraum erreicht hat. Reservierungs-ID erforderlich.	Allgemeine Dimensionen für Kapazität und Kapazitätsreservierung	
`ReservationAvgUtilization`	Der durchschnittliche Prozentsatz Ihrer reservierten Kapazität, der im ausgewählten Zeitraum genutzt wurde.	Allgemeine Dimensionen für Kapazität und Kapazitätsreservierung	vCPU, Instance
`ReservationTotalCount`	Die Gesamtzahl der Kapazitätsreservierungen, die Sie während des ausgewählten Zeitraums hatten.	Allgemeine Dimensionen für Kapazität und Kapazitätsreservierung	
`ReservationAvgFutureSize`	Die durchschnittliche Anzahl von Kapazitätsreservierungen, deren Start in der Zukunft geplant ist, die aber im ausgewählten Zeitraum noch nicht aktiv wurden. Die Größe wird für alle Dimensionen summiert und über die Zeit gemittelt.	Allgemeine Dimensionen für Kapazität und Kapazitätsreservierung	vCPU, Instance

Metrik	Beschreibung	Verfügbare Dimensionen	Verfügbare Einheiten
`ReservationMaxFutureSize`	Die maximale Anzahl an Kapazitätsreservierungen, deren Start in der Zukunft geplant ist, die aber im ausgewählten Zeitraum noch nicht aktiv geworden sind. Die Größe wird über alle Dimensionen hinweg summiert und der Maximalwert für den Zeitraum verwendet.	Allgemeine Dimensionen für Kapazität und Kapazitätsreservierung	vCPU, Instance
`ReservationMinFutureSize`	Die Mindestanzahl an Kapazitätsreservierungen, deren Start in der Zukunft geplant ist, aber zu keinem Zeitpunkt im ausgewählten Zeitraum aktiv geworden ist. Die Größe wird über alle Dimensionen hinweg summiert, und es wird der Mindestwert für den Zeitraum verwendet.	Allgemeine Dimensionen für Kapazität und Kapazitätsreservierung	vCPU, Instance
`ReservationAvgCommittedSize`	Die durchschnittliche Gesamtkapazität in einem aktiven oder geplanten Status mit einer Verpflichtung. Die Größe wird für alle Dimensionen summiert und über die Zeit gemittelt.	Allgemeine Dimensionen für Kapazität und Kapazitätsreservierung	vCPU, Instance

Metrik	Beschreibung	Verfügbare Dimensionen	Verfügbare Einheiten
`ReservationMaxCommittedSize`	Die maximale Gesamtkapazität in einem aktiven oder geplanten Status mit einer Verpflichtung. Die Größe wird über alle Dimensionen hinweg summiert und der Maximalwert für den Zeitraum verwendet.	Allgemeine Dimensionen für Kapazität und Kapazitätsreservierung	vCPU, Instance
`ReservationMinCommittedSize`	Die Mindestgesamtkapazität in einem aktiven oder geplanten Status mit einer Verpflichtung. Die Größe wird über alle Dimensionen hinweg summiert, und es wird der Mindestwert für den Zeitraum verwendet.	Allgemeine Dimensionen für Kapazität und Kapazitätsreservierung	vCPU, Instance
`ReservedTotalUsageHrs`	Gesamtzahl der Stunden der Nutzung der On-Demand-Instance, die im ausgewählten Zeitraum durch eine Kapazitätsreservierung abgedeckt wurden. Dies schließt die Spot-Nutzung aus.	Abmessungen für Allgemeine Kapazität und Reservierte Nutzung	vCPU, Instance
`UnreservedTotalUsageHrs`	Gesamtzahl der Stunden der Nutzung der On-Demand-Instance, die im ausgewählten Zeitraum nicht durch eine Kapazitätsreservierung abgedeckt wurden. Dies schließt die Spot-Nutzung aus.	Allgemeine Kapazitätsdimensionen	vCPU, Instance

Metrik	Beschreibung	Verfügbare Dimensionen	Verfügbare Einheiten
`ReservedTotalEstimatedCost`	Geschätzte Kosten für die Nutzung von On-Demand-Instances, die im ausgewählten Zeitraum durch eine Kapazitätsreservierung gedeckt wurde. Dies schließt die Spot-Nutzung aus.	Abmessungen für Allgemeine Kapazität und Reservierte Nutzung	
`UnreservedTotalEstimatedCost`	Geschätzte Kosten für die Nutzung von On-Demand-Instances, die im ausgewählten Zeitraum nicht durch eine Kapazitätsreservierung gedeckt wurde. Dies schließt die Spot-Nutzung aus.	Allgemeine Kapazitätsdimensionen	
`SpotTotalUsageHrs`	Gesamtzahl der Nutzungsstunden der Spot Instance im ausgewählten Zeitraum.	Allgemeine Kapazitätsdimensionen	vCPU, Instance
`SpotTotalEstimatedCost`	Geschätzte Kosten für die Nutzung von Spot Instances im ausgewählten Zeitraum (berechnet anhand der veröffentlichten Spot-Tarife).	Allgemeine Kapazitätsdimensionen	
`SpotAvgRunTimeBeforeInterruption`	Durchschnittliche Laufzeit in Stunden für Instances, die im ausgewählten Zeitraum unterbrochen wurden.	Nur die Abmessungen Region, AZ und Konto-ID	Instance
`SpotMaxRunTimeBeforeInterruption`	Maximale Laufzeit in Stunden für Instances, die im ausgewählten Zeitraum unterbrochen wurden.	Nur die Abmessungen Region, AZ und Konto-ID	Instance

Metrik	Beschreibung	Verfügbare Dimensionen	Verfügbare Einheiten
`SpotMinRunTimeBeforeInterruption`	Mindestlaufzeit in Stunden für Instances, die im ausgewählten Zeitraum unterbrochen wurden.	Nur die Abmessungen Region, AZ und Konto-ID	Instance

> **Note**
>
> Wenn Sie Instances in Ihre Einheiten aufnehmen, empfehlen wir, den Instance-Typ in Ihre Abmessungen aufzunehmen.

Daten gruppieren und filtern

Capacity Manager aggregiert Ihre Metriken auf der Grundlage der von Ihnen ausgewählten Dimensionen und des von Ihnen ausgewählten Datumszeitraums. Wenn keine Dimensionen ausgewählt wurden, aggregiert Capacity Manager die Daten und gibt einen Datenpunkt pro Zeitraum im Datumsbereich zurück. Sie können Ihre Daten in kleinere Aggregationen gruppieren, indem Sie Dimensionen hinzufügen.

- Gruppierung – Unterteilen Sie Ihre Kapazitätsdaten nach Dimensionen wie Region, Instance-Familie oder Konto-ID. Sie können Ihre Metriken nach mehreren Dimensionen gruppieren, um Ihre Daten weiter aufzuschlüsseln. Wenn Sie beispielsweise nach Region und Availability Zone gruppieren, erhalten Sie einen Datenpunkt für jede Kombination aus Region und AZ, die Sie nutzen.
- Filterung – Zeigt nur bestimmte Teilmengen der von Ihnen ausgewählten Dimensionen an. Wenn Sie beispielsweise nach Instance-Familien gruppieren, erhalten Sie Datenpunkte für alle Familien, die Sie verwenden. Wenn Sie jedoch auch nach p5 filtern, werden Ihnen nur Datenpunkte für die p5-Instance-Familie angezeigt.
- Metrische Einheiten – Zeigen Sie Ergebnisse nach verschiedenen Einheiten wie vCPUs, Instances oder geschätzten Kosten an. Nachdem Sie die Daten beispielsweise nach Regionen gruppiert und nach einer bestimmten Instance-Familie gefiltert haben, können Sie die Daten auf unterschiedliche Weise anzeigen. Wechseln Sie zwischen der Gesamtzahl der verwendeten vCPUs, der Anzahl der laufenden Instances oder den geschätzten Kosten.

So gruppieren und filtern Sie Daten in der Konsole

So gruppieren und filtern Sie Daten in Capacity Manager

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Capacity Manager aus.
3. Wählen Sie die Registerkarte für den Ressourcentyp, den Sie analysieren möchten: Nutzung, Reservierungen oder Spot.
4. Wählen Sie im Abschnitt Datumsfilter einen Datumsbereich, eine Zeitzone und ein Intervall aus.
5. Wählen Sie im Abschnitt Dimensionsfilter eine Dimension aus der Dropdownliste Dimension auswählen aus.
6. Wählen Sie in der Dropdownliste die Dimensionen aus, nach denen Sie gruppieren möchten. Beachten Sie, dass die Dimensionsoptionen für jeden Ressourcentyp unterschiedlich sind. Weitere Informationen finden Sie unter Metriken von EC2 Capacity Manager.

   Sie können mehrere Dimensionen hinzufügen, um detailliertere Gruppierungen zu erstellen.
7. Um nach den ausgewählten Dimensionen zu filtern, wählen Sie eine Filteroption aus der Dropdownliste Nach Dimension filtern aus.
8. Wählen Sie im Abschnitt Aggregationen eine Einheit aus, um Ihre Ergebnisse nach vCPUs, Instances oder geschätzten Kosten anzuzeigen.

Capacity Manager mit der AWS-Konsole navigieren

Die Capacity-Manager-Konsole ist in Registerkarten unterteilt, die verschiedene Ansichten Ihrer Kapazitätsdaten bieten:

- Dashboard – Bietet einen umfassenden Überblick über alle On-Demand-Kapazitätsreservierungen, On-Demand- und Spot-Nutzung, einschließlich wichtiger Metriken und wichtiger Warnmeldungen, um Ihren Kapazitätsstatus zu verbessern.
- Nutzung – Bietet einen Überblick über Ihre Instance-Nutzungsmuster für On-Demand- und Spot Instances. Analysieren Sie die Abdeckung anhand von Kapazitätsreservierungen und identifizieren Sie Optimierungsmöglichkeiten durch flexible Gruppierung und Filterung.
- Reservierungen – Bietet eine Analyse der Auslastung der Kapazitätsreservierungen, der Verwaltungsfunktionen und detaillierte Reservierungsmetriken für Konten und Regionen.
- Spot – Überwacht Spot-Nutzungsmuster und bietet Kostenanalysen für Spot Instances in allen Konten und Regionen.

- Datenexporte – Verwaltet die Konfiguration des Datenexports nach Amazon S3, einschließlich Planung, Formatierung und Vorlagenauswahl.
- Einstellungen – Bietet Optionen zur Servicekonfiguration, einschließlich Organisationszugriff und regionaler Einstellungen.

Auf den Registerkarten Nutzung und Reservierungen bietet Capacity Manager eine hierarchische Navigationsstruktur, die es Ihnen ermöglicht, von allgemeinen Übersichten bis hin zu detaillierten Ressourceninformationen vorzugehen. Wenn Sie dieses Navigationsmuster verstehen, können Sie Ihre Kapazitätsdaten effizient analysieren und Optimierungsmöglichkeiten identifizieren.

Themen

- Navigationshierarchie
- Sehen Sie sich die Aufschlüsselung und Einzelheiten zu Nutzung und Reservierungen an

Navigationshierarchie

Capacity Manager verwendet eine dreistufige Navigationsstruktur für Nutzung und Reservierungen:

1. Übersichtsseite – Allgemeine Zusammenfassung mit aggregierten Metriken.
2. Aufschlüsselungsseite – Detaillierte Analyse mit Filter- und Gruppierungsoptionen
3. Detailseiten:
   - Nutzungsdetails – Informationen zu Ihrer ausgewählten Dimensionskombination, die Statistiken und Zeitreihendaten bereitstellen, die Ihnen helfen, Nutzungsmuster zu verstehen.
   - Reservierungsdetails – Informationen über eine bestimmte Kapazitätsreservierung, einschließlich Nutzungsstatistiken, Nutzungsmuster im Laufe der Zeit und Konfigurationsdetails.

> **Note**
>
> Spot folgt einer vereinfachten Struktur mit nur der Übersichtsseite.

Sehen Sie sich die Aufschlüsselung und Einzelheiten zu Nutzung und Reservierungen an

Sowohl die Registerkarten Nutzung als auch Reservierungen folgen derselben dreistufigen Navigationsstruktur, sodass Sie von der Übersicht über die Aufschlüsselung zu den Detailseiten gelangen können. Die Verfahren für den Zugriff auf Aufschlüsselungs- und Detailseiten sind ähnlich, mit nur geringfügigen Unterschieden darin, wo sich die Navigationslinks innerhalb der einzelnen Tabs befinden.

Zugreifen auf die Ressourcen-Aufschlüsselungsseiten

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Capacity Manager aus.
3. Wählen Sie die Registerkarte für den Ressourcentyp, den Sie analysieren möchten: Nutzung oder Reservierungen.
4. Suchen Sie im Abschnitt Aggregationen nach dem Link zur Aufschlüsselung:

   - Nutzung: Wählen Sie in der Spalte Aktionen die Option Aufschlüsselung anzeigen aus.

     > **Note**
     >
     > Abhängig von Ihrer Bildschirmgröße oder der Anzahl der Dimensionen, die Sie angewendet haben, müssen Sie möglicherweise horizontal über die Seite scrollen, um den Link zum Anzeigen der Aufschlüsselung zu finden.

   - Reservierungen: Wählen Sie in der Spalte Reservierungen die Nummer (die Nummer ist ein Link) der Reservierung aus, die Sie sich ansehen möchten.

So greifen Sie auf die Detailseiten zu

1. Navigieren Sie auf der Aufschlüsselungsseite zum entsprechenden Abschnitt:

   - Nutzung: Der Abschnitt Eindeutige Dimensionskombinationen.
   - Reservierungen: Der Abschnitt Reservierungen.

2. Rufen Sie im entsprechenden Abschnitt der von Ihnen ausgewählten Ressourcen die Detailseite auf.

   - Nutzung: Wählen Sie in der Spalte Aktionen die Option Details anzeigen aus.

> **Note**
>
> Abhängig von Ihrer Bildschirmgröße oder der Anzahl der Dimensionen, die Sie angewendet haben, müssen Sie möglicherweise horizontal über die Seite scrollen, um den Link „Details anzeigen“ zu finden.

- Reservierungen: Wählen Sie in der Spalte Reservierungs-ID die Reservierung aus, die Sie sich ansehen möchten.

Exportieren von Capacity-Manager-Daten

Sie können Kapazitätsdaten aus EC2 Capacity Manager nach Amazon S3 zur weiteren Analyse, Berichterstattung und Integration mit anderen AWS-Services exportieren. Sie können Ihre Daten im CSV- oder Parquet-Format exportieren. In den folgenden Abschnitten finden Sie Informationen zum Exportieren von Capacity-Manager-Daten.

> **Note**
>
> Capacity Manager erlaubt nur einen Datenexport pro AWS-Konto.

Themen

- Einrichten eines Amazon-S3-Buckets für Capacity-Manager-Datenexporte
- Erstellen eines Datenexports für Ihre Capacity-Manager-Daten

Einrichten eines Amazon-S3-Buckets für Capacity-Manager-Datenexporte

Um Capacity-Manager-Datenexporte zu erhalten, müssen Sie einen Amazon-S3-Bucket in Ihrem AWS-Konto haben, um Ihre Exportdateien zu empfangen und zu speichern. Wenn Sie einen Datenexport in der Capacity-Manager-Konsole erstellen, können Sie einen vorhandenen Amazon-S3-Bucket auswählen, der Sie besitzen, oder einen neuen Bucket erstellen.

In beiden Fällen müssen Sie die erforderliche Bucket-Richtlinie anwenden, damit Capacity Manager Exportdateien liefern kann. Wenn Sie diese Richtlinie in der Amazon-S3-Konsole bearbeiten oder den Bucket-Besitzer ändern, nachdem Sie einen Datenexport erstellt haben, kann Capacity Manager Ihre Exporte nicht bereitstellen.

Informationen zum Erstellen eines Amazon-S3-Buckets finden Sie unter Erstellen eines S3-Buckets im Benutzerhandbuch für Amazon Simple Storage Service.

Die folgende Richtlinie muss auf Ihren S3-Bucket angewendet werden, damit Capacity Manager Datenexporte bereitstellen kann:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.capacitymanager.amazonaws.com"
            },
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111122223333:capacity-
manager-data-export/*"
                }
            }
        }
    ]
}
```

Diese Bucket-Richtlinie trägt dazu bei, dass Capacity-Manager-Datenexportdateien sicher an Ihren Bucket übermittelt werden können. Das heißt:

- Jedes Mal, wenn ein Capacity-Manager-Datenexport zugestellt wird, überprüft AWS zunächst, ob der Bucket noch dem Konto gehört, das den Export eingerichtet hat. Wenn sich der Besitzer

des Buckets geändert hat, wird der Export nicht zugestellt. Dies hilft, die Sicherheit der Capacity-Manager-Daten zu gewährleisten. Mit dieser Bucket-Richtlinie kann AWS (`"Effect": "Allow"`) überprüfen, welchem Konto der Bucket gehört (`"Action": ["s3:ListBucket"]`).

- Die Richtlinie gewährt dem Capacity-Manager-Service (`"Service": "ec2.capacitymanager.amazonaws.com"`) die Berechtigung, Exportdateien zu schreiben (`"Action": "s3:PutObject"`) und Objekte zu lesen (`"Action": "s3:GetObject"`), um Daten in Ihren Bucket zu kopieren.

Erstellen eines Datenexports für Ihre Capacity-Manager-Daten

Um einen Datenexport zu erstellen, können Sie die Seite Datenexporte in der Capacity-Manager-Konsole oder die AWS CLI verwenden.

Voraussetzungen

Sie müssen einen Amazon Simple Storage Service (Amazon S3)-Bucket erstellen. Stellen Sie Folgendes sicher:

- Ihr S3-Bucket muss sich in der AWS-Region befinden, in der Sie Capacity Manager aktiviert haben.
- Ihr S3-Bucket verfügt über die erforderlichen Berechtigungsrichtlinien, damit der Capacity-Manager-Service Dateien bereitstellen kann.

Weitere Informationen finden Sie unter Einrichten eines Amazon-S3-Buckets für Capacity-Manager-Datenexporte.

Verfahren

Sie können Ihre Capacity-Manager-Daten mit der AWS-Konsole oder der AWS CLI exportieren.

Console

So erstellen Sie einen Datenexport

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Capacity Manager aus.
3. Wählen Sie die Registerkarte Datenexporte.
4. Wählen Sie Export erstellen.

5. Konfigurieren Sie die Exporteigenschaften, den Lieferort und die Tags (optional).
6. Wählen Sie Erstellen aus.

AWS CLI

So erstellen Sie einen Datenexport

Verwenden Sie den folgenden Befehl, um einen Datenexport mit der angegebenen Konfiguration zu erstellen:

```
aws ec2 create-capacity-manager-data-export \
    --s3-bucket-name my-exports-bucket \
    --s3-bucket-prefix capacity-data-exports \
    --schedule hourly \
    --output-format parquet/CSV \
    --tag-specifications 'ResourceType=capacity-manager-data-
export,Tags=[{Key=environment,Value=production}]'
```

Gerätetreiber für Ihre EC2 Instanz verwalten

Gerätetreiber sind Softwarekomponenten, die mit der virtualisierten Hardware für Ihre EC2 Amazon-Instance kommunizieren. Um Systemfehler, Leistungsprobleme und anderes unerwartetes Verhalten zu vermeiden, ist es wichtig, dass Sie Ihre Treiber up-to-date behalten. Dies gilt insbesondere für Treiber, die je nach Verwendung einen starken Einfluss auf die Systemleistung haben können, z. B. Netzwerk-, Grafik- und Speichergerätetreiber. Neue Treiberversionen können Fehlerkorrekturen beinhalten oder erweiterte Funktionen einführen, die Sie möglicherweise für Instances nutzen möchten, die gerade ausgeführt werden.

Netzwerktreiber

Linux-Distributionen können Netzwerk-Feature wie Elastic Network Adapter (ENA) oder Elastic-Fabric-Adapter (EFA) in den Kernel integrieren. Der Zeitpunkt für die Implementierung von Kernel-Treiber-Feature innerhalb der verschiedenen Distributionen kann jedoch variieren.

ENA- und EFA-Linux-Kerneltreiber sind im Amazon GitHub Drivers-Repository verfügbar. Weitere Informationen und Links zu den verfügbaren Treibern finden Sie unter Amazon Drivers on GitHub.

Weitere Informationen zu ENA-Treibern finden Sie unter Ermöglichen Sie Enhanced Networking mit ENA auf Ihren EC2 Instances. Mehr Informationen über EFA-Treiber finden Sie unter Elastic Fabric Adapter für AI/ML und HPC-Workloads bei Amazon EC2 Themen Erste Schritte in diesem Handbuch.

Informationen zum Installieren oder Aktualisieren von Netzwerktreibern auf Windows-Instances finden Sie in den folgenden Themen:

- Installieren des NVIDIA-Treibers unter Windows
- Installieren der aktuellen AWS PV-Treiber

  Weitere Informationen finden Sie unter Paravirtual-Treiber für Windows-Instances.

> **Note**
>
> EFA wird von Windows-Instances nicht unterstützt.

Grafiktreiber

Informationen zum Installieren oder Aktualisieren von Grafiktreibern finden Sie in den folgenden Themen:

- AMD-Treiber für Ihre EC2-Instance
- NVIDIA-Treiber für Ihre EC2 Amazon-Instance

Speichergerätetreiber

Informationen zum Installieren oder Aktualisieren von Speichertreibern finden Sie in den folgenden Themen:

- Informationen zu Linux-Instances finden Sie unter Installieren oder Aktualisieren des NVMe Treibers im Amazon EBS-Benutzerhandbuch.
- Für Windows-Instances siehe AWS NVMe-Treiber.

AMD-Treiber für Ihre EC2-Instance

Auf Instances mit einer angeschlossenen AMD-GPU, z. B. einer G4ad-Instance, muss der entsprechende AMD-Treiber installiert sein. Je nach Ihren Anforderungen können Sie entweder ein AMI mit vorinstalliertem Treiber verwenden oder einen Treiber Amazon S3 von herunterladen.

Informationen zum Installieren von NVIDIA-Treibern auf einer Instance mit einer angeschlossenen NVIDIA-GPU, z. B. einer G4DN-Instance, finden Sie stattdessen unter NVIDIA-Treiber.

Inhalt

- AMD Radeon Pro Software für Enterprise Driver
- AMIs mit installiertem AMD-Treiber
- AMD-Treiber-Download

AMD Radeon Pro Software für Enterprise Driver

Die AMD Radeon Pro Software for Enterprise Driver wurde entwickelt, um Support für professionelle Grafik-Anwendungsfälle zu bieten. Mit dem Treiber können Sie Ihre Instances mit zwei 4K-Displays pro GPU konfigurieren.

Unterstützte APIs

- OpenGL, OpenCL
- Vulkan
- AMD Advanced Media Framework
- Video Acceleration API
- DirectX 9 und höher
- Microsoft Hardware Media Foundation Transformation

AMIs mit installiertem AMD-Treiber

AWS bietet verschiedene Amazon Machine Images (AMI) an, die mit installierten AMD-Treibern geliefert werden. Öffnen Sie Marketplace-Angebote mit AMD-Treiber.

AMD-Treiber-Download

Wenn Sie kein AMI mit dem installierten AMD-Treiber verwenden, können Sie den AMD-Treiber herunterladen und auf Ihrer Instance installieren. Nur die folgenden Betriebssystemversionen unterstützen AMD-Treiber:

- Amazon Linux 2 mit Kernel-Version 5.4
- Ubuntu 20.04
- Ubuntu 22.04
- Ubuntu 24.04
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Diese Downloads sind nur für AWS-Kunden verfügbar. Wenn Sie die Software herunterladen, stimmen Sie zu, diese nur für die Entwicklung von AMIs für den Einsatz auf AMD-Radeon-Pro-V520-Hardware zu verwenden. Durch die Installation der Software stimmen Sie den Bedingungen in der Endbenutzer-Lizenzvereinbarung für AMD zu.

AMD-Treiber auf Ihrer Amazon-Linux-2-Instance installieren

1. Herstellen einer Verbindung mit Ihrer Linux-Instance.
2. Installieren Sie die AWS CLI auf Ihrer Linux-Instance und konfigurieren Sie die Standardanmeldeinformationen. Weitere Informationen finden Sie unter Installieren der AWS CLI im AWS Command Line Interface-Benutzerhandbuch.

   > **Important**
   >
   > Ihr Benutzer oder Ihre Rolle muss über die Berechtigungen verfügen, die die AmazonS3ReadOnlyAccess-Richtlinie enthält. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinie: AmazonS3ReadOnlyAccess im Benutzerhandbuch von Amazon Simple Notification Service.

3. Kernel 5.4 installieren

```
$ sudo amazon-linux-extras disable kernel-5.10
```

```
$ sudo amazon-linux-extras enable kernel-5.4
$ sudo yum install -y kernel
```

4. Installieren Sie gcc und make, falls sie noch nicht installiert sind.

```
$ sudo yum install gcc make
```

5. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
$ sudo amazon-linux-extras install epel -y
$ sudo yum update -y
```

6. Starten Sie die Instance neu.

```
$ sudo reboot
```

7. Stellen Sie nach dem Neustart erneut eine Verbindung mit der Instance her.
8. Laden Sie den neuesten AMD-Treiber herunter.

```
$ aws s3 cp --recursive s3://ec2-amd-linux-drivers/latest/ .
```

9. Extrahieren Sie die Datei.

```
$ tar -xf amdgpu-pro-*rhel*.tar.xz
```

10. Wechseln Sie in den Ordner für den extrahierten Treiber.
11. Führen Sie das Selbstinstallationsskript aus, um den vollständigen Grafik-Stack zu installieren.

```
$ ./amdgpu-pro-install -y --opencl=pal,legacy
```

12. Starten Sie die Instance neu.

```
$ sudo reboot
```

13. Vergewissern Sie sich, dass der Treiber funktioniert.

```
$ sudo dmesg | grep amdgpu
```

Die Antwort sollte wie folgt aussehen:

```
Initialized amdgpu
```

AMD-Treiber auf Ihrer Ubuntu-Linux-Instance installieren

1. Herstellen einer Verbindung mit Ihrer Linux-Instance.
2. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
$ sudo apt-get update --fix-missing && sudo apt-get upgrade -y
```

3. Installieren Sie gcc und make, falls sie noch nicht installiert sind.

```
$ sudo apt install build-essential -y
```

4. Linux-Firmware und Kernelmodule installieren

```
$ sudo apt install linux-firmware linux-modules-extra-aws -y
```

5. Instance neu starten

```
$ sudo reboot
```

6. Stellen Sie nach dem Neustart erneut eine Verbindung mit der Instance her.
7. AMD-Linux-Treiberpaket installieren

   - Für Ubuntu 20.04:

```
$ wget https://repo.radeon.com/.preview/afe3e25b8f1beff0bb312e27924d63b5/amdgpu-install/5.4.02.01/ubuntu/focal/amdgpu-install_5.4.02.01.50402-1_all.deb
$ sudo dpkg --add-architecture i386
$ sudo apt install ./amdgpu-install_5.4.02.01.50402-1_all.deb
```

   - Für spätere Ubuntu-Versionen gehen Sie zu Linux® Drivers for AMD Radeon™ Graphics und laden Sie das neueste Ubuntu-Paket herunter und installieren Sie es.

```
$ sudo apt install ./amdgpu-install_{version-you-downloaded}.deb
```

8. Führen Sie das Selbstinstallationsskript aus, um den vollständigen Grafik-Stack zu installieren.

```
$ amdgpu-install --usecase=workstation --vulkan=pro -y
```

9. Starten Sie die Instance neu.

```
$ sudo reboot
```

10. Vergewissern Sie sich, dass der Treiber funktioniert.

```
$ sudo dmesg | grep amdgpu
```

Die Antwort sollte wie folgt aussehen:

```
Initialized amdgpu
```

AMD-Treiber auf Ihrer Windows-Instance installieren

1. Stellen Sie eine Verbindung mit Ihrer Windows-Instance her und öffnen Sie ein PowerShell-Fenster.
2. Konfigurieren der Standardanmeldeinformationen für AWS Tools for Windows PowerShell auf Ihrer Windows-Instance. Weitere Informationen finden Sie unter Erste Schritte in AWS Tools for Windows PowerShell im AWS -Tools für PowerShell-Benutzerhandbuch.

> **Important**
>
> Ihr Benutzer oder Ihre Rolle muss über die Berechtigungen verfügen, die die AmazonS3ReadOnlyAccess-Richtlinie enthält. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinie: AmazonS3ReadOnlyAccess im Benutzerhandbuch von Amazon Simple Notification Service.

3. Stellen Sie das Schlüssel-Präfix entsprechend Ihrer Windows-Version ein:

   - Windows 10 und Windows 11

   ```
   $KeyPrefix = "latest/AMD_GPU_WINDOWS10"
   ```

   - Windows Server 2016

```
$KeyPrefix = "archives"
```

- Windows Server 2019

```
$KeyPrefix = "latest/AMD_GPU_WINDOWS_2K19" # use "archives" for Windows Server
 2016
```

- Windows Server 2022

```
$KeyPrefix = "latest/AMD_GPU_WINDOWS_2K22"
```

4. Laden Sie die Treiber von Amazon S3 mit den folgenden PowerShell-Befehlen auf Ihren Desktop herunter.

```
$Bucket = "ec2-amd-windows-drivers"
$LocalPath = "$home\Desktop\AMD"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
    }
}
```

5. Entpacken Sie die heruntergeladene Treiberdatei und führen Sie das Installationsprogramm mithilfe der folgenden PowerShell-Befehle aus.

```
Expand-Archive $LocalFilePath -DestinationPath "$home\Desktop\AMD\$KeyPrefix" -
Verbose
```

Prüfen Sie als Nächstes den Inhalt des neuen Verzeichnisses. Der Verzeichnisname kann mit dem `Get-ChildItem`-PowerShell-Befehl abgerufen werden.

```
Get-ChildItem "$home\Desktop\AMD\$KeyPrefix"
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
Directory: C:\Users\Administrator\Desktop\AMD\latest
```

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----       10/13/2021  12:52 AM                210414a-365562C-Retail_End_User.2
```

Installieren der Treiber:

```
pnputil /add-driver $home\Desktop\AMD\$KeyPrefix\*.inf /install /subdirs
```

6. Befolgen Sie die Anweisungen, um den Treiber zu installieren, und starten Sie die Instance neu, wenn Sie dazu aufgefordert werden.
7. Sie können prüfen, ob die GPU richtig funktioniert, indem Sie den Geräte-Manager verwenden. Sie sollten "AMD Radeon Pro V520 MxGPU" als Grafikkarte aufgeführt sehen.
8. Um die Vorteile der vier Displays mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll Amazon DCV ein.

NVIDIA-Treiber für Ihre EC2 Amazon-Instance

Auf Instances mit einer angehängten NVIDIA-GPU, z. B. Instances der P- oder G-Serie, muss der entsprechende NVIDIA-Treiber installiert sein. Je nach Instance-Typ können Sie entweder einen öffentlichen NVIDIA-Treiber herunterladen, einen Treiber von Amazon S3 herunterladen, der nur für AWS Kunden verfügbar ist, oder ein AWS AMI mit vorinstalliertem Treiber verwenden.

Informationen zum Installieren von AMD-Treibern auf einer Instance mit einer angeschlossenen AMD-GPU, z. B. einer G4ad-Instance, finden Sie stattdessen unter AMD-Treiber.

Themen

- Typen von NVIDIA-Treibern
- Verfügbare Treiber nach Instance-Typ
- Installationsoptionen
- Verwenden Sie AMIs diese, einschließlich NVIDIA-Treiber
- Öffentliche NVIDIA-Treiber installieren
- NVIDIA-GRID-Treiber (G6-, Gr6-, G6e-, G6f-, Gr6f-, G5-, G4dn- und G3-Instances) installieren
- NVIDIA-Gaming-Treiber (G6-, G6e-, G5- und G4dn-Instances)

Typen von NVIDIA-Treibern

Im Folgenden finden Sie die wichtigsten Typen von NVIDIA-Treibern, die mit GPU-basierten Instances verwendet werden können.

Tesla-Treiber

Diese Treiber sind in erster Linie für Rechen-Workloads vorgesehen, die GPUs für Rechenaufgaben wie parallelisierte Gleitkommaberechnungen für maschinelles Lernen und schnelle Fourier-Transformationen für Hochleistungsrechneranwendungen verwendet werden.

GRID-Treiber

Diese Treiber wurden dafür zertifiziert, dass sie optimale Leistung für professionelle Visualisierungsanwendungen bieten, die Inhalte wie 3D-Modelle oder hochauflösende Videos rendern. Sie können GRID-Treiber zum Support zweier Modi konfigurieren. Quadro Virtual Workstations bieten pro GPU Zugriff auf vier 4K-Displays. GRID vApps bieten RDSH-App-Hosting-Funktionen.

Gaming-Treiber

Diese Treiber enthalten Optimierungen für Spiele und werden häufig aktualisiert, um Leistungsverbesserungen zu bieten. Sie unterstützen ein einzelnes 4K-Display pro GPU.

Konfigurierter Modus

Unter Windows sind die Tesla-Treiber so konfiguriert, dass sie im TCC-Modus (Tesla Compute Cluster) ausgeführt werden. Die GRID- und Gaming-Treiber sind für die Ausführung im WDDM-Modus (Windows Display Driver Model) konfiguriert. Im TCC-Modus ist die Karte für Datenverarbeitungs-Workloads bestimmt. Im WDDM-Modus unterstützt die Karte sowohl Datenverarbeitungs- als auch Grafik-Workloads.

NVIDIA-Steuerfeld

Das NVIDIA-Steuerfeld wird mit GRID und Gaming-Treibern unterstützt. Es wird nicht mit Tesla-Treibern unterstützt.

Wird für Tesla-, GRID- und Gaming-Treiber unterstützt APIs

- OpenCL, OpenGL und Vulkan
- NVIDIA CUDA und verwandte Bibliotheken (z. B. cuDNN, TensorRT, nvJPEG und cuBLAS)

- NVENC für Videocodierung und NVDEC für Videodecodierung
- Nur für Windows APIs: DirectX, Direct2D, DirectX-Videobeschleunigung, DirectX Raytracing

Verfügbare Treiber nach Instance-Typ

In der folgenden Tabelle werden die unterstützten NVIDIA-Treiber für jeden GPU-Instance-Typ zusammengefasst.

Instance-Typ	Tesla-Treiber	GRID-Treiber	Gaming-Treiber
G3	Ja	Ja	Nein
G4dn	Ja	Ja	Ja
G5	Ja	Ja	Ja
G5g	Ja[1]	Nein	Nein
G6	Ja	Ja	Ja
G6e	Ja	Ja	Ja
G6f	Nein	Ja	Nein
Gr6	Ja	Ja	Nein
Gr6f	Nein	Ja	Nein
P2	Ja	Nein	Nein
P3	Ja	Nein	Nein
P4d	Ja	Nein	Nein
P4de	Ja	Nein	Nein
P5	Ja	Nein	Nein
P5e	Ja	Nein	Nein
P5en	Ja	Nein	Nein

Instance-Typ	Tesla-Treiber	GRID-Treiber	Gaming-Treiber
P6-B200	Ja	Nein	Nein
GB2P6e-00	Ja	Nein	Nein
P6-B-300	Ja	Nein	Nein

[1] Dieser Tesla-Treiber unterstützt auch plattformspezifische, optimierte Grafikanwendungen ARM64

Installationsoptionen

Verwenden Sie eine der folgenden Optionen, um die für Ihre GPU-Instance erforderlichen NVIDIA-Treiber abzurufen.

Optionen

1. Verwenden Sie AMIs diese, einschließlich NVIDIA-Treiber
2. Öffentliche NVIDIA-Treiber installieren
3. NVIDIA-GRID-Treiber (G6-, Gr6-, G6e-, G6f-, Gr6f-, G5-, G4dn- und G3-Instances) installieren
4. NVIDIA-Gaming-Treiber (G6-, G6e-, G5- und G4dn-Instances)

Verwenden Sie AMIs diese, einschließlich NVIDIA-Treiber

AWS und NVIDIA bieten verschiedene Amazon Machine Images (AMIs) an, auf denen die NVIDIA-Treiber installiert sind.

- Marketplace-Angebote mit dem öffentlichen Tesla-Treiber
- Marketplace-Angebote mit dem GRID-Treiber
- Marketplace-Angebote mit dem Gaming-Treiber

Um die Überlegungen zu überprüfen, die von Ihrer Betriebssystem-Plattform (OS) abhängen, wählen Sie die Registerkarte, die für Ihr AMI gilt.

Linux

Um die mit einer dieser Optionen installierte Treiberversion zu aktualisieren AMIs, müssen Sie die NVIDIA-Pakete von Ihrer Instance deinstallieren, um Versionskonflikte zu vermeiden. Verwenden Sie den folgenden Befehl, um die NVIDIA-Pakete zu deinstallieren:

```
[ec2-user ~]$ sudo yum erase nvidia cuda
```

Das CUDA-Toolkit-Paket weist Abhängigkeiten zu den NVIDIA-Treibern auf. Durch die Deinstallation der NVIDIA-Pakete wird das CUDA-Toolkit gelöscht. Sie müssen das CUDA-Toolkit nach der Installation des NVIDIA-Treibers erneut installieren.

Windows

Wenn Sie ein benutzerdefiniertes Windows AMI mit einem der AWS Marketplace -Angebote erstellen, muss es sich bei AMI um ein mit Sysprep erstelltes standardisiertes Image handeln, um sicherzustellen, dass der GRID-Treiber funktioniert. Weitere Informationen finden Sie unter Ein Amazon-EC2-AMI mit Windows Sysprep erstellen.

Öffentliche NVIDIA-Treiber installieren

Wenn die AWS Marketplace AMIs unter beschriebenen Treiber Verwenden Sie AMIs diese, einschließlich NVIDIA-Treiber nicht zu Ihrem Anwendungsfall passen, können Sie die öffentlichen Treiber installieren und Ihre eigene Lizenz mitbringen. Es gibt die folgenden Installationsoptionen:

- Option 1: Installation nur über den Treiber
- Option 2: Installation mit dem CUDA-Toolkit (empfohlen für Linux-Distributionen)

Überlegungen zu den Instanztypen P6-B200 und P6-B300

Die Plattformen P6-B200 und P6-B300 sind insofern einzigartig, als sie der Instanz Mellanox ConnectX-Netzwerkschnittstellenkarten () als Geräte zur Verfügung stellen. NICs PCIe Diese fungieren NICs nicht als typische Netzwerkschnittstellen, sondern als NVSwitch Brücken, die einen Steuerpfad für die Initialisierung und Konfiguration der Topologie der NVFabric GPU-Verbindung bereitstellen. NVLink

Um das System vollständig zu initialisieren, muss der NVIDIA Fabric Manager die Topologie konfigurieren `NVFabric` und einrichten. NVSwitch Dadurch können InfiniBand Kernelmodule mit dem Mellanox ConnectX kommunizieren. NICs

NVIDIA Fabric Manager ist im CUDA-Toolkit enthalten. Wir empfehlen Option 2: Installation mit dem CUDA-Toolkit für diesen Instance-Typ.

Option 1: Installation nur über den Treiber

Um einen bestimmten Treiber zu installieren, melden Sie sich bei Ihrer Instance an und laden Sie den öffentlichen 64-Bit-NVIDIA-Treiber für den Instance-Typ von http://www.nvidia herunter. com/Download/Find.aspx. Verwenden Sie für Produkttyp Produktserie und Produkt die Optionen in der folgenden Tabelle.

Folgen Sie anschließend den Anweisungen zur Installation des lokalen Repositorys im NVIDIA-Treiberinstallationshandbuch.

> **Note**
>
> Die Instance-Typen P6-B200 und P6-B300 erfordern die Installation und Konfiguration zusätzlicher Pakete, die im NVIDIA CUDA Toolkit enthalten sind. Weitere Informationen finden Sie in den Anweisungen für Ihre Linux-Distribution in Option 2: Installation mit dem CUDA-Toolkit.

Instance	Produkttyp	Produktserie	Produkt	Minimale Treiberversion
G3	Tesla	M-Klasse	M60	--
G4dn	Tesla	T-Series	T4	--
G5	Tesla	A-Serie	A10	470.00 oder höher
G5g[1]	Tesla	T-Series	NVIDIA T4G	470.82.01 oder höher
G6	Tesla	L-Serie	L4	525.0 oder höher

Instance	Produkttyp	Produktserie	Produkt	Minimale Treiberversion
G6e	Tesla	L-Serie	L40S	535.0 oder höher
Gr6	Tesla	L-Serie	L4	525.0 oder höher
P2	Tesla	K-Serie	K80	--
P3	Tesla	V-Serie	V100	--
P4d	Tesla	A-Serie	A100	--
P4de	Tesla	A-Serie	A100	--
P5	Tesla	H-Serie	H100	530 oder höher
P5e	Tesla	H-Serie	H200	550 oder höher
P5en	Tesla	H-Serie	H200	550 oder höher
P6-B200[2]	Tesla	HGX-Serie	B200	570 oder höher
P6e-00 GB2	Tesla	HGX-Serie	B200	570 oder später
P6-B300 2	Tesla	HGX-Serie	B300	580 oder später

[1] Das Betriebssystem für G5g-Instances ist Linux aarch64.

[2] Für die Instanztypen P6-B200 und P6-B300 gelten zusätzliche Installationsanforderungen für die Konfiguration von NVIDIA Fabric Manager.

Option 2: Installation mit dem CUDA-Toolkit

Die Installationsanweisungen variieren je nach Betriebssystem geringfügig. Folgen Sie den Anweisungen für das Betriebssystem Ihrer Instance, um öffentliche Treiber mit dem NVIDIA-CUDA-Toolkit auf Ihrer Instance zu installieren. Folgen Sie für Instance-Betriebssysteme, die hier nicht aufgeführt sind, den Anweisungen für Ihr Betriebssystem und Ihre Instance-Typ-Architektur auf der NVIDIA-Developer-Website. Weitere Informationen finden Sie unter CUDA-Toolkit-Downloads.

Informationen zur Instance-Typ-Architektur oder anderen Spezifikationen finden Sie in den Spezifikationen für beschleunigte Datenverarbeitung in der EC2 Amazon-Instanztypen-Referenz.

Amazon Linux 2023

Dieser Abschnitt behandelt die Installation eines NVIDIA-CUDA-Toolkits auf einer Amazon-Linux-2023-Instance. Die Befehlsbeispiele in diesem Abschnitt basieren auf einer `x86_64`-Architektur.

`arm64-sbsa`-Befehle finden Sie unter CUDA-Toolkit-Downloads. Wählen Sie die Optionen aus, die für Ihre Distribution gelten. Anweisungen werden angezeigt, nachdem Sie Ihre endgültige Auswahl getroffen haben.

Voraussetzung

Führen Sie vor der Installation des Toolkits und der Treiber den folgenden Befehl aus, um sicherzustellen, dass Sie über die richtige Version der Kernel-Header und Entwicklungspakete verfügen.

```
[ec2-user ~]$ sudo dnf install kernel-devel-$(uname -r) kernel-headers-$(uname -r) -y
```

Toolkit und Treiber herunterladen

Wählen Sie den Installationstyp aus, den Sie für Ihre Instance verwenden möchten, und folgen Sie den entsprechenden Schritten.

RPM local installation

Sie können diesen Anweisungen folgen, um das Repository-Paket für drn CUDA Toolkit Installer auf Ihre Instance herunterzuladen und anschließend das angegebene Paket zu extrahieren und zu registrieren.

Anweisungen finden Sie auf der NVIDIA-Entwickler-Website unter CUDA-Toolkit-Downloads.

```
[ec2-user ~]$ wget https://developer.download.nvidia.com/compute/cuda/13.0.0/
local_installers/cuda-repo-amzn2023-13-0-local-13.0.0_580.65.06-1.x86_64.rpm
[ec2-user ~]$ sudo rpm -i cuda-repo-amzn2023-13-0-
local-13.0.0_580.65.06-1.x86_64.rpm
```

RPM network installation

Sie können diesen Anweisungen folgen, um das CUDA-Repository beim Paketmanager auf Ihrer Instance zu registrieren. Wenn Sie die Installationsschritte ausführen, lädt der Paketmanager nur die benötigten Pakete herunter.

Anweisungen finden Sie auf der NVIDIA-Entwickler-Website unter CUDA-Toolkit-Downloads.

```
[ec2-user ~]$ wget https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2404/x86_64/cuda-keyring_1.1-1_all.deb
[ec2-user ~]$ sudo dpkg -i cuda-keyring_1.1-1_all.deb
```

Die verbleibenden Schritte sind für die lokale Installation und die Netzwerkinstallation identisch.

1. Die Installation des CUDA-Toolkits abschließen

```
[ec2-user ~]$ sudo dnf clean all
[ec2-user ~]$ sudo dnf install cuda-toolkit -y
```

2. Die offene Kernel-Modulvariante des Treibers installieren

```
[ec2-user ~]$ sudo dnf module install nvidia-driver:open-dkms -y
```

3. Installieren Sie GPUDirect Storage und Fabric Manager

```
[ec2-user ~]$ sudo dnf install nvidia-gds -y
[ec2-user ~]$ sudo dnf install nvidia-fabric-manager -y
```

4. Fabric Manager und Treiberpersistenz aktivieren

```
[ec2-user ~]$ sudo systemctl enable nvidia-fabricmanager
[ec2-user ~]$ sudo systemctl enable nvidia-persistenced
```

5. (Nur P6-B200 und P6-B300) Diese Instance-Typen erfordern die Installation und Konfiguration zusätzlicher Pakete, die im Lieferumfang des NVIDIA CUDA Toolkit enthalten sind.

   1. Installieren Sie den NVIDIA Link Subnet Manager und `ibstat`.

      ```
      [ec2-user ~]$ sudo dnf install nvlink5
      ```

   2. Aktivieren Sie das automatische Laden des Infiniband-Moduls beim Start.

```
[ec2-user ~]$ echo "ib_umad" | sudo tee -a /etc/modules-load.d/modules.conf
```

6. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

Ubuntu 24.04

Dieser Abschnitt behandelt die Installation eines NVIDIA-CUDA-Toolkits auf einer Ubuntu-24.04-Instance. Die Befehlsbeispiele in diesem Abschnitt basieren auf einer x86_64-Architektur.

`arm64-sbsa`-Befehle finden Sie unter CUDA-Toolkit-Downloads. Wählen Sie die Optionen aus, die für Ihre Distribution gelten. Anweisungen werden angezeigt, nachdem Sie Ihre endgültige Auswahl getroffen haben.

Voraussetzung

Führen Sie vor der Installation des Toolkits und der Treiber den folgenden Befehl aus, um sicherzustellen, dass Sie über die richtige Version der Kernel-Header und Entwicklungspakete verfügen.

```
$ apt install linux-headers-$(uname -r)
```

Toolkit und Treiber herunterladen

Wählen Sie den Installationstyp aus, den Sie für Ihre Instance verwenden möchten, und folgen Sie den entsprechenden Schritten.

RPM local installation

Sie können diesen Anweisungen folgen, um das Repository-Paket für drn CUDA Toolkit Installer auf Ihre Instance herunterzuladen und anschließend das angegebene Paket zu extrahieren und zu registrieren.

Anweisungen finden Sie auf der NVIDIA-Entwickler-Website unter CUDA-Toolkit-Downloads.

```
$ wget https://developer.download.nvidia.com/compute/cuda/repos/ubuntu2404/
x86_64/cuda-ubuntu2404.pin
$ sudo mv cuda-ubuntu2404.pin /etc/apt/preferences.d/cuda-repository-pin-600
```

```
$ wget https://developer.download.nvidia.com/compute/cuda/13.0.0/
local_installers/cuda-repo-ubuntu2404-13-0-local_13.0.0-580.65.06-1_amd64.deb
$ sudo dpkg -i cuda-repo-ubuntu2404-13-0-local_13.0.0-580.65.06-1_amd64.deb
$ sudo cp /var/cuda-repo-ubuntu2404-13-0-local/cuda-*-keyring.gpg /usr/share/
keyrings/
```

RPM network installation

Sie können diesen Anweisungen folgen, um das CUDA-Repository beim Paketmanager auf Ihrer Instance zu registrieren. Wenn Sie die Installationsschritte ausführen, lädt der Paketmanager nur die benötigten Pakete herunter.

Anweisungen finden Sie auf der NVIDIA-Entwickler-Website unter CUDA-Toolkit-Downloads.

```
$ wget https://developer.download.nvidia.com/compute/cuda/repos/ubuntu2404/x86_64/
cuda-keyring_1.1-1_all.deb
$ sudo dpkg -i cuda-keyring_1.1-1_all.deb
```

Die verbleibenden Schritte sind für die lokale Installation und die Netzwerkinstallation identisch.

1. Die Installation des CUDA-Toolkits abschließen

```
$ sudo apt update
$ sudo apt install cuda-toolkit -y
```

2. Die offene Kernel-Modulvariante des Treibers installieren

```
$ sudo apt install nvidia-open -y
```

3. Installieren Sie GPUDirect Storage und Fabric Manager

```
$ sudo apt install nvidia-gds -y
$ sudo apt install nvidia-fabricmanager -y
```

4. Fabric Manager und Treiberpersistenz aktivieren

```
$ sudo systemctl enable nvidia-fabricmanager
$ sudo systemctl enable nvidia-persistenced
```

5. (Nur P6-B200 und P6-B300) Diese Instance-Typen erfordern die Installation und Konfiguration zusätzlicher Pakete, die im Lieferumfang des NVIDIA CUDA Toolkit enthalten sind.

1. Installieren Sie die neuesten spezifischen Gerätetreiber- und Diagnoseprogramme. InfiniBand

```
$ sudo apt install linux-modules-extra-$(uname -r) -y
$ sudo apt install infiniband-diags -y
```

2. Installieren Sie den NVIDIA Link Subnet Manager.

```
$ sudo apt install nvlsm -y
```

6. Starten Sie die Instance neu.

```
sudo reboot
```

7. Aktualisieren Sie Ihren Pfad und fügen Sie die folgende Umgebungsvariable hinzu.

```
$ export PATH=${PATH}:/usr/local/cuda-13.0/bin
$ export LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/usr/local/cuda-13.0/lib64
```

Windows-Betriebssysteme

Zur Installation des NVIDIA-Treibers unter Windows führen Sie die folgenden Schritte aus:

1. Öffnen Sie das Verzeichnis, in das Sie den Treiber heruntergeladen haben, und starten Sie die Installationsdatei. Befolgen Sie die Anweisungen, um den Treiber zu installieren, und starten Sie die Instance neu, wenn Sie dazu aufgefordert werden.
2. Deaktivieren Sie im Geräte-Manager den Displayadapter mit dem Namen Microsoft Basic Display Adapter, der mit einem Warnsymbol gekennzeichnet ist. Installieren Sie die folgenden Windows-Features: Media Foundation und Quality Windows Audio Video Experience.

> **Important**
>
> Deaktivieren Sie nicht den Displayadapter mit dem Namen Microsoft Remote Display Adapter. Wenn der Microsoft Remote Display Adapter deaktiviert ist, wird Ihre Verbindung möglicherweise unterbrochen und Versuche, nach dem Neustart eine Verbindung zur Instance herzustellen, schlagen möglicherweise fehl.

3. Prüfen Sie im Geräte-Manager, ob die GPU korrekt funktioniert.

4. Führen Sie die Optimierungsschritte unter Optimieren Sie die GPU-Einstellungen auf EC2 Amazon-Instances aus, um die beste Leistung für Ihre GPU zu erzielen.

NVIDIA-GRID-Treiber (G6-, Gr6-, G6e-, G6f-, Gr6f-, G5-, G4dn- und G3-Instances) installieren

Diese Downloads stehen nur AWS Kunden zur Verfügung. Durch das Herunterladen erklären Sie sich damit einverstanden, die heruntergeladene Software nur zur Entwicklung AMIs für die NVIDIA L4-, NVIDIA L40S-, NVIDIA A10G-, NVIDIA Tesla T4- oder NVIDIA Tesla M60-Hardware zu verwenden, um die Anforderungen der AWS Lösung zu erfüllen, auf die in der NVIDIA GRID Cloud Endbenutzer-Lizenzvereinbarung (EULA) verwiesen wird. Sie können die GRID-Treiber sowohl für die Erstellung als auch für die Verwendung in der Umgebung verwenden. AMIs AWS Durch die Installation der Software stimmen Sie den Bedingungen in der Endbenutzer-Lizenzvereinbarung für NVIDIA GRID Cloud zu. Informationen zur Version des NVIDIA-GRID-Treibers für Ihr Betriebssystem finden Sie unter NVIDIA Virtual GPU (vGPU) Software auf der NVIDIA-Website.

Überlegungen

- G6f- und Gr6f-Instances benötigen GRID 18.4 oder höher.
- G6e-Instances benötigen GRID 17.4 oder höher.
- G6- und Gr6-Instances benötigen GRID 17.1 oder höher.
- G5-Instances erfordern GRID 13.1 oder höher (oder GRID 12.4 oder höher).
- G3-Instances benötigen die AWS bereitgestellte DNS-Auflösung, damit die GRID-Lizenzierung funktioniert.
- IMDSv2wird nur mit der NVIDIA-Treiberversion 14.0 oder höher unterstützt.
- Wenn Sie Ihre Windows-Instances von einem benutzerdefinierten Windows AMI starten, muss das AMI ein standardisiertes Image sein, das mit Windows Sysprep erstellt wurde, um sicherzustellen, dass der GRID-Treiber funktioniert. Weitere Informationen finden Sie unter Ein Amazon-EC2-AMI mit Windows Sysprep erstellen.
- GRID 17.0 und höher unterstützen Windows Server 2019 nicht.
- GRID 14.2 und höher unterstützen Windows Server 2016 nicht.
- GRID 17.0 und höher wird mit G3-Instances nicht unterstützt.
- Für Linux-Instances müssen Sie möglicherweise Pakete wie gcc installieren oder aktualisieren, wenn das NVIDIA-Installationsprogramm mit einer Fehlermeldung fehlschlägt. Die Einzelheiten

hängen von den Versionen des Betriebssystems und des Kernels ab. Weitere Informationen finden Sie im NVIDIA Enterprise Support Portal.

Voraussetzungen

- (Linux) Stellen Sie sicher, dass der auf Ihrer Instanz installiert und mit Standardanmeldedaten konfiguriert AWS CLI ist. Weitere Informationen finden Sie unter Installieren der AWS CLI im AWS Command Line Interface -Benutzerhandbuch.
- (Windows) Konfigurieren Sie Standardanmeldedaten für die AWS Tools for Windows PowerShell auf Ihrer Instance. Weitere Informationen finden Sie unter Erste Schritte mit dem AWS Tools for Windows PowerShell im AWS -Tools für PowerShell -Benutzerhandbuch.
- Ihrem Benutzer oder Ihrer Rolle müssen die Berechtigungen erteilt worden sein, die die ReadOnlyAccessAmazonS3-Richtlinie enthalten.

Amazon Linux 2023

So installieren Sie den NVIDIA-GRID-Treiber auf Ihrer Instance:

1. Verbinden Sie sich mit der Instance. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
[ec2-user ~]$ sudo dnf update -y
```

2. Installieren Sie gcc und make, falls sie noch nicht installiert sind.

```
[ec2-user ~]$ sudo dnf install gcc make
```

3. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
[ec2-user ~]$ sudo reboot
```

4. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
5. Installieren Sie die Kernel-Header-Pakete.

```
[ec2-user ~]$ sudo dnf install -y kernel-devel kernel-modules-extra
```

6. Laden Sie das GRID-Treiberinstallationsprogramm anhand des folgenden Befehls herunter:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Mehrere Versionen des GRID-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiberinstallationsprogramms hinzu.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Führen Sie das Selbstinstallationsskript wie folgt aus, um den heruntergeladenen GRID-Treiber zu installieren. Beispiel:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

9. Vergewissern Sie sich, dass der Treiber funktioniert. In der Antwort für den folgenden Befehl sind die installierte Version des NVIDIA-Treibers sowie Einzelheiten zum aufgeführt. GPUs

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Wenn Sie die NVIDIA-vGPU-Software Version 14.x oder höher auf den G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie in der NVIDIA-Dokumentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

12. (Optional) Je nach Anwendungsfall können Sie die folgenden optionalen Schritte ausführen. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diese Schritte nicht aus.

    a. Um die Vorteile der vier Displays mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll Amazon DCV ein.

    b. Der NVIDIA Quadro Virtual Workstation-Modus ist standardmäßig aktiviert. Um die Hosting-Funktionen von GRID Virtual Applications for RDSH Application zu aktivieren, führen Sie die Aktivierungsschritte für GRID Virtual Application in Aktivieren Sie virtuelle NVIDIA GRID-Anwendungen auf Ihren Amazon EC2 GPU-basierten Instances aus.

Amazon Linux 2

So installieren Sie den NVIDIA-GRID-Treiber auf Ihrer Instance:

1. Verbinden Sie sich mit der Instance. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
[ec2-user ~]$ sudo yum update -y
```

2. Installieren Sie gcc und make, falls sie noch nicht installiert sind.

```
[ec2-user ~]$ sudo yum install gcc make
```

3. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
[ec2-user ~]$ sudo reboot
```

4. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
5. Installieren Sie das Kernel-Header-Paket für die Version des Kernels, die ausgeführt wird.

```
[ec2-user ~]$ sudo yum install -y kernel-devel-$(uname -r)
```

6. Laden Sie das GRID-Treiberinstallationsprogramm anhand des folgenden Befehls herunter:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   Mehrere Versionen des GRID-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiberinstallationsprogramms hinzu.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Führen Sie das Selbstinstallationsskript wie folgt aus, um den heruntergeladenen GRID-Treiber zu installieren. Zum Beispiel:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

   Wenn Sie Amazon Linux 2 mit Kernelversion 5.10 verwenden, installieren Sie den GRID-Treiber mithilfe des folgenden Befehls.

```
[ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
```

   Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

9. Vergewissern Sie sich, dass der Treiber funktioniert. In der Antwort für den folgenden Befehl werden die installierte Version des NVIDIA-Treibers sowie Einzelheiten zum aufgeführt GPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Wenn Sie die NVIDIA-vGPU-Software Version 14.x oder höher auf den G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie in der NVIDIA-Dokumentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

12. (Optional) Je nach Anwendungsfall können Sie die folgenden optionalen Schritte ausführen. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diese Schritte nicht aus.

    a. Um die Vorteile der vier Displays mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll Amazon DCV ein.

    b. Der NVIDIA Quadro Virtual Workstation-Modus ist standardmäßig aktiviert. Um die Hosting-Funktionen von GRID Virtual Applications for RDSH Application zu aktivieren, führen Sie die Aktivierungsschritte für GRID Virtual Application in Aktivieren Sie virtuelle NVIDIA GRID-Anwendungen auf Ihren Amazon EC2 GPU-basierten Instances aus.

CentOS 7 und Red Hat Enterprise Linux 7

So installieren Sie den NVIDIA-GRID-Treiber auf Ihrer Instance:

1. Verbinden Sie sich mit der Instance. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
[ec2-user ~]$ sudo yum update -y
```

2. Installieren Sie gcc und make, falls sie noch nicht installiert sind.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

3. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
[ec2-user ~]$ sudo reboot
```

4. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
5. Installieren Sie das Kernel-Header-Paket für die Version des Kernels, die Sie ausführen.

```
[ec2-user ~]$ sudo yum install -y kernel-devel-$(uname -r)
```

6. Deaktivieren Sie den Open-Source-Treiber `nouveau` für NVIDIA-Grafikkarten.

    a. Fügen Sie der Negativliste in der Datei `nouveau` den Eintrag `/etc/modprobe.d/blacklist.conf` hinzu. Kopieren Sie den folgenden Codeblock und fügen Sie ihn in ein Terminalfenster ein.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
```

```
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

b. Bearbeiten Sie die Datei `/etc/default/grub` und fügen Sie folgende Zeile hinzu.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

c. Erstellen Sie die neue Grub-Konfiguration.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Laden Sie das GRID-Treiberinstallationsprogramm anhand des folgenden Befehls herunter:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Mehrere Versionen des GRID-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

8. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiberinstallationsprogramms hinzu.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

9. Führen Sie das Selbstinstallationsskript wie folgt aus, um den heruntergeladenen GRID-Treiber zu installieren. Beispiel:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

10. Vergewissern Sie sich, dass der Treiber funktioniert. In der Antwort für den folgenden Befehl werden die installierte Version des NVIDIA-Treibers sowie Einzelheiten zum aufgeführt GPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

11. Wenn Sie die NVIDIA-vGPU-Software Version 14.x oder höher auf den G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie in der NVIDIA-Dokumentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

12. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

13. (Optional) Je nach Anwendungsfall können Sie die folgenden optionalen Schritte ausführen. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diese Schritte nicht aus.

    a. Um die Vorteile der vier Displays mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll Amazon DCV ein.

    b. Der NVIDIA Quadro Virtual Workstation-Modus ist standardmäßig aktiviert. Um die Hosting-Funktionen von GRID Virtual Applications for RDSH Application zu aktivieren, führen Sie die Aktivierungsschritte für GRID Virtual Application in Aktivieren Sie virtuelle NVIDIA GRID-Anwendungen auf Ihren Amazon EC2 GPU-basierten Instances aus.

    c. Installieren Sie das desktop/workstation GUI-Paket.

    ```
    [ec2-user ~]$ sudo yum groupinstall -y "Server with GUI"
    ```

CentOS Stream 8 und Red Hat Enterprise Linux 8

So installieren Sie den NVIDIA-GRID-Treiber auf Ihrer Instance:

1. Verbinden Sie sich mit der Instance. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
[ec2-user ~]$ sudo yum update -y
```

2. Installieren Sie gcc und make, falls sie noch nicht installiert sind.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

3. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
[ec2-user ~]$ sudo reboot
```

4. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
5. Installieren Sie das Kernel-Header-Paket für die Version des Kernels, die Sie ausführen.

```
[ec2-user ~]$ sudo dnf install -y elfutils-libelf-devel libglvnd-devel kernel-
devel-$(uname -r)
```

6. Laden Sie das GRID-Treiberinstallationsprogramm anhand des folgenden Befehls herunter:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   Mehrere Versionen des GRID-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiberinstallationsprogramms hinzu.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Führen Sie das Selbstinstallationsskript wie folgt aus, um den heruntergeladenen GRID-Treiber zu installieren. Beispiel:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

   Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

9. Vergewissern Sie sich, dass der Treiber funktioniert. Die Antwort für den folgenden Befehl listet die installierte Version des NVIDIA-Treibers und Details zu GPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Wenn Sie die NVIDIA-vGPU-Software Version 14.x oder höher auf den G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie in der NVIDIA-Dokumentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

12. (Optional) Je nach Anwendungsfall können Sie die folgenden optionalen Schritte ausführen. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diese Schritte nicht aus.

    a. Um die Vorteile der vier Displays mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll Amazon DCV ein.

    b. Der NVIDIA Quadro Virtual Workstation-Modus ist standardmäßig aktiviert. Um die Hosting-Funktionen von GRID Virtual Applications for RDSH Application zu aktivieren, führen Sie die Aktivierungsschritte für GRID Virtual Application in Aktivieren Sie virtuelle NVIDIA GRID-Anwendungen auf Ihren Amazon EC2 GPU-basierten Instances aus.

    c. Installieren Sie das GUI-Workstation-Paket.

    ```
    [ec2-user ~]$ sudo dnf groupinstall -y workstation
    ```

Rocky Linux 8

So installieren Sie den NVIDIA GRID-Treiber auf einer Linux-Instance

1. Verbinden Sie sich mit der Instance. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
[ec2-user ~]$ sudo yum update -y
```

2. Installieren Sie gcc und make, falls sie noch nicht installiert sind.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

3. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
[ec2-user ~]$ sudo reboot
```

4. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
5. Installieren Sie das Kernel-Header-Paket für die Version des Kernels, die Sie ausführen.

```
[ec2-user ~]$ sudo dnf install -y elfutils-libelf-devel libglvnd-devel kernel-
devel-$(uname -r)
```

6. Laden Sie das GRID-Treiberinstallationsprogramm anhand des folgenden Befehls herunter:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   Mehrere Versionen des GRID-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiberinstallationsprogramms hinzu.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Führen Sie das Selbstinstallationsskript wie folgt aus, um den heruntergeladenen GRID-Treiber zu installieren. Beispiel:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

   Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

9. Vergewissern Sie sich, dass der Treiber funktioniert. In der Antwort für den folgenden Befehl werden die installierte Version des NVIDIA-Treibers sowie Einzelheiten zum aufgeführt GPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Wenn Sie die NVIDIA-vGPU-Software Version 14.x oder höher auf den G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie in der NVIDIA-Dokumentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

12. (Optional) Je nach Anwendungsfall können Sie die folgenden optionalen Schritte ausführen. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diese Schritte nicht aus.

    a. Um die Vorteile der vier Displays mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll Amazon DCV ein.

    b. Der NVIDIA Quadro Virtual Workstation-Modus ist standardmäßig aktiviert. Um die Hosting-Funktionen von GRID Virtual Applications for RDSH Application zu aktivieren, führen Sie die Aktivierungsschritte für GRID Virtual Application in Aktivieren Sie virtuelle NVIDIA GRID-Anwendungen auf Ihren Amazon EC2 GPU-basierten Instances aus.

Ubuntu und Debian

So installieren Sie den NVIDIA-GRID-Treiber auf Ihrer Instance:

1. Verbinden Sie sich mit der Instance. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
$ sudo apt-get update -y
```

2. Installieren Sie gcc und make, falls sie noch nicht installiert sind.

```
$ sudo apt-get install -y gcc make
```

3. (Ubuntu) Führen Sie ein Upgrade des `linux-aws`-Pakets durch, um die aktuelle Version zu erhalten.

```
$ sudo apt-get upgrade -y linux-aws
```

(Debian) Führen Sie ein Upgrade des Pakets durch, um die aktuelle Version zu erhalten.

```
$ sudo apt-get upgrade -y
```

4. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
$ sudo reboot
```

5. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
6. Installieren Sie das Kernel-Header-Paket für die Version des Kernels, die Sie gerade verwenden.

```
$ sudo apt-get install -y linux-headers-$(uname -r) linux-modules-extra-$(uname -r)
```

7. Deaktivieren Sie den Open-Source-Treiber `nouveau` für NVIDIA-Grafikkarten.

   a. Fügen Sie der Negativliste in der Datei `nouveau` den Eintrag `/etc/modprobe.d/blacklist.conf` hinzu. Kopieren Sie den folgenden Codeblock und fügen Sie ihn in ein Terminalfenster ein.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Bearbeiten Sie die Datei `/etc/default/grub` und fügen Sie folgende Zeile hinzu.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Erstellen Sie die neue Grub-Konfiguration.

```
$ sudo update-grub
```

8. Laden Sie das GRID-Treiberinstallationsprogramm anhand des folgenden Befehls herunter:

```
$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Mehrere Versionen des GRID-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen.

```
$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

9. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiberinstallationsprogramms hinzu.

```
$ chmod +x NVIDIA-Linux-x86_64*.run
```

10. Führen Sie das Selbstinstallationsskript wie folgt aus, um den heruntergeladenen GRID-Treiber zu installieren. Beispiel:

```
$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

11. Vergewissern Sie sich, dass der Treiber funktioniert. In der Antwort für den folgenden Befehl werden die installierte Version des NVIDIA-Treibers sowie Einzelheiten zum aufgeführt GPUs.

```
$ nvidia-smi -q | head
```

12. Wenn Sie die NVIDIA-vGPU-Software Version 14.x oder höher auf den G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie in der NVIDIA-Dokumentation.

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
modprobe.d/nvidia.conf
```

13. Starten Sie die Instance neu.

```
$ sudo reboot
```

14. (Optional) Je nach Anwendungsfall können Sie die folgenden optionalen Schritte ausführen. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diese Schritte nicht aus.

    a. Um die Vorteile der vier Displays mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll Amazon DCV ein.

    b. Der NVIDIA Quadro Virtual Workstation-Modus ist standardmäßig aktiviert. Um die Hosting-Funktionen von GRID Virtual Applications for RDSH Application zu aktivieren, führen Sie die Aktivierungsschritte für GRID Virtual Application in Aktivieren Sie virtuelle NVIDIA GRID-Anwendungen auf Ihren Amazon EC2 GPU-basierten Instances aus.

    c. Installieren Sie das desktop/workstation GUI-Paket.

```
$ sudo apt-get install -y lightdm ubuntu-desktop
```

Windows-Betriebssysteme

So installieren Sie den NVIDIA GRID-Treiber auf einer Windows-Instance

1. Connect zu Ihrer Windows-Instanz her und öffnen Sie ein PowerShell Fenster.
2. Laden Sie die Treiber und die NVIDIA GRID Cloud-Endbenutzer-Lizenzvereinbarung mit den folgenden PowerShell Befehlen von Amazon S3 auf Ihren Desktop herunter.

```
$Bucket = "ec2-windows-nvidia-drivers"
$KeyPrefix = "latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
$LocalFilePath = Join-Path $LocalPath $LocalFileName
Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

   Mehrere Versionen des NVIDIA GRID-Treibers werden in diesem Bucket gespeichert. Sie können alle verfügbaren Windows-Versionen im Bucket herunterladen, indem Sie die `-KeyPrefix $KeyPrefix`-Option entfernen. Informationen zur Version des NVIDIA-GRID-

Treibers für Ihr Betriebssystem finden Sie unter NVIDIA Virtual GPU (vGPU) Software auf der NVIDIA-Website.

Ab GRID-Version 11.0 können Sie die Treiber unter `latest` für G3- und für G4dn-Instances verwenden. Wir werden keine Versionen nach 11.0 zu `g4/latest` hinzufügen, aber die Version 11.0 und die früheren für G4dn spezifischen Versionen unter `g4/latest` beibehalten.

G5-Instances erfordern GRID 13.1 oder höher (oder GRID 12.4 oder höher).

3. Navigieren Sie zu Ihrem Desktop und doppelklicken Sie auf die Installationsdatei, um sie auszuführen (wählen Sie die Treiberversion für das Betriebssystem Ihrer Instance aus). Befolgen Sie die Anweisungen, um den Treiber zu installieren, und starten Sie die Instance neu, wenn Sie dazu aufgefordert werden. Sie können prüfen, ob die GPU richtig funktioniert, indem Sie den Geräte-Manager verwenden.
4. (Optional) Verwenden Sie den folgenden Befehl, um die Lizenzierungsseite in der Systemsteuerung zu deaktivieren und damit zu verhindern, dass Benutzer versehentlich den Produkttyp ändern (NVIDIA GRID Virtual Workstation ist standardmäßig aktiviert). Weitere Informationen finden Sie im GRID-Lizenzierungs-Benutzerhandbuch.

   PowerShell

   Führen Sie die folgenden PowerShell Befehle aus, um den Registrierungswert für die Deaktivierung der Lizenzierungsseite im Kontrollpanel zu erstellen. AWS -Tools für PowerShell In AWS Windows wird AMIs standardmäßig die 32-Bit-Version verwendet, und dieser Befehl schlägt fehl. Verwenden Sie stattdessen die 64-Bit-Version von, die im Betriebssystem PowerShell enthalten ist.

   ```
   New-Item -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name GridLicensing
   New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" -
   Name "NvCplDisableManageLicensePage" -PropertyType "DWord" -Value "1"
   ```

   Eingabeaufforderung

   Führen Sie den folgenden Registry-Befehl aus, um den Registrierungswert zum Deaktivieren der Lizenzierungsseite in der Systemsteuerung zu erstellen. Sie können es über das Befehlszeilenfenster oder eine 64-Bit-Version von ausführenPowerShell.

   ```
   reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" /v
    NvCplDisableManageLicensePage /t REG_DWORD /d 1
   ```

5. (Optional) Je nach Anwendungsfall können Sie die folgenden optionalen Schritte ausführen. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diese Schritte nicht aus.

   a. Um die Vorteile der vier Displays mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll Amazon DCV ein.

   b. Der NVIDIA Quadro Virtual Workstation-Modus ist standardmäßig aktiviert. Um die Hosting-Funktionen von GRID Virtual Applications for RDSH Application zu aktivieren, führen Sie die Aktivierungsschritte für GRID Virtual Application in Aktivieren Sie virtuelle NVIDIA GRID-Anwendungen auf Ihren Amazon EC2 GPU-basierten Instances aus.

NVIDIA-Gaming-Treiber (G6-, G6e-, G5- und G4dn-Instances)

Diese Treiber sind nur für AWS-Kunden verfügbar. Wenn Sie die Treiber herunterladen, stimmen Sie zu, diese nur für die Entwicklung von AMIs für den Einsatz auf NVIDIA-L4-, NVIDIA-L40S-, NVIDIA-A10G-, NVIDIA-Tesla-T4- oder NVIDIA-Tesla-M60-Hardware zu verwenden. Sie können die GRID-Treiber verwenden, um AMIs sowohl zu erstellen als auch innerhalb der AWS-Umgebung zu verwenden. Durch die Installation der Software stimmen Sie den Bedingungen in der Endbenutzer-Lizenzvereinbarung für NVIDIA GRID Cloud zu.

Überlegungen

- G3-Instances benötigen eine von AWS bereitgestellte DNS-Auflösung, damit die GRID-Lizenzierung funktioniert.
- IMDSv2 wird nur mit NVIDIA-Treiberversion 495.x oder höher unterstützt.

Voraussetzungen

- (Linux) Überprüfen Sie, ob die AWS CLI auf der Instance installiert und mit Standardanmeldeinformationen konfiguriert ist. Weitere Informationen finden Sie unter Installieren der AWS CLI im AWS Command Line Interface-Benutzerhandbuch.
- Ihr Benutzer oder Ihre Rolle muss über die Berechtigungen verfügen, die die AmazonS3ReadOnlyAccess-Richtlinie enthält.

Amazon Linux 2023

So installieren Sie den NVIDIA-Gaming-Treiber auf Ihrer Instance

1. Verbinden Sie sich mit der Instance. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

   ```
   [ec2-user ~]$ sudo dnf update -y
   ```

2. Installieren Sie gcc und make, falls sie noch nicht installiert sind.

   ```
   [ec2-user ~]$ sudo dnf install gcc make
   ```

3. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

   ```
   [ec2-user ~]$ sudo reboot
   ```

4. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
5. Installieren Sie die Kernel-Header-Pakete.

   ```
   [ec2-user ~]$ sudo dnf install -y kernel-devel kernel-modules-extra kernel-devel-
   $(uname -r) kernel-headers-$(uname -r) dkms
   ```

6. Laden Sie das Installationsprogramm für den Gaming-Treiber anhand des folgenden Befehls herunter:

   ```
   [ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
   ```

   Mehrere Versionen des Gaming-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen:

   ```
   [ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
   ```

7. Extrahieren Sie das Installationsprogramm für den Gaming-Treiber aus dem heruntergeladenen `.zip`-Archiv.

   ```
   [ec2-user ~]$ unzip latest-driver-name.zip -d nvidia-drivers
   ```

8. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiber-Installationsprogramms hinzu:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Führen Sie das Installationsprogramm über den folgenden Befehl aus:

```
[ec2-user ~]$ sudo ./nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

   Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

10. Verwenden Sie den folgenden Befehl zum Erstellen der benötigten Konfigurationsdatei.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Laden Sie die Zertifizierungsdatei mit dem folgenden Befehl herunter und benennen Sie sie um.
    - Für Version 460.39 oder höher:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
```

    - Für Version 440.68 bis 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

    - Für frühere Versionen:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Wenn Sie NVIDIA-Treiberversion 510.x oder höher für die G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie in der NVIDIA-Dokumentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

13. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

14. Verifizieren Sie die NVIDIA Gaming-Lizenz mit dem folgenden Befehl:

```
[ec2-user ~]$ nvidia-smi.exe -q
```

    Suchen Sie in der Ausgabe nach `vGPU Software Licensed Product`.

15. (Optional) Um die Vorteile einer Einzelanzeige mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll Amazon DCV ein.

Amazon Linux 2

So installieren Sie den NVIDIA-Gaming-Treiber auf Ihrer Instance

1. Verbinden Sie sich mit der Instance. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
[ec2-user ~]$ sudo yum update -y
```

2. Installieren Sie gcc und make, falls sie noch nicht installiert sind.

```
[ec2-user ~]$ sudo yum install gcc make
```

3. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
[ec2-user ~]$ sudo reboot
```

4. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
5. Installieren Sie das Kernel-Header-Paket für die Version des Kernels, die Sie gerade verwenden.

```
[ec2-user ~]$ sudo yum install -y kernel-devel-$(uname -r)
```

6. Laden Sie das Installationsprogramm für den Gaming-Treiber anhand des folgenden Befehls herunter:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Mehrere Versionen des Gaming-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Extrahieren Sie das Installationsprogramm für den Gaming-Treiber aus dem heruntergeladenen `.zip`-Archiv.

```
[ec2-user ~]$ unzip latest-driver-name.zip -d nvidia-drivers
```

8. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiber-Installationsprogramms hinzu:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Führen Sie das Installationsprogramm über den folgenden Befehl aus:

```
[ec2-user ~]$ sudo ./nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Wenn Sie Amazon Linux 2 mit der Kernel-Version 5.10 verwenden, installieren Sie die NVIDIA-Gaming-Treiber mit dem folgenden Befehl.

```
[ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
```

Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

10. Verwenden Sie den folgenden Befehl zum Erstellen der benötigten Konfigurationsdatei.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Laden Sie die Zertifizierungsdatei mit dem folgenden Befehl herunter und benennen Sie sie um.

    - Für Version 460.39 oder höher:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
```

- Für Version 440.68 bis 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Für frühere Versionen:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Wenn Sie NVIDIA-Treiberversion 510.x oder höher für die G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie in der NVIDIA-Dokumentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

13. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

14. Verifizieren Sie die NVIDIA Gaming-Lizenz mit dem folgenden Befehl:

```
[ec2-user ~]$ nvidia-smi.exe -q
```

    Suchen Sie in der Ausgabe nach `vGPU Software Licensed Product`.

15. (Optional) Um die Vorteile einer Einzelanzeige mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll Amazon DCV ein.

CentOS 7 und Red Hat Enterprise Linux 7

So installieren Sie den NVIDIA-Gaming-Treiber auf Ihrer Instance

1. Herstellen einer Verbindung mit Ihrer Linux-Instance. Installieren Sie gcc und make, falls sie noch nicht installiert sind.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

2. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
[ec2-user ~]$ sudo yum update -y
```

3. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
[ec2-user ~]$ sudo reboot
```

4. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
5. Installieren Sie das Kernel-Header-Paket für die Version des Kernels, die Sie gerade verwenden.

```
[ec2-user ~]$ sudo yum install -y unzip kernel-devel-$(uname -r)
```

6. Deaktivieren Sie den Open-Source-Treiber `nouveau` für NVIDIA-Grafikkarten.

   a. Fügen Sie der Negativliste in der Datei `nouveau` den Eintrag `/etc/modprobe.d/blacklist.conf` hinzu. Kopieren Sie den folgenden Codeblock und fügen Sie ihn in ein Terminalfenster ein.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Bearbeiten Sie die Datei `/etc/default/grub` und fügen Sie folgende Zeile hinzu.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Erstellen Sie die neue Grub-Konfiguration.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Laden Sie das Installationsprogramm für den Gaming-Treiber anhand des folgenden Befehls herunter:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Mehrere Versionen des Gaming-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

8. Extrahieren Sie das Installationsprogramm für den Gaming-Treiber aus dem heruntergeladenen `.zip`-Archiv.

```
[ec2-user ~]$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

9. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiber-Installationsprogramms hinzu:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

10. Führen Sie das Installationsprogramm über den folgenden Befehl aus:

```
[ec2-user ~]$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

11. Verwenden Sie den folgenden Befehl zum Erstellen der benötigten Konfigurationsdatei.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

12. Laden Sie die Zertifizierungsdatei mit dem folgenden Befehl herunter und benennen Sie sie um.
    - Für Version 460.39 oder höher:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
      gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
      ```

    - Für Version 440.68 bis 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Für frühere Versionen:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

13. Wenn Sie NVIDIA-Treiberversion 510.x oder höher für die G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie in der NVIDIA-Dokumentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

14. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

15. (Optional) Um die Vorteile einer Einzelanzeige mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll Amazon DCV ein. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diesen Schritt nicht aus.

CentOS Stream 8 und Red Hat Enterprise Linux 8

So installieren Sie den NVIDIA-Gaming-Treiber auf Ihrer Instance

1. Herstellen einer Verbindung mit Ihrer Linux-Instance. Installieren Sie gcc und make, falls sie noch nicht installiert sind.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

2. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
[ec2-user ~]$ sudo yum update -y
```

3. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
[ec2-user ~]$ sudo reboot
```

4. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
5. Installieren Sie das Kernel-Header-Paket für die Version des Kernels, die Sie gerade verwenden.

```
[ec2-user ~]$ sudo yum install -y unzip kernel-devel-$(uname -r)
```

6. Laden Sie das Installationsprogramm für den Gaming-Treiber anhand des folgenden Befehls herunter:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   Mehrere Versionen des Gaming-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Extrahieren Sie das Installationsprogramm für den Gaming-Treiber aus dem heruntergeladenen `.zip`-Archiv.

```
[ec2-user ~]$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiber-Installationsprogramms hinzu:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Führen Sie das Installationsprogramm über den folgenden Befehl aus:

```
[ec2-user ~]$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

   Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

10. Verwenden Sie den folgenden Befehl zum Erstellen der benötigten Konfigurationsdatei.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
```

```
EOF
```

11. Laden Sie die Zertifizierungsdatei mit dem folgenden Befehl herunter und benennen Sie sie um.
    - Für Version 460.39 oder höher:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
      ```

    - Für Version 440.68 bis 445.48:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

    - Für frühere Versionen:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
      ```

12. Wenn Sie NVIDIA-Treiberversion 510.x oder höher für die G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie in der NVIDIA-Dokumentation.

    ```
    [ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
    ```

    ```
    [ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
    ```

13. Starten Sie die Instance neu.

    ```
    [ec2-user ~]$ sudo reboot
    ```

14. (Optional) Um die Vorteile einer Einzelanzeige mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll Amazon DCV ein.

Rocky Linux 8

So installieren Sie den NVIDIA-Gaming-Treiber auf Ihrer Instance

1. Herstellen einer Verbindung mit Ihrer Linux-Instance. Installieren Sie gcc und make, falls sie noch nicht installiert sind.

```
[ec2-user ~]$ sudo yum install -y gcc make
```

2. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
[ec2-user ~]$ sudo yum update -y
```

3. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
[ec2-user ~]$ sudo reboot
```

4. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
5. Installieren Sie das Kernel-Header-Paket für die Version des Kernels, die Sie gerade verwenden.

```
[ec2-user ~]$ sudo dnf install -y unzip elfutils-libelf-devel libglvnd-devel
 kernel-devel-$(uname -r)
```

6. Laden Sie das Installationsprogramm für den Gaming-Treiber anhand des folgenden Befehls herunter:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   Mehrere Versionen des Gaming-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Extrahieren Sie das Installationsprogramm für den Gaming-Treiber aus dem heruntergeladenen `.zip`-Archiv.

```
[ec2-user ~]$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiber-Installationsprogramms hinzu:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

9. Führen Sie das Installationsprogramm über den folgenden Befehl aus:

```
[ec2-user ~]$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

10. Verwenden Sie den folgenden Befehl zum Erstellen der benötigten Konfigurationsdatei.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Laden Sie die Zertifizierungsdatei mit dem folgenden Befehl herunter und benennen Sie sie um.
    - Für Version 460.39 oder höher:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
      ```

    - Für Version 440.68 bis 445.48:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

    - Für frühere Versionen:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
      ```

12. Wenn Sie NVIDIA-Treiberversion 510.x oder höher für die G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie in der NVIDIA-Dokumentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

13. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

14. (Optional) Um die Vorteile einer Einzelanzeige mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll Amazon DCV ein.

Ubuntu und Debian

So installieren Sie den NVIDIA-Gaming-Treiber auf Ihrer Instance

1. Herstellen einer Verbindung mit Ihrer Linux-Instance. Installieren Sie gcc und make, falls sie noch nicht installiert sind.

```
$ sudo apt-get install -y gcc make build-essential
```

2. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
$ sudo apt-get update -y
```

3. Führen Sie ein Upgrade des `linux-aws`-Pakets durch, um die aktuelle Version zu erhalten.

```
$ sudo apt-get upgrade -y linux-aws
```

4. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
$ sudo reboot
```

5. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
6. Installieren Sie das Kernel-Header-Paket für die Version des Kernels, die Sie gerade verwenden.

```
$ sudo apt install -y unzip dkms linux-headers-$(uname -r)
```

7. Deaktivieren Sie den Open-Source-Treiber `nouveau` für NVIDIA-Grafikkarten.

   a. Fügen Sie der Negativliste in der Datei `nouveau` den Eintrag `/etc/modprobe.d/blacklist.conf` hinzu. Kopieren Sie den folgenden Codeblock und fügen Sie ihn in ein Terminalfenster ein.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
```

```
blacklist nvidiafb
blacklist rivatv
EOF
```

b. Bearbeiten Sie die Datei `/etc/default/grub` und fügen Sie folgende Zeile hinzu.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

c. Erstellen Sie die neue Grub-Konfiguration.

```
$ sudo update-grub
```

8. Laden Sie das Installationsprogramm für den Gaming-Treiber anhand des folgenden Befehls herunter:

```
$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Mehrere Versionen des Gaming-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen:

```
$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

9. Extrahieren Sie das Installationsprogramm für den Gaming-Treiber aus dem heruntergeladenen `.zip`-Archiv.

```
$ unzip *Gaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

10. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiber-Installationsprogramms hinzu:

```
$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

11. Führen Sie das Installationsprogramm über den folgenden Befehl aus:

```
$ sudo nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

12. Verwenden Sie den folgenden Befehl zum Erstellen der benötigten Konfigurationsdatei.

```
$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

13. Laden Sie die Zertifizierungsdatei mit dem folgenden Befehl herunter und benennen Sie sie um.

    - Für Version 460.39 oder höher:

      ```
      $ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
      gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2024_02_22.cert"
      ```

    - Für Version 440.68 bis 445.48:

      ```
      $ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
      gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

    - Für frühere Versionen:

      ```
      $ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
      gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
      ```

14. Wenn Sie NVIDIA-Treiberversion 510.x oder höher für die G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie in der NVIDIA-Dokumentation.

    ```
    $ sudo touch /etc/modprobe.d/nvidia.conf
    ```

    ```
    $ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
    modprobe.d/nvidia.conf
    ```

15. Starten Sie die Instance neu.

    ```
    $ sudo reboot
    ```

16. (Optional) Um die Vorteile einer Einzelanzeige mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll Amazon DCV ein. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diesen Schritt nicht aus.

Windows-Betriebssysteme

Bevor Sie einen NVIDIA-Gaming-Treiber auf Ihrer Instance installieren, müssen Sie sicherstellen, dass zusätzlich zu den für alle Gaming-Treiber genannten Überlegungen die folgenden Voraussetzungen erfüllt sind.

- Wenn Sie Ihre Windows-Instance mit einem benutzerdefinierten Windows-AMI starten, muss es sich bei dem AMI um ein mit Windows Sysprep erstelltes standardisiertes Image handeln, um sicherzustellen, dass der Gaming-Treiber funktioniert. Weitere Informationen finden Sie unter Ein Amazon-EC2-AMI mit Windows Sysprep erstellen.
- Konfigurieren der Standardanmeldeinformationen für AWS Tools for Windows PowerShell auf Ihrer Windows-Instance. Weitere Informationen finden Sie unter Erste Schritte in AWS Tools for Windows PowerShell im AWS -Tools für PowerShell-Benutzerhandbuch.

So installieren Sie den NVIDIA-Gaming-Treiber auf einer Windows-Instance

1. Stellen Sie eine Verbindung mit Ihrer Windows-Instance her und öffnen Sie ein PowerShell-Fenster.
2. Laden Sie den Gaming-Treiber anhand der folgenden PowerShell-Befehle herunter und installieren Sie ihn.

```
$Bucket = "nvidia-gaming"
$KeyPrefix = "windows/latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
$LocalFilePath = Join-Path $LocalPath $LocalFileName
Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

   Mehrere Versionen des NVIDIA GRID-Treibers werden in diesem S3-Bucket gespeichert. Sie können alle verfügbaren Versionen im Bucket herunterladen, wenn Sie den Wert der `$KeyPrefix`-Variablen von „windows/latest“ auf „windows“ ändern.
3. Navigieren Sie zu Ihrem Desktop und doppelklicken Sie auf die Installationsdatei, um sie auszuführen (wählen Sie die Treiberversion für das Betriebssystem Ihrer Instance aus). Befolgen

Sie die Anweisungen, um den Treiber zu installieren, und starten Sie die Instance neu, wenn Sie dazu aufgefordert werden. Sie können prüfen, ob die GPU richtig funktioniert, indem Sie den Geräte-Manager verwenden.

4. Verwenden Sie eine der folgenden Methoden, um den Treiber zu registrieren.

   Version 527.27 or above

   Erstellen Sie den folgenden Registrierungsschlüssel mit der 64-Bit-Version von PowerShell oder dem Eingabeaufforderungsfenster.

   key: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global`

   Name: vGamingMarketplace

   Typ: DWord

   Wert: 2

   PowerShell

   Führen Sie den folgenden PowerShell-Befehl aus, um diesen Registrierungswert zu erstellen. Die AWS -Tools für PowerShell in AWS-Windows-AMIs ist standardmäßig eine 32-Bit-Version und dieser Befehl schlägt fehl. Verwenden Sie stattdessen die 64-Bit-Version von PowerShell, die im Betriebssystem enthalten ist.

   ```
   New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global"
    -Name "vGamingMarketplace" -PropertyType "DWord" -Value "2"
   ```

   Eingabeaufforderung

   Führen Sie den folgenden Registrierungsbefehl aus, um diesen Registrierungswert zu erstellen. Sie können ihn im Eingabeaufforderungsfenster oder in einer 64-Bit-Version von PowerShell ausführen.

   ```
   reg add "HKLM\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global" /v
    vGamingMarketplace /t REG_DWORD /d 2
   ```

Earlier versions

Erstellen Sie den folgenden Registrierungsschlüssel mit der 64-Bit-Version von PowerShell oder dem Eingabeaufforderungsfenster.

key: `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global`

Name: vGamingMarketplace

Typ: DWord

Wert: 2

PowerShell

Führen Sie den folgenden PowerShell-Befehl aus, um diesen Registrierungswert zu erstellen. Die AWS -Tools für PowerShell in AWS-Windows-AMIs ist standardmäßig eine 32-Bit-Version und dieser Befehl schlägt fehl. Verwenden Sie stattdessen die 64-Bit-Version von PowerShell, die im Betriebssystem enthalten ist.

```
New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name
 "vGamingMarketplace" -PropertyType "DWord" -Value "2"
```

Eingabeaufforderung

Führen Sie den folgenden Registrierungsbefehl aus, um diesen Registrierungsschlüssel im Eingabeaufforderungsfenster zu erstellen. Sie können diesen Befehl auch in der 64-Bit-Version von PowerShell verwenden.

```
reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global" /v vGamingMarketplace /t
 REG_DWORD /d 2
```

5. Führen Sie den folgenden Befehl in PowerShell aus. Dadurch wird die Zertifizierungsdatei heruntergeladen, die Datei in `GridSwCert.txt` umbenannt und in den Ordner „Öffentliche Dokumente“ auf dem Systemlaufwerk verschoben. In der Regel lautet der Ordnerpfad `C:\Users\Public\Documents`.
   - Für Version 460.39 oder höher:

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
Archive/GridSwCertWindows_2024_02_22.cert" -OutFile "$Env:PUBLIC\Documents
\GridSwCert.txt"
```

- Für Version 445.87:

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
Archive/GridSwCert-Windows_2020_04.cert" -OutFile "$Env:PUBLIC\Documents
\GridSwCert.txt"
```

- Für frühere Versionen:

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
Archive/GridSwCert-Windows_2019_09.cert" -OutFile "$Env:PUBLIC\Documents
\GridSwCert.txt"
```

Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 oder früher verwenden, muss TLS 1.2 möglicherweise für Ihr PowerShell-Terminal aktiviert werden. Sie können TLS 1.2 für die aktuelle PowerShell-Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

6. Starten Sie Ihre Instance neu.
7. Suchen Sie die `nvidia-smi.exe`-Datei auf der Instance.

```
Get-ChildItem -Path C:\ -Recurse -Filter "nvidia-smi.exe"
```

Verifizieren Sie die NVIDIA Gaming-Lizenz mit dem folgenden Befehl: Ersetzen Sie *Pfad* durch den Namen des Ordners in der Ausgabe vom vorherigen Befehl.

```
C:\Windows\System32\DriverStore\FileRepository\path\nvidia-smi.exe -q
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen.

```
vGPU Software Licensed Product
Product Name              : NVIDIA Cloud Gaming
License Status            : Licensed (Expiry: N/A)
```

8. (Optional) Um die Vorteile der Einzelanzeige mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll Amazon DCV ein. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diesen Schritt nicht aus.

ENA-Treiber auf EC2-Windows-Instances installieren

Wenn Ihre Instance nicht auf einem der neuesten Windows Amazon Machine Images (AMIs) basiert, die Amazon bereitstellt, verwenden Sie das folgende Verfahren, um den aktuellen ENA-Treiber auf Ihrer Instance zu installieren. Sie sollten diese Aktualisierung zu einem Zeitpunkt durchführen, zu dem Ihre Instance neu gestartet werden kann. Wenn das Installationsskript Ihre Instance nicht automatisch neu startet, empfehlen wir, die Instance als letzten Schritt neu zu starten.

Wenn Sie ein Instance-Speicher-Volume verwenden, um Daten zu speichern, während die Instance läuft, werden diese Daten gelöscht, wenn Sie die Instance beenden. Stellen Sie vor dem Anhalten Ihrer Instance sicher, dass Sie alle benötigten Daten aus den Instance-Speicher-Volumes in einen persistenten Speicher kopiert haben, z. B. Amazon EBS oder Amazon S3.

Voraussetzungen

Um den ENA-Treiber zu installieren oder zu aktualisieren, muss Ihre Windows-Instance die folgenden Voraussetzungen erfüllen:

- PowerShell Version 3.0 oder höher ist installiert.
- Die in diesem Abschnitt aufgeführten Befehle müssen in der 64-Bit-Version von PowerShell ausgeführt werden. Verwenden Sie nicht die x86-Version von PowerShell. Das ist die 32-Bit-Version der Shell und wird für diese Befehle nicht unterstützt.

Schritt 1: Ihre Daten sichern

Wir empfehlen Ihnen, ein Backup-AMI zu erstellen, falls Sie Ihre Änderungen nicht über den Geräte-Manager rückgängig machen können. Gehen Sie wie folgt vor, um ein Backup-AMI mit der AWS-Managementkonsole zu erstellen:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance, die ein Treiberupgrade benötigt und wählen Sie Instance stoppen aus dem Menü Instance-Status aus.

4. Nachdem die Instance angehalten wurde, wählen Sie die Instance erneut aus. Um Ihr Backup zu erstellen, wählen Sie die Option Image und Vorlagen im Menü Aktionen und dann Image erstellen.
5. Um Ihre Instance neu zu starten, wählen Sie Instance starten aus dem Menü Instance-Status.

Schritt 2: Installieren oder aktualisieren Ihres ENA-Treibers

Sie können Ihren ENA-Treiber mit AWS Systems Manager-Distributor oder PowerShell cmdlets installieren oder aktualisieren. Für weitere Anweisungen wählen Sie die Registerkarte aus, die der Methode entspricht, die Sie verwenden möchten.

Systems Manager Distributor

Sie können das Systems-Manager-Distributor-Feature verwenden, um Pakete für Ihre von Systems Manager verwalteten Knoten bereitzustellen. Mit Systems Manager Distributor können Sie das ENA-Treiberpaket einmal oder mit geplanten Aktualisierungen installieren. Weitere Informationen zur Installation des ENA-Treiberpakets (`AwsEnaNetworkDriver`) mit Systems Manager Distributor finden Sie unter Installieren oder Aktualisieren von Paketen im AWS Systems Manager-Benutzerhandbuch.

PowerShell

In diesem Abschnitt wird beschrieben, wie Sie ENA-Treiberpakete mit PowerShell cmdlets herunterladen und auf Ihrer Instance installieren.

Option 1: Die neueste Version herunterladen und extrahieren

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
2. Verwenden Sie das invoke-webrequest cmdlet, um das neueste Treiberpaket herunterzuladen:

```
PS C:\> invoke-webrequest https://ec2-windows-drivers-
downloads.s3.amazonaws.com/ENA/Latest/AwsEnaNetworkDriver.zip -
outfile $env:USERPROFILE\AwsEnaNetworkDriver.zip
```

> **Note**
>
> Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 oder früher verwenden, muss TLS 1.2 möglicherweise für Ihr PowerShell-Terminal aktiviert werden. Sie können TLS 1.2 für die aktuelle PowerShell-Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```
>
> Alternativ können Sie das neueste Treiberpaket aus einem Browserfenster auf Ihrer Instance herunterladen.

3. Verwenden Sie das expand-archive cmdlet, um das ZIP-Archiv zu extrahieren, das Sie auf Ihre Instance heruntergeladen haben:

```
PS C:\> expand-archive $env:userprofile\AwsEnaNetworkDriver.zip -
DestinationPath $env:userprofile\AwsEnaNetworkDriver
```

Option 2: Eine bestimmte Version herunterladen und extrahieren

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
2. Laden Sie das ENA-Treiberpaket für die gewünschte Version über den Versionslink in der Versionsverlauf für den ENA-Windows-Treiber-Tabelle herunter.
3. Extrahieren Sie die ZIP-Datei auf Ihre Instance.

Installieren der ENA-Treiber mit PowerShell

Die Installationsschritte sind dieselben, unabhängig davon, ob Sie den neuesten Treiber oder eine bestimmte Version heruntergeladen haben. Um den ENA-Treiber zu installieren, gehen Sie folgendermaßen vor.

1. Um den Treiber zu installieren, führen Sie das `install.ps1`-PowerShell-Skript aus dem `AwsEnaNetworkDriver`-Verzeichnis auf Ihrer Instance aus. Wenn ein Fehler angezeigt wird, stellen Sie sicher, dass Sie PowerShell 3.0 oder höher verwenden.
2. Wenn das Installationsprogramm Ihre Instance nicht automatisch neu startet, führen Sie den Restart-Computer PowerShell Cmdlet aus.

```
PS C:\> Restart-Computer
```

Schritt 3 (optional): Überprüfen Sie die ENA-Treiberversion nach der Installation

Um sicherzustellen, dass das ENA-Treiberpaket erfolgreich auf Ihrer Instance installiert wurde, können Sie die neue Version wie folgt überprüfen:

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
2. Zum Aufrufen des Windows-Geräte-Managers geben Sie `devmgmt.msc` im Feld Run (Ausführen) ein.
3. Wählen Sie OK aus. Dadurch wird das Fenster „Device Manager“ (Geräte-Manager) geöffnet.
4. Wählen Sie den Pfeil links neben Network adapters (Netzwerkadapter) aus, um die Liste zu erweitern.
5. Wählen Sie den Namen aus oder öffnen Sie das Kontextmenü für den Amazon Elastic Network Adapter und wählen Sie dann Properties (Eigenschaften) aus. Dadurch wird das Dialogfeld mit den Eigenschaften des Amazon Elastic Network Adapters geöffnet.

   > **Note**
   >
   > ENA-Adapter verwenden alle denselben Treiber. Wenn Sie mehrere ENA-Adapter haben, können Sie einen von ihnen auswählen, um den Treiber für alle ENA-Adapter zu aktualisieren.

6. Um zu überprüfen, welche Version aktuell installiert ist, öffnen Sie die Registerkarte Treiber und überprüfen Sie die Treiberversion. Falls die aktuelle Version nicht mit Ihrer Zielversion übereinstimmt, finden Sie weitere Informationen unter Fehlerbehebung beim Windows-Treiber von Elastic Network Adapter.

Eine ENA-Treiberinstallation rückgängig machen

Wenn bei der Installation etwas schiefgeht, müssen Sie möglicherweise den Treiber zurücksetzen. Gehen Sie wie folgt vor, um zur vorherigen Version des ENA-Treibers zurückzukehren, der auf Ihrer Instance installiert war.

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
2. Zum Aufrufen des Windows-Geräte-Managers geben Sie `devmgmt.msc` im Feld Run (Ausführen) ein.
3. Wählen Sie OK aus. Dadurch wird das Fenster „Device Manager“ (Geräte-Manager) geöffnet.
4. Wählen Sie den Pfeil links neben Network adapters (Netzwerkadapter) aus, um die Liste zu erweitern.
5. Wählen Sie den Namen aus oder öffnen Sie das Kontextmenü für den Amazon Elastic Network Adapter und wählen Sie dann Properties (Eigenschaften) aus. Dadurch wird das Dialogfeld mit den Eigenschaften des Amazon Elastic Network Adapters geöffnet.

   > **Note**
   >
   > ENA-Adapter verwenden alle denselben Treiber. Wenn Sie mehrere ENA-Adapter haben, können Sie einen von ihnen auswählen, um den Treiber für alle ENA-Adapter zu aktualisieren.

6. Um den Treiber zurückzusetzen, öffnen Sie die Registerkarte Treiber und wählen Sie Treiber zurücksetzen. Dadurch wird das Rollback-Fenster für das Treiberpaket geöffnet.

   > **Note**
   >
   > Wenn auf der Registerkarte Treiber die Aktion Treiber zurücksetzen nicht angezeigt wird oder wenn die Aktion nicht verfügbar ist, bedeutet dies, dass der Treiberspeicher auf Ihrer Instance das zuvor installierte Treiberpaket nicht enthält. Um dieses Problem zu beheben, siehe Fehlerbehebungsszenarien und erweitern Sie den Abschnitt Unerwartete ENA-Treiberversion installiert. Weitere Informationen zur Auswahl von Gerätetreiberpaketen finden Sie auf der Microsoft-Dokumentationswebsite unter So wählt Windows ein Treiberpaket für ein Gerät aus.

NA-Windows-Treiber-Versionen verfolgen

Windows AMIs inkludieren den Amazon-ENA-Treiber zum Aktivieren von Erweitertem Netzwerk.

Für Windows Server-Versionen 2016 und höher empfehlen wir, die neueste Treiberversion zu verwenden. Für frühere Versionen von Windows Server können Sie anhand der folgenden Tabelle ermitteln, welche ENA-Treiberversion verwendet werden sollte.

Windows Server Version	ENA-Treiberversion
Windows Server 2012 R2	2.6.0 und niedriger
Windows Server 2012	2.6.0 und niedriger
Windows Server 2008 R2	2.2.3 und niedriger

Versionsverlauf für den ENA-Windows-Treiber

Die folgende Tabelle fasst die Änderungen für jede Version zusammen.

Treiberversion	Details	Datum der Veröffentlichung
2.11.0	Neue Features • Unterstützung für dynamische Warteschlangenzuweisung mit Skalierung auf bis zu 64 I/O-Warteschlangen hinzugefügt, vorbehaltlich der Limits für den Instance-Typ. Bugfixes • Fehlende Behandlung von Fehlerbedingungen beim Abrufen der physikalischen DMA-Adressbreite vom Gerät behoben.	1. August 2025

Treiberversion	Details	Datum der Veröffentlichung
2.10.0	Bugfixes • Die unsachgemäße Behandlung von Fehlern bei der Speicherzuweisung während der Warteschlangeninitialisierung wurde behoben, um unerwartete Neustarts zu verhindern. • Es wurde eine mögliche Fehlkonfiguration von Netzwerk-Offloads behoben, bei der Gerätefunktionen ignoriert wurden.	24. Juni 2025

Treiberversion	Details	Datum der Veröffentlichung
2.9.0	Neue Features • Unterstützung für asynchrone Reset-Anfragen hinzugefügt, die vom Gerät initiiert wurden. • Unterstützung für die Verarbeitung des vom Gerät bereitgestellten maximalen LLQ-Tiefenwerts wurde hinzugefügt. • In der Windows-Ereignisanzeige wurde eine Ereignis-ID `58001` hinzugefügt, um die Sichtbarkeit unerwarteter Energiestatussübergänge zu verbessern, die durch eine Fehlkonfiguration des Geräts verursacht werden. Bugfixes • Die unsachgemäße Behandlung von Fehlern bei der Arbeitsspeicherzuweisung während der Geräteinitialisierung wurde behoben, um unerwartete Neustarts zu verhindern. • Es wurde ein Problem in der Interrupt-Serviceroutine behoben, durch das ein DPC beim Anhalten des Geräts in die Warteschlange gestellt werden konnte, wodurch unerwartete Neustarts verhindert wurden.	12. Dezember 2024

Treiberversion	Details	Datum der Veröffentlichung
2.8.0	Bugfixes • Bei der Verarbeitung der ausgehenden Netzwerkp ufferliste (Network Buffer List, NBL) wurde ein Problem behoben, das zu Speicherfehlern führen konnte, wenn versucht wurde, eine bereits veröffentlichte NBL zu veröffentlichen. • Fehlerhafte Erkennung des L3-Protokolls bei der Deaktivierung aller LSO- und Prüfsummen-Offloads, die zu unerwartetem Verhalten führen konnte, wurde behoben.	30. September 2024

Treiberversion	Details	Datum der Veröffentlichung
2.7.0	Neue Features • Die Unterstützung für Windows Server 2012 (Windows 8) und Windows Server 2012 R2 (Windows 8.1) wurde entfernt. Diese Betriebssystemversionen haben das Ende des Supports von AWS erreicht. Die Treiberin stallation wird unter Windows Server 2012 und früheren Versionen fehlschlagen. • Unterstützung für die Übertragung der IPv6-Tx-P rüfsummenberechnung auf das Gerät wurde hinzugefü gt. • Umfassende Unterstützung für Low Latency Queuing (LLQ) hinzugefügt. Dies wird basierend auf der Geräteempfehlung dynamisch aktiviert. Sie können diese Einstellung mit dem neuen Registrierungsschl üssel „WideLLQ“ überschreiben. • Es wurde eine Meldung für Paketverluste hinzugefügt, die auf einen Rx-Überlauf zurückzuführen sind, was darauf hindeutet, dass im Rx-Ring nicht genügend Speicherplatz für eingehende Pakete verfügbar ist. • Unterstützung für Benachrichtigungen zu suboptima len Konfigurationen vom Gerät wurde hinzugefügt. Sehen Sie sich die Ereignis-ID `59000` in der Windows-Ereignisanzeige an. Bugfixes •	1. Mai 2024

Treiberversion	Details	Datum der Veröffentlichung
	Vermeiden Sie unnötiges Zurücksetzen von Geräten, die durch Tx-Pakete verursacht werden, deren Header die maximale Low Latency Queuing (LLQ)-Header-Größe überschreiten.	

Treiberversion	Details	Datum der Veröffentlichung

2.6.0	Neue Features
	• Fügt die folgenden Netzwerkleistungsmetriken für Instance-Typen hinzu, die ENA Express unterstützen.
	  • `ena_srd_mode`
	  • `ena_srd_tx_pkts`
	  • `ena_srd_eligible_tx_pkts`
	  • `ena_srd_rx_pkts`
	  • `ena_srd_resource_utilization`
	• Fügt die Netzwerkleistungsmetrik `conntrack_allowance_available` für Nitro-basierte Instance-Typen hinzu.
	• Fügt einen neuen Grund für das Zurücksetzen des Adapters hinzu, weil eine Beschädigung der RX-Daten erkannt wurde.
	• Aktualisiert die Infrastruktur zur Treiberprotokollierung.
	
	Bugfixes
	• Verhindert das Zurücksetzen des Adapters für den Fall, dass ein Update der Netzwerkleistungsmetriken aufgrund von CPU-Mangel fehlschlägt.
	•
		20. Juni 2023

Treiberversion	Details	Datum der Veröffentlichung
	Verhindert die falsche Erkennung einer Unterbrechung des Geräte-Heartbeats. • Korrigiert das Treiberinstallationsskript, um den Downgrade-Vorgang zu unterstützen. • Korrigiert die Statistik zur Anzahl der Empfangsfehler.	
2.5.0	Ankündigung Die ENA-Windows-Treiberversion 2.5.0 wurde zurückgesetzt, da die Initialisierung auf dem Windows-Domain-Controller fehlgeschlagen ist. Windows Client und Windows Server sind nicht betroffen.	17. Februar 2023

Treiberversion	Details	Datum der Veröffentlichung
2.4.0	Neue Features • Fügt Unterstützung für Windows Server 2022 hinzu. • Entfernt Unterstützung für Windows Server 2008 R2. • Setzt Low Latency Queuing (LLQ) auf immer aktiviert , um die Leistung bei Amazon-EC2-Instances der sechsten Generation zu verbessern. Bugfixes • Behebt ein Problem, durch das die Weitergabe von Netzwerkleistungsmetriken an die Leistungsindikatoren für Windows (PCW) fehlschlug. • Behebt ein Speicherleck während des Lesevorgangs des Registrierungsschlüssels. • Verhindert eine unendliche Reset-Schleife im Falle eines nicht behebbaren Fehlers während der Adapterrü cksetzung.	28. April 2022

Treiberversion	Details	Datum der Veröffentlichung
2.2.4	Ankündigung Die ENA-Windows-Treiberversion 2.2.4 wurde aufgrund einer möglichen Leistungsverschlechterung bei EC2-Instances der sechsten Generation zurückgesetzt. Es wird empfohlen, dass Sie ein Downgrade des Treibers mit einer der folgenden Methoden durchführen: • Installieren der vorherigen Version 1. Laden Sie das vorherige Versionspaket über den Link in dieser Tabelle herunter (Version 2.2.3). 2. Führen Sie das install.ps1-PowerShell-Installationsskript aus. Weitere Informationen zu Schritten vor und nach der Installation finden Sie unter Aktivieren von Enhanced Networking unter Windows. • Verwenden von Amazon EC2 Systems Manager für ein Massenupdate • Führen Sie eine Massenaktualisierung über ein SSM-Dokument `AWS-ConfigureAWSPackage` mit folgenden Parametern durch: • Name: AwsEnaNetworkDriver • Version: 2.2.3	26. Oktober 2021

Treiberversion	Details	Datum der Veröffentlichung
2.2.3	Neue Features • Integriert Unterstützung für neue Nitro-Karten mit bis zu 400 Gbit/s Instance-Netzwerken. Bugfixes • Behebt die Race-Bedingung zwischen der Änderung der Systemzeit und der Abfrage der Systemzeit durch den ENA-Treiber, was zu einer fälschlicherweise positiven Erkennung von HW-Nichtreaktionen führt. Ankündigung Die Windows-ENA-Treiberversion 2.2.3 ist die letzte Version, die Unterstützung für Windows Server 2008 R2 bietet. Derzeit verfügbare Instance-Typen, die ENA verwenden, werden unter Windows Server 2008 R2 weiterhin unterstützt. Die Treiber sind per Download verfügbar. Künftige Instance-Typen bieten keine Unterstützung für Windows Server 2008 R2 und Sie können Images mit Windows Server 2008 R2 nicht auf künftige Instance-Typen importieren, migrieren oder auf diesen starten.	25. März 2021

Treiberversion	Details	Datum der Veröffentlichung
2.2.2	Neue Features • Fügt Unterstützung für die Abfrage von Netzwerkadapter-Performance-Metriken mit CloudWatch und den Leistungsindikatoren für Windows-Verbraucher hinzu. Bugfixes • Behebt Leistungsprobleme bei Bare-Metal-Instances.	21. Dezember 2020
2.2.1	Neue Features • Fügt eine Methode hinzu, mit der der Host den Elastic-Network-Adapter nach Netzwerkleistungsmetriken abfragen kann.	1. Oktober 2020

Treiberversion	Details	Datum der Veröffentlichung
2.2.0	Neue Features • Fügt Unterstützung für Hardwaretypen der nächsten Generation hinzu. • Verbessert die Startzeit der Instance nach der Wiederaufnahme aus dem Stop-Ruhezustand und eliminiert falsch positive ENA-Fehlermeldungen. Leistungsoptimierungen • Optimiert die Verarbeitung des eingehenden Datenverkehrs. • Verbessert die Verwaltung des gemeinsam genutzten Speichers in einer Umgebung mit geringen Ressourcen. Bugfixes • Vermeidet Systemabsturz beim Entfernen von ENA-Geräten in seltenen Fällen, in denen der Treiber nicht zurückgesetzt werden kann.	12. August 2020
2.1.5	Bugfixes • Behebt gelegentliche Netzwerkadapter-Initialisierungsfehler auf Bare-Metal-Instances.	23. Juni 2020

Treiberversion	Details	Datum der Veröffentlichung
2.1.4	Bugfixes • Verhindern Sie Verbindungsprobleme durch vom Netzwerk-Stack eingehende beschädigte LSO-Paket metadaten. • Verhindern Sie einen Systemabsturz durch eine seltene Race-Condition, die zum Zugriff auf einen bereits freigegebenen Paketspeicher führt.	25. November 2019
2.1.2	Neue Features • Unterstützung für den Vendor-ID-Bericht hinzugefügt, um dem Betriebssystem das Generieren MAC-basierter UUIDs zu ermöglichen. Bugfixes • Verbesserte DHCP-Netzwerkkonfigurationsleistung während der Initialisierung. • Korrekte Berechnung der L4-Prüfsumme für eingehend en IPv6-Datenverkehr, wenn die maximale Übertragu ngseinheit (MTU) 4 K überschreitet. • Allgemeine Verbesserungen der Treiberstabilität und kleinere Fehlerbehebungen.	4. November 2019

Treiberversion	Details	Datum der Veröffentlichung
2.1.1	Bugfixes • Verhinderung von Drops hoch fragmentierter TCP-LSO-Pakete, die aus dem Betriebssystem eingehen. • Ordnungsgemäße Verarbeitung des Encapsulating Security Payload (ESP)-Protokolls innerhalb von IPSec in IPv6-Netzwerken.	16. September 2019

Treiberversion	Details	Datum der Veröffentlichung

2.1.0	ENA Windows-Treiber v2.1 führt neue ENA-Gerät efunktionalitäten ein. Die Leistung wird gesteigert, es werden neue Features hinzugefügt und mehrere Stabilitä tsverbesserungen vorgenommen.
	
	Neue Features
	
	• Verwenden Sie den standardisierten Windows-R egistrierungsschlüssel für Jumbo-Rahmenkonfig urationen.
	• Erlauben Sie die VLAN-ID-Einstellung über die ENA-Treibereigenschaften-GUI.
	• Verbesserte Wiederherstellungsflüsse
	  • Verbesserte Mechanismen zur Ausfallidentifikation.
	  • Zusätzliche Unterstützung für einstellbare Wiederher stellungsparameter.
	• Unterstützung für bis zu 32 I/O-Warteschlangen für neuere EC2-Instances, die mehr als 8 vCPUs haben.
	• ~90 % Verringerung des Treiber-Arbeitsspeicherplat zes.
	
	Leistungsoptimierungen
	
	• Geringere Latenz des Übertragungspfads.
	• Unterstützung für den Empfang des Checksum Offload.
	•
		1. Juli 2019

Treiberversion	Details	Datum der Veröffentlichung
	Leistungsoptimierung für schwer geladenes System (optimierte Nutzung der Sperrmechanismen). • Weitere Verbesserungen, um die CPU-Nutzung zu verringern und die Reaktionsfähigkeit des Systems unter Last zu verbessern. Bugfixes • Absturz während ungültigem Parsing nicht fortlaufender Tx-Header behoben. • Absturz des Treibers v1.5 während Trennung der Elastic-Network-Schnittstelle auf Bare-Metal-Instances behoben. • Berechungsfehler über IPv6 der LSO-Pseudo-Header-Prüfsumme behoben • Potenzielles Leck der Arbeitsspeicherressource bei fehlgeschlagener Initialisierung behoben. • TCP/UDP Checksum Offload für IPv4-Fragmente deaktiviert. • Fix für VLAN-Konfiguration. VLAN wurde falsch deaktiviert, als nur die VLAN-Priorität hätte deaktiviert werden sollen. • Korrektes Parsing der Kunden-Treibermeldungen durch die Ereignisanzeige aktiviert. •	

Treiberversion	Details	Datum der Veröffentlichung
	Fehler beim Initialisieren des Treibers aufgrund ungültiger Zeitstempel-Bearbeitung behoben. • Laufbedingung zwischen Datenverarbeitung und ENA-Gerätedeaktivierung behoben.	
1.5.0	Aktualisierungen • Stabilitäts- und Leistungsverbesserungen. • Empfangspuffer können jetzt mit einem Wert bis zu 8192 in den erweiterten Eigenschaften der ENA NIC konfiguriert werden. • Standardempfangspuffer 1k.	4. Oktober 2018
1.2.3	Enthält Zuverlässigkeitskorrekturen und vereinheitlicht die Unterstützung für Windows Server 2008 R2 bis Windows Server 2016.	13. Februar 2018
1.0.8	Die Erstversion. Enthalten in AMIs für Windows Server 2008 R2, Windows Server 2012 RTM, Windows Server 2012 R2 und Windows Server 2016.	. Juli 2016

ENA-Benachrichtigungen zur Windows-Treiberveröffentlichung von Amazon SNS abonnieren

Amazon SNS kann Sie benachrichtigen, wenn neue Versionen von EC2-Windows-Treibern veröffentlicht werden. Führen Sie die folgenden Schritte durch, um diese Benachrichtigungen zu abonnieren.

EC2-Benachrichtigungen abonnieren

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Ändern Sie, falls erforderlich, die Region in der Navigationsleiste zu US East (N. Virginia). Sie müssen diese Region auswählen, weil sich die SNS-Benachrichtigungen, die Sie abonnieren, in dieser Region befinden.
3. Wählen Sie im Navigationsbereich Subscriptions aus.
4. Wählen Sie Create subscription.
5. Führen Sie im Dialogfeld Create subscription Folgendes aus:
   a. Kopieren Sie den folgenden Amazon-Ressourcennamen (ARN) unter TopicARN:

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers
   b. Wählen Sie unter Protocol die Option `Email` aus.
   c. Geben Sie als Endpunkt eine E-Mail-Adresse ein, an die die Benachrichtigungen gesendet werden sollen.
   d. Wählen Sie Create subscription (Abonnement erstellen) aus.
6. Sie erhalten eine Bestätigungs-E-Mail. Öffnen Sie die E-Mail und befolgen Sie die Anweisungen, um Ihr Abonnement abzuschließen.

Jedes Mal wenn neue EC2-Treiber für Windows veröffentlicht werden, senden wir ein Benachrichtigung an die Abonnenten. Wenn Sie diese Benachrichtigungen nicht mehr erhalten möchten, führen Sie die folgenden Schritte aus, um sich abzumelden.

Kündigen eines Abonnements der Benachrichtigungen zu Amazon-EC2-Treibern für Windows

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie im Navigationsbereich Subscriptions aus.
3. Aktivieren Sie das Kontrollkästchen für das Abonnement und wählen Sie dann Actions und Delete subscriptions (Löschen) aus. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

Paravirtual-Treiber für Windows-Instances

Windows-AMIs enthalten eine Reihe von Treibern, die den Zugriff auf virtualisierte Hardware ermöglichen. Diese Treiber werden von Amazon EC2 verwendet, um Instance-Speicher und

Amazon EBS-Volumes den jeweiligen Geräte zuzuordnen. Die folgende Tabelle zeigt die wichtigsten Unterschiede zwischen den verschiedenen Treibern.

	Red Hat PV	Citrix PV	AWS PV
Instance-Typ	Wird nicht für alle Instance-Typen unterstützt. Wenn Sie einen nicht unterstützten Instance-Typ angeben, ist die Instance beeinträchtigt.	Wird für Xen-Instance-Typen unterstützt.	Wird für Xen-Instance-Typen unterstützt.
Zugeordnete Volumes	Unterstützt bis zu 16 zugeordnete Volumes	Unterstützt mehr als 16 zugeordnete Volumes	Unterstützt mehr als 16 zugeordnete Volumes
Netzwerk	Bekannte Probleme mit dem Treiber: Die Netzwerkverbindung wird bei hohen Workloads zurückgesetzt, z. B bei schneller Datenübertragung über FTP.		Der Treiber konfiguriert automatisch Jumbo-Frames auf dem Netzwerkadapter, wenn er sich in einem kompatiblen Instance-Typ befindet. Wenn sich die Instance in einer Cluster-Placement-Gruppe befindet, wird die Netzwerkl

	Red Hat PV	Citrix PV	AWS PV
			eistung zwischen den Instances in der Cluster-Placement-Gruppe verbesser t. Weitere Informati onen finden Sie unter Platzieru ngsgruppe n für Ihre Amazon-EC 2-Instances.

Die folgende Tabelle zeigt, welche PV-Treiber Sie unter den einzelnen Versionen von Windows Server in Amazon EC2 verwenden sollten;.

Windows Server Version	PV-Treiber Version
Windows Server 2025	Nicht unterstützt
Windows Server 2022	AWSAktuelle PV-Version
Windows Server 2019	AWSAktuelle PV-Version
Windows Server 2016	AWSAktuelle PV-Version
Windows Server 2012 R2	AWS PV-Version 8.4.3
Windows Server 2012	AWS PV-Version 8.4.3
Windows Server 2008 R2	AWS-PV, Version 8.3.5

Windows Server Version	PV-Treiber Version
Windows Server 2008	Citrix PV 5.9
Windows Server 2003	Citrix PV 5.9

Inhalt

- AWS PV-Treiber
- Citrix-PV-Treiber
- PV-Treiber von Red Hat
- Abonnieren von -Benachrichtigungen
- Upgrade von PV-Treibern auf EC2-Windows-Instances
- Fehler bei PV-Treibern auf Windows-Instances beheben

AWS PV-Treiber

Die AWS PV-Treiber werden im Verzeichnis `%ProgramFiles%\Amazon\Xentools` gespeichert. In diesem Verzeichnis sind außerdem öffentliche Symbole und das Befehlszeilen-Tool `xenstore_client.exe` enthalten, mit dem Sie auf Elemente in XenStore zugreifen können. Der folgende PowerShell-Befehl gibt z B. die aktuelle Zeit von dem Hypervisor zurück:

```
PS C:\> [DateTime]::FromFileTimeUTC((gwmi -n root\wmi -cl
 AWSXenStoreBase).XenTime).ToString("hh:mm:ss")
11:17:00
```

Die AWS PV-Treiberkomponenten werden in der Windows-Registry unter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services` aufgelistet. Diese Treiberkomponenten umfassen im Einzelnen: xenbus, xeniface, xennet, xenvbd und xenvif.

AWS PV-Treiber beinhalten auch einen Windows-Service mit dem Namen LiteAgent, der im Benutzermodus ausgeführt wird. Er übernimmt Aufgaben wie das Beenden und erneute Starten von Ereignissen über AWS-APIs auf Instances der Xen-Generation. Sie können auf Services zugreifen und diese verwalten, indem Sie `Services.msc` in der Befehlszeile ausführen. Bei der Ausführung auf Instances der Nitro-Generation werden die AWS PV-Treiber nicht verwendet und der LiteAgent-Service stoppt ab Treiberversion 8.2.4 selbst. Ein Update auf den neuesten AWS PV-Treiber aktualisiert auch den LiteAgent und verbessert die Zuverlässigkeit auf allen Instance-Generationen.

Installieren der aktuellen AWS PV-Treiber

Amazon Windows-AMIs enthalten eine Reihe von Treibern, die den Zugriff auf virtualisierte Hardware ermöglichen. Diese Treiber werden von Amazon EC2 verwendet, um Instance-Speicher und Amazon EBS-Volumes den jeweiligen Geräte zuzuordnen. Wir empfehlen, die aktuellen Treiber zu installieren, um die Stabilität und Leistung Ihrer EC2 Instances unter Windows zu verbessern.

Installationsoptionen

- Verwenden Sie AWS Systems Manager, um die PV-Treiber automatisch zu aktualisieren. Weitere Informationen finden Sie unter Schrittweise Anleitung: Automatische Aktualisierung von PV-Treibern in EC2-Windows-Instances im Benutzerhandbuch für AWS Systems Manager.
- Download des Treiberpakets und manuelles Ausführen des Installationsprogramms. Achten Sie darauf, die `readme.txt`-Datei auf Systemanforderungen zu überprüfen. Informationen zum Herunterladen und Installieren der AWS PV-Treiber oder zum Aktualisieren eines Domänen-Controllers finden Sie unter Manuelles Upgrade für Windows-Server-Instances (AWS-PV-Upgrade).

AWS PV-Treiber – Paketverlauf

In der folgende Tabelle sind die Änderungen an den AWS PV-Treibern für die einzelnen Treiberversionen aufgeführt.

Paketversion	Details	Datum der Veröffentlichung
8.6.0	• Stabilitätskorrekturen für XenStore-Interaktionen.	27. Mai 2025
8.5.0	• Stabilitätsverbesserungen, um seltene Fälle von Abstürzen beim Trennen von Netzwerkgeräten zu beheben. • Stabilitätskorrekturen zur Behebung seltener Fälle von Abstürzen während der EBS-Volumenablösung • Behebung von Fehlern im Paketinstallationsprogramm. • Das PV-Installationsprogramm wurde für die Verwendung von `Pnputil` aktualisiert.	31. Oktober 2024

Paketversion	Details	Datum der Veröffentlichung
8.4.3	Behebung von Fehlern im Paketinstallationsprogramm zur Verbesserung der Upgrade-Erfahrung. Dies ist die letzte Version, die auf Windows Server 2012 und 2012 R2 ausgeführt werden kann. Diese Version steht zum Download zur Verfügung, wird jedoch nicht mehr unterstützt, da Windows Server 2012 und 2012 R2 das Ende der Unterstützung erreicht haben.	24. Januar 2023
8.4.2	Stabilitätsbehebungen für Race-Bedingung.	13. April 2022
8.4.1	Verbessertes Paketinstallationsprogramm.	07. Januar 2022
8.4.0	• Stabilitätskorrekturen zur Behebung seltener Fälle von hängengebliebenen Festplatten-I/O. • Stabilitätskorrekturen zur Behebung seltener Fälle von Abstürzen während der EBS-Volumenablösung • Es wurde ein Feature hinzugefügt, um die Last auf mehrere Kerne für Workloads zu verteilen, die mehr als 20 000 IOPS verursachen und einen Leistungsabfall aufgrund von Engpässen erfahren. Informationen zum Aktivieren dieses Features finden Sie unter Workloads, die mehr als 20 000 Festplatten-IOPS nutzen, führen zu einem Leistungsabfall aufgrund von CPU-Engpässen.	2. März 2021
8.3.5	Verbessertes Paketinstallationsprogramm. Dies ist die letzte Version, die auf Windows Server 2008 R2 ausgeführt werden kann. Diese Version steht zum Download zur Verfügung, wird aber nicht mehr unterstützt. Windows Server 2008 R2 hat das Ende seiner Lebensdauer erreicht und wird von Microsoft nicht mehr unterstützt.	07. Januar 2022
8.3.4	Verbesserte Zuverlässigkeit der Netzwerkgeräteanbindung.	4. August 2020

Paketversion	Details	Datum der Veröffentlichung
8.3.3	• Aktualisieren Sie auf die XenStore-bezogene Komponente, um die Fehlerprüfung während der Fehlerbehandlungspfade zu verhindern. • Aktualisieren Sie die Speicherkomponente, um Abstürze zu vermeiden, wenn ein ungültiger SRB gesendet wird. Um diesen Treiber auf Windows Server 2008 R2-Instances zu aktualisieren, müssen Sie zunächst überprüfen, ob die entsprechenden Patches installiert sind, um der folgende Microsoft-Sicherheitsempfehlung nachzukommen: Microsoft Security Advisory 3033929.	4. Februar 2020
8.3.2	Verbesserte Zuverlässigkeit der Netzwerkkomponenten.	30. Juli 2019
8.3.1	Verbesserte Performance und Robustheit der Speicherkomponente.	12. Juni 2019
8.2.7	Verbesserte Effizienz bei der Migration auf Instance-Typen der neuesten Generation.	20. Mai 2019
8.2.6	Verbesserte Effizienz beim Absturzabbildpfad.	15. Januar 2019
8.2.5	Zusätzliche Verbesserungen bei der Sicherheit. Das PowerShell-Installationsprogramm ist jetzt im Paket enthalten.	12. Dezember 2018
8.2.4	Verbesserung der Zuverlässigkeit.	2. Oktober 2018

Paketversion	Details	Datum der Veröffentlichung
8.2.3	Fehlerbehebungen und Leistungsverbesserungen. EBS-Volume-ID als Datenträger-Seriennummer für EBS-Volumen melden. Dies ermöglicht Cluster-Szenarien wie S2D.	29. Mai 2018
8.2.1	Verbesserung der Netzwerk- und Speicherleistung sowie mehrere Stabilitätskorrekturen. Eine Information dazu, ob diese Version installiert wurde, erhalten Sie über den folgenden Windows-Registrierungswert: `HKLM\Software\Amazon\PVDriver\Version 8.2.1` .	8. März 2018
7.4.3	Unterstützung für Windows Server 2016 hinzugefügt Fehlerbehebungen zur Erhöhung der Stabilität für alle unterstützten Windows-Versionen *AWSDie Signatur der PV-Treiber Version 7.4.3 läuft am 29. März 2019 ab. Wir empfehlen die Aktualisierung auf den neuesten AWS PV-Treiber.	18. Nov. 2016
7.4.2	Fehlerbehebungen zur Erhöhung der Stabilität für den Instance-Typ X1	2. Aug. 2016
7.4.1	• Verbesserung der Leistung des AWS PV Storage-Treibers • Fehlerbehebungen zur Erhöhung der Stabilität des AWS PV-Speichertreibers: Behebung eines Problems, der zu einem Systemabsturz mit dem Fehlercode 0x0000DEAD führt. • Fehlerbehebungen zur Erhöhung der Stabilität des AWS PV-Netzwerktreibers • Unterstützung für Windows Server 2008 R2 hinzugefügt	12. Juli 2016

Paketversion	Details	Datum der Veröffentlichung
7.3.2	• Verbesserte Protokollierung und Diagnose • Fehlerbehebung zur Erhöhung der Stabilität des AWS PV-Speichertreibers. In manchen Fällen werden Datenträger unter Windows nicht angezeigt, nachdem sie der Instance erneut zugeordnet wurden. • Unterstützung für Windows Server 2012 hinzugefügt	24. Juni 2015
7.3.1	TRIM-Aktualisierung: Fehlerbehebung für TRIM-Anfragen. Dieser Patch erhöht die Stabilität und Leistung von Instances bei der Verwaltung einer großen Anzahl von TRIM-Anfragen.	
7.3.0	TRIM-Unterstützung: Der AWS PV-Treiber ist nun in der Lage, TRIM-Anfragen an den Hypervisor zu senden. Flüchtige Datenträger verarbeiten TRIM-Anfragen korrekt, wenn der zugrundeliegende Speicher TRIM (SSD) unterstützt. Beachten Sie, dass EBS-basierter Speicher TRIM nicht unterstützt (Stand März 2015).	
7.2.5	• Fehlerbehebung zur Erhöhung der Stabilität des AWS PV-Speichertreibers: In manchen Fällen dereferenziert der AWS PV-Treiber ungültigen Speicher und verursacht einen Systemausfall. • Fehlerbehebung zur Erhöhung der Stabilität bei der Generierung eines Speicherauszugs (crash dump): In manchen Fällen bleibt der AWS PV-Treiber bei einem kritischen Wettlauf (race condition) hängen, wenn ein Speicherauszug geschrieben wird. Vor dieser Version konnte das Problem nur dadurch gelöst werden, dass der Treiber beendet und erneut gestartet wurde, wodurch der Speicherauszug verloren ging.	

Paketversion	Details	Datum der Veröffentlichung
7.2.4	Persistenz der Geräte-ID: Dieser Patch maskiert die PCI-Geräte-ID der Plattform und erzwingt die Anzeige derselben Geräte-ID im System, auch wenn die Instance verschoben wird. Allgemeiner formuliert wirkt sich der Patch darauf aus, wie der Hypervisor virtuelle Geräte anzeigt. Außerdem enthält der Patch Änderungen an dem Co-Installationsprogramm für den AWS PV-Treiber, sodass zugewiesene virtuelle Geräte im System erhalten bleiben.	
7.2.2	• Laden der AWS PV-Treiber im DSRM-Modus (Directory Services Restore Mode): Der DSRM-Modus ist eine Boot-Option für den abgesicherten Modus für Windows Server-Domain-Controller. • Persistenz der Geräte-ID, wenn ein virtueller Netzwerkadapter neu zugewiesen wird: Dieser Patch erzwingt eine Prüfung der Zuordnung von MAC-Adressen im System, sodass die Geräte-ID erhalten bleibt. Durch diesen Patch wird sichergestellt, dass die Adapter ihre statischen Einstellungen beibehalten, wenn Sie neu zugewiesen werden.	
7.2.1	• Ausführung im abgesicherten Modus: Behebung eines Problems, bei dem der Treiber im abgesicherten Modus nicht geladen wird. Vor dieser Version wurden AWS-PV-Treiber nur in normal ausgeführten Systemen instanziiert. • Hinzufügen von Datenträgern zu Microsoft Windows-Speicherpools: Vor dieser Version wurden Abfragen für Speicherseite 83 synthetisiert. Der Patch entfernt die Unterstützung für Speicherseite 83. Beachten Sie, dass dies keine Auswirkungen auf Speicherpools hat, die in einer Cluster-Umgebung verwendet werden, da PV-Datenträger keine gültigen Cluster-Datenträger sind.	
7.2.0	Basis: Die AWS PV-Basisversion.	

Citrix-PV-Treiber

Die Citrix PV-Treiber werden im Verzeichnis `%ProgramFiles%\Citrix\XenTools` (32-Bit-Instances) oder `%ProgramFiles(x86)%\Citrix\XenTools` (64-Bit-Instances) gespeichert.

Die Citrix PV-Treiberkomponenten werden in der Windows-Registry unter aufgeliste `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services`. Diese Treiberkomponenten umfassen im Einzelnen: xenevtchn, xeniface, xennet, Xennet6, xensvc, xenvbd und xenvif.

Citrix beinhaltet eine weitere Treiberkomponente mit dem Namen XenGuestAgent, die als Windows-Service ausgeführt wird. Sie übernimmt Aufgaben wie das Beenden und erneute Starten von Ereignissen über die API. Sie können auf Services zugreifen und diese verwalten, indem Sie `Services.msc` in der Befehlszeile ausführen.

Wenn bei der Verarbeitung bestimmter Workloads Netzwerkfehler auftreten, müssen Sie möglicherweise das TCP-Offloading-Feature für den Citrix PV-Treiber deaktivieren. Weitere Informationen finden Sie unter TCP-Offloading.

PV-Treiber von Red Hat

Red-Hat-Treiber werden für ältere Instances unterstützt, werden aber für neuere Instances mit mehr als 12 GB RAM aufgrund ihrer Einschränkungen nicht empfohlen. Instances mit mehr als 12 GB RAM, auf denen Red-Hat-Treiber ausgeführt werden, lassen sich unter Umständen nicht mehr hochfahren, sodass kein Zugriff mehr möglich ist. Wir empfehlen ein Upgrade von Red-Hat-Treibern auf Citrix-PV-Treiber und anschließend ein Upgrade von Citrix-PV-Treibern auf AWS-PV-Treiber.

Die Quelldateien für Red-Hat-Treiber werden im Verzeichnis `%ProgramFiles%\RedHat` (32-Bit-Instances) oder `%ProgramFiles(x86)%\RedHat` (64-Bit-Instances) gespeichert. Die beiden Treiber sind `rhelnet`, der Red Hat Paravirtualized Network Driver und `rhelscsi`, der Red Hat SCSI Miniport Driver.

Abonnieren von -Benachrichtigungen

Amazon SNS kann Sie benachrichtigen, wenn neue Versionen von EC2-Windows-Treibern veröffentlicht werden. Sie können diese Benachrichtigungen abonnieren.

> **Note**
>
> Sie müssen die Region angeben, in der das SNS-Thema erstellt wurde.

Jedes Mal wenn neue EC2-Treiber für Windows veröffentlicht werden, senden wir ein Benachrichtigung an die Abonnenten. Wenn Sie diese Benachrichtigungen nicht mehr erhalten möchten, können Sie sich abmelden. Weitere Informationen finden Sie unter SNS-Thema und Abonnement löschen.

Console

So abonnieren Sie -Benachrichtigungen

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Ändern Sie, falls erforderlich, die Region in der Navigationsleiste zu US East (N. Virginia). Sie müssen diese Region auswählen, weil sich die SNS-Benachrichtigungen, die Sie abonnieren, in dieser Region befinden.
3. Wählen Sie im Navigationsbereich Subscriptions aus.
4. Wählen Sie Create subscription.
5. Führen Sie im Dialogfeld Create subscription Folgendes aus:
   a. Kopieren Sie den folgenden Amazon-Ressourcennamen (ARN) unter TopicARN:

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers
   b. Wählen Sie unter Protocol die Option `Email` aus.
   c. Geben Sie unter Endpoint eine E-Mail-Adresse ein, um die Benachrichtigungen zu empfangen.
   d. Wählen Sie Create subscription (Abonnement erstellen) aus.
6. Sie erhalten eine Bestätigungs-E-Mail. Öffnen Sie die E-Mail und befolgen Sie die Anweisungen, um Ihr Abonnement abzuschließen.

AWS CLI

So abonnieren Sie -Benachrichtigungen

Verwenden Sie den folgenden Befehl.

```
aws sns subscribe \
    --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers \
    --region us-east-1 \
    --protocol email \
    --notification-endpoint YourUserName@YourDomainName.ext
```

PowerShell

So abonnieren Sie -Benachrichtigungen

Verwenden Sie den folgenden Befehl.

```
Connect-SNSNotification `
    -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers' `
    -Region us-east-1 `
    -Protocol email `
    -Endpoint "YourUserName@YourDomainName.ext"
```

Upgrade von PV-Treibern auf EC2-Windows-Instances

Wir empfehlen, die aktuellen PV-Treiber zu installieren, um die Stabilität und Leistung Ihrer EC2-Instances unter Windows zu verbessern. Die Anweisungen auf dieser Seite helfen Ihnen, das Treiberpaket herunterzuladen und das Installationsprogramm manuell ausführen.

Überprüfen, welchen Treiber Ihre Windows-Instance verwendet

Öffnen Sie den Geräte-Manager und zeigen Sie Netzwerkadapter an. Prüfen Sie, ob der PV-Treiber einer der Folgenden ist:

- AWS PV Network Device
- Citrix PV Ethernet Adapter
- Red Hat PV NIC Driver

Systemanforderungen

Überprüfen Sie unbedingt die `readme.txt`-Datei im Download auf Systemanforderungen.

Inhalt

- Upgrade für Windows-Server-Instances (AWS-PV-Upgrade) mit Distributor
- Manuelles Upgrade für Windows-Server-Instances (AWS-PV-Upgrade)
- Upgrade für einen Domain-Controller (AWS PV-Upgrade)
- Upgrade für Instances unter Windows Server 2008 und 2008 R2 (Upgrade von Red Hat auf Citrix PV)

- Upgrade des Citrix-Xen-Guest-Agent-Service

Upgrade für Windows-Server-Instances (AWS-PV-Upgrade) mit Distributor

Sie können Distributor, eine Fähigkeit von AWS Systems Manager, verwenden, um das AWS-PV-Treiberpaket zu installieren oder zu aktualisieren. Die Installation oder das Upgrade kann einmal durchgeführt werden, oder Sie können sie nach einem Zeitplan installieren oder aktualisieren. Die `In-place update`-Option für den Installationstyp wird für dieses Distributor-Paket nicht unterstützt.

> **Important**
>
> Wenn Ihre Instance ein Domain-Controller ist, finden Sie weitere Informationen unter Upgrade für einen Domain-Controller (AWS PV-Upgrade). Das Upgrade-Verfahren für Domain-Controller-Instances unterscheidet sich von dem für die Standard Editions von Windows.

1. Wir empfehlen Ihnen, ein Backup zu erstellen, falls Sie Ihre Änderungen rückgängig machen müssen.

   > **Tip**
   >
   > Anstatt das AMI von der Amazon-EC2-Konsole aus zu erstellen, können Sie Systems Manager Automation verwenden, um das AMI mit dem `AWS-CreateImage`-Runbook zu erstellen. Weitere Informationen finden Sie unter AWS-CreateImage im Benutzerhandbuch zur AWS Systems Manager-Automatisierungs-Runbook-Referenz.

   a. Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Stellen Sie vor dem Anhalten einer Instance sicher, dass Sie alle benötigten Daten aus den Instance-Speicher-Volumes in den persistenten Speicher kopiert haben, z. B. Amazon EBS oder Amazon S3.
   b. Wählen Sie im Navigationsbereich Instances aus.
   c. Wählen Sie die Instance, die ein Treiberupgrade benötigt und wählen Sie Instance state (Instance-Zustand), Stop instance (Instance stoppen) aus.
   d. Nachdem die Instance angehalten wurde, wählen Sie die Instance aus, wählen Sie Actions (Aktionen), Image and Templates (Image und Vorlagen) und dann Create image (Image erstellen) aus.

e. Wählen Sie Instance state (Instance-Status), Start instance (Instance starten).

2. Verbindung mit der Instance über Remote Desktop. Weitere Informationen finden Sie unter the section called “Verbindung mit einem RDP-Client herstellen”.
3. Wir empfehlen, dass Sie alle Nicht-System-Laufwerke offline nehmen und alle Laufwerksbuchstabenzuordnungen zu den sekundären Laufwerken in der Laufwerksverwaltung notieren, bevor Sie dieses Upgrade durchführen. Wenn Sie eine direkte Aktualisierung der AWS PV-Treiber durchführen, ist dieser Schritt nicht erforderlich. Wir empfehlen außerdem, die Start-Option für alle nicht erforderlichen Services in der Services-Konsole auf Manual zu setzen.
4. Anweisungen zum Installieren des AWS-PV-Treiberpakets mit Distributor finden Sie in den Verfahren unter Installieren oder Aktualisieren von Paketen im Benutzerhandbuch für AWS Systems Manager.
5. Wählen Sie bei Name AWSPVDriver aus.
6. Wählen Sie für Installationstyp Deinstallieren und neu installieren aus.
7. Konfigurieren Sie die anderen Parameter für das Paket nach Bedarf und führen Sie die Installation oder das Upgrade mit dem unter referenzierten Verfahren in Step 4 aus.

   Wenn Sie das Distributor-Paket ausgeführt haben, wird die Instance automatisch neu gestartet und das Upgrade des Treibers durchgeführt. Die Instance ist für die Dauer von bis zu 15 Minuten nicht verfügbar.
8. Wenn das Upgrade abgeschlossen wurde und die Instance beide Zustandsprüfungen in der Amazon-EC2-Konsole bestanden hat, stellen Sie über Remote Desktop eine Verbindung mit der Instance her und prüfen so, dass der neue Treiber installiert wurde.
9. Nachdem Sie die Verbindung hergestellt haben, führen Sie den folgenden PowerShell-Befehl aus:

   ```
   Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
   ```
10. Vergewissern Sie sich, dass die Treiberversion identisch mit der aktuellen Version in der Tabelle für den Treiber-Versionsverlauf ist. Weitere Informationen finden Sie unter AWS PV-Treiber – Paketverlauf Open Disk Management, um alle sekundären Offline-Volumes zu überprüfen und online zu bringen, die den in Step 3 angegebenen Laufwerksbuchstaben entsprechen.

Wenn Sie das TCP-Offloading über Netsh für Citrix PV-Treiber deaktiviert haben, empfehlen wir, dieses Feature nach dem Upgrade auf die AWS PV-Treiber wieder zu aktivieren. Die von Citrix-

Treibern beim TCP-Offloading verursachten Probleme treten mit AWS PV-Treibern nicht auf. Durch TCP-Offloading wird deshalb mit AWS PV-Treibern eine bessere Leistung erzielt.

Wenn Sie zuvor eine statische IP-Adresse oder DNS-Konfiguration auf die Netzwerkschnittstelle angewendet haben, müssen Sie möglicherweise die statische IP-Adresse oder DNS-Konfiguration nach dem Upgrade von AWS-PV-Treibern erneut anwenden.

Manuelles Upgrade für Windows-Server-Instances (AWS-PV-Upgrade)

Verwenden Sie das folgende Verfahren, um ein In-Place-Upgrade von AWS-PV-Treibern oder ein Upgrade von Citrix PV-Treibern auf AWS-PV-Treiber unter Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 oder Windows Server 2022 durchzuführen. Dieses Upgrade ist für Red-Hat-Treiber oder für andere Versionen von Windows Server nicht verfügbar.

Einige ältere Versionen von Windows Server können die neuesten Treiber nicht verwenden. Um zu überprüfen, welche Treiberversion für Ihr Betriebssystem verwendet werden soll, lesen Sie die Tabelle mit den Treiberversionen auf der Seite Paravirtual-Treiber für Windows-Instances an.

> **Important**
>
> Wenn Ihre Instance ein Domain-Controller ist, finden Sie weitere Informationen unter Upgrade für einen Domain-Controller (AWS PV-Upgrade). Das Upgrade-Verfahren für Domain-Controller-Instances unterscheidet sich von dem für die Standard Editions von Windows.

So aktualisieren Sie AWS-PV-Treiber manuell

1. Wir empfehlen Ihnen, ein Backup zu erstellen, falls Sie Ihre Änderungen rückgängig machen müssen.

   > **Tip**
   >
   > Anstatt das AMI von der Amazon-EC2-Konsole aus zu erstellen, können Sie Systems Manager Automation verwenden, um das AMI mit dem `AWS-CreateImage`-Runbook zu erstellen. Weitere Informationen finden Sie unter AWS-CreateImage im Benutzerhandbuch zur AWS Systems Manager-Automatisierungs-Runbook-Referenz.

a. Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Stellen Sie vor dem Anhalten einer Instance sicher, dass Sie alle benötigten Daten aus den Instance-Speicher-Volumes in den persistenten Speicher kopiert haben, z. B. Amazon EBS oder Amazon S3.

b. Wählen Sie im Navigationsbereich Instances aus.

c. Wählen Sie die Instance, die ein Treiberupgrade benötigt und wählen Sie Instance state (Instance-Zustand), Stop instance (Instance stoppen) aus.

d. Nachdem die Instance angehalten wurde, wählen Sie die Instance aus, wählen Sie Actions (Aktionen), Image and Templates (Image und Vorlagen) und dann Create image (Image erstellen) aus.

e. Wählen Sie Instance state (Instance-Status), Start instance (Instance starten).

2. Verbindung mit der Instance über Remote Desktop.

3. Wir empfehlen, dass Sie alle Nicht-System-Laufwerke offline nehmen und alle Laufwerksbuchstabenzuordnungen zu den sekundären Laufwerken in der Laufwerksverwaltung notieren, bevor Sie dieses Upgrade durchführen. Wenn Sie eine direkte Aktualisierung der AWS PV-Treiber durchführen, ist dieser Schritt nicht erforderlich. Wir empfehlen außerdem, die Start-Option für alle nicht erforderlichen Services in der Services-Konsole auf Manual zu setzen.

4. Laden Sie die Treiber mit einer der folgenden Optionen auf Ihre Instance herunter:

   - Browser – Download des neuesten Treiberpakets auf die Instance und Extrahieren des ZIP-Archivs.
   - PowerShell – Führen Sie die folgenden Befehle aus:

     ```
     Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/
     Latest/AWSPVDriver.zip -outfile $env:USERPROFILE\pv_driver.zip
     Expand-Archive $env:userprofile\pv_driver.zip -DestinationPath $env:userprofile
     \pv_drivers
     ```

     Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 oder früher verwenden, muss TLS 1.2 möglicherweise für Ihr PowerShell-Terminal aktiviert werden. Sie können TLS 1.2 für die aktuelle PowerShell-Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:

     ```
     [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
     ```

5. Führen Sie Folgendes aus: `AWSPVDriverSetup.msi`.

Wenn Sie die MSI-Datei ausgeführt haben, wird die Instance automatisch neu gestartet und das Upgrade des Treibers durchgeführt. Die Instance ist für die Dauer von bis zu 15 Minuten nicht verfügbar. Wenn das Upgrade abgeschlossen wurde und die Instance beide Zustandsprüfungen in der Amazon EC2-Konsole bestanden hat, können Sie sich vergewissern, dass der neue Treiber installiert wurde, indem Sie über Remote Desktop eine Verbindung zur Instance herstellen und anschließend folgenden PowerShell-Befehl ausführen:

```
Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
```

Vergewissern Sie sich, dass die Treiberversion identisch mit der aktuellen Version in der Tabelle für den Treiber-Versionsverlauf ist. Weitere Informationen finden Sie unter AWS PV-Treiber – Paketverlauf Open Disk Management, um alle sekundären Offline-Volumes zu überprüfen und online zu bringen, die den in Step 3 angegebenen Laufwerksbuchstaben entsprechen.

Wenn Sie das TCP-Offloading über Netsh für Citrix PV-Treiber deaktiviert haben, empfehlen wir, dieses Feature nach dem Upgrade auf die AWS PV-Treiber wieder zu aktivieren. Die von Citrix-Treibern beim TCP-Offloading verursachten Probleme treten mit AWS PV-Treibern nicht auf. Durch TCP-Offloading wird deshalb mit AWS PV-Treibern eine bessere Leistung erzielt.

Wenn Sie zuvor eine statische IP-Adresse oder DNS-Konfiguration auf die Netzwerkschnittstelle angewendet haben, müssen Sie möglicherweise die statische IP-Adresse oder DNS-Konfiguration nach dem Upgrade von AWS-PV-Treibern erneut anwenden.

Upgrade für einen Domain-Controller (AWS PV-Upgrade)

Führen Sie die folgenden Schritte aus, um auf einem Domain-Controller entweder ein direktes Upgrade der AWS PV-Treiber oder ein Upgrade von Citrix PV-Treibern auf AWS PV-Treiber durchzuführen. Um sicherzustellen, dass Ihre FSMO-Rollen während des Upgrades betriebsbereit bleiben, empfehlen wir Ihnen, diese Rollen vor Beginn des Upgrades auf andere Domain-Controller zu übertragen. Weitere Informationen finden Sie auf der Microsoft Learn-Website unter So können Sie FSMO-Rollen anzeigen und übertragen.

So führen Sie ein Upgrade für einen Domain-Controller durch

1. Wir empfehlen Ihnen, ein Backup für Ihren Domain-Controller zu erstellen, falls Sie Ihre Änderungen rückgängig machen müssen. Die Verwendung eines AMI als Backup wird

nicht unterstützt. Weitere Informationen finden Sie in der Microsoft-Dokumentation unter Überlegungen zu Backup und Wiederherstellung.

2. Führen Sie den folgenden Befehl aus, um Windows so zu konfigurieren, dass nach einem Neustart in den DSRM-Modus (Directory Services Restore Mode) gebootet wird.

> **Warning**
>
> Stellen Sie sicher, dass Sie das DSRM-Passwort kennen, bevor Sie diesen Befehl ausführen. Sie benötigen diese Informationen, um sich bei Ihrer Instance anmelden zu können, wenn das Upgrade durchgeführt wurde und die Instance automatisch neu gestartet wird.

```
bcdedit /set {default} safeboot dsrepair
```

PowerShell:

```
PS C:\> bcdedit /set "{default}" safeboot dsrepair
```

Das System muss im DSRM-Modus gestartet werden, da das Upgrade-Dienstprogramm die Citrix PV-Speichertreiber entfernt, um die AWS PV-Treiber installieren zu können. Daher empfehlen wir, in der Datenträgerverwaltung alle Laufwerksbuchstaben und Ordnerzuordnungen auf die sekundären Laufwerke zu beachten. Wenn keine Citrix-PV-Speichertreiber vorhanden sind, werden sekundäre Laufwerke nicht erkannt. Domain-Controller, die NTDS-Ordner auf sekundären Laufwerken verwenden, können nicht gebootet werden, da der sekundäre Datenträger nicht erkannt wird.

> **Warning**
>
> Wenn Sie diesen Befehl ausgeführt haben, führen Sie keinen manuellen Neustart des Systems durch. Das System wird nicht gebootet, da die Citrix PV-Treiber DSRM nicht unterstützen.

3. Führen Sie den folgenden Befehl aus, um der Registrierung den Eintrag **`DisableDCCheck`** hinzuzufügenden:

```
reg add HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck /t
 REG_SZ /d true
```

4. Download des neuesten Treiberpakets auf die Instance und Extrahieren des ZIP-Archivs.
5. Führen Sie Folgendes aus: `AWSPVDriverSetup.msi`.

   Wenn Sie die MSI-Datei ausgeführt haben, wird die Instance automatisch neu gestartet und das Upgrade des Treibers durchgeführt. Die Instance ist für die Dauer von bis zu 15 Minuten nicht verfügbar.
6. Wenn das Upgrade abgeschlossen wurde und die Instance beide Zustandsprüfungen in der Amazon EC2-Konsole bestanden hat, stellen Sie über Remote Desktop eine Verbindung mit der Instance her. Öffnen Sie die Datenträgerverwaltung, um alle sekundären Offline-Volumes zu überprüfen und online zu bringen, die den zuvor beschriebenen Laufwerksbuchstaben und Ordnerzuordnungen entsprechen.

   Sie müssen eine Verbindung mit der Instance herstellen, indem Sie den Benutzernamen im folgenden Format angeben hostname\administrator. Beispiel: Win2k12TestBox\administrator.
7. Führen Sie den folgenden Befehl aus, um die DSRM-Bootkonfiguration zu entfernen:

   ```
   bcdedit /deletevalue safeboot
   ```
8. Starten Sie die Instance neu.
9. Vergewissern Sie sich am Ende des Upgrades-Verfahrens, dass der neue Treiber installiert wurde. Suchen Sie im Geräte-Manager unter Storage Controllers den AWS PV Storage Host Adapter. Vergewissern Sie sich, dass die Treiberversion identisch mit der aktuellen Version in der Tabelle für den Treiber-Versionsverlauf ist. Weitere Informationen finden Sie unter AWS PV-Treiber – Paketverlauf.
10. Führen Sie den folgenden Befehl aus, um den Eintrag **`DisableDCCheck`** aus der Registrierung zu löschen:

    ```
    reg delete HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck
    ```

> **Note**
>
> Wenn Sie das TCP-Offloading über Netsh für Citrix PV-Treiber deaktiviert haben, empfehlen wir, dieses Feature nach dem Upgrade auf die AWS PV-Treiber wieder zu aktivieren. Die

von Citrix-Treibern beim TCP-Offloading verursachten Probleme treten mit AWS PV-Treibern nicht auf. Durch TCP-Offloading wird deshalb mit AWS PV-Treibern eine bessere Leistung erzielt.

Upgrade für Instances unter Windows Server 2008 und 2008 R2 (Upgrade von Red Hat auf Citrix PV)

Bevor Sie mit dem Upgrade Ihrer Red-Hat-Treiber auf Citrix-PV-Treiber beginnen können, müssen Sie die folgenden Schritte ausführen:

- Installieren Sie die aktuelle Version des EC2Config-Service. Weitere Informationen finden Sie unter Installieren der neuesten Version von EC2Config.
- Stelle Sie sicher, dass Sie Windows PowerShell 3.0 installiert haben. Sie prüfen die installierte Version, indem Sie den folgenden Befehl in einem PowerShell-Fenster ausführen:

  ```
  PS C:\> $PSVersionTable.PSVersion
  ```

  Windows PowerShell 3.0 ist im Installationspaket für Windows Management Framework (WMF) Version 3.0 enthalten. Wenn Sie Windows PowerShell 3.0 installieren müssen, lesen Sie Windows Management Framework 3.0 im Microsoft Download Center.
- Erstellen Sie ein Backup Ihrer wichtigen Daten in der Instance oder erstellen Sie ein AMI aus der Instance. Weitere Informationen zum Erstellen eines AMI finden Sie unter Ein Amazon-EBS-gestütztes AMI erstellen.

  > **Tip**
  >
  > Anstatt das AMI von der Amazon-EC2-Konsole aus zu erstellen, können Sie Systems Manager Automation verwenden, um das AMI mit dem `AWS-CreateImage`-Runbook zu erstellen. Weitere Informationen finden Sie unter AWS-CreateImage im Benutzerhandbuch zur AWS Systems Manager-Automatisierungs-Runbook-Referenz.

  Wenn Sie ein AMI erstellen, sollten Sie unbedingt wie folgt vorgehen:
  - Notieren Sie sich Ihr Passwort.
  - Führen Sie das Sysprep-Tool nicht manuell oder mithilfe des EC2Config-Service aus.
  - Stellen Sie Ihren Ethernet-Adapter so ein, dass ihm automatisch eine IP-Adresse über DHCP zugewiesen wird.

So führen Sie ein Upgrade der Red-Hat-Treiber durch

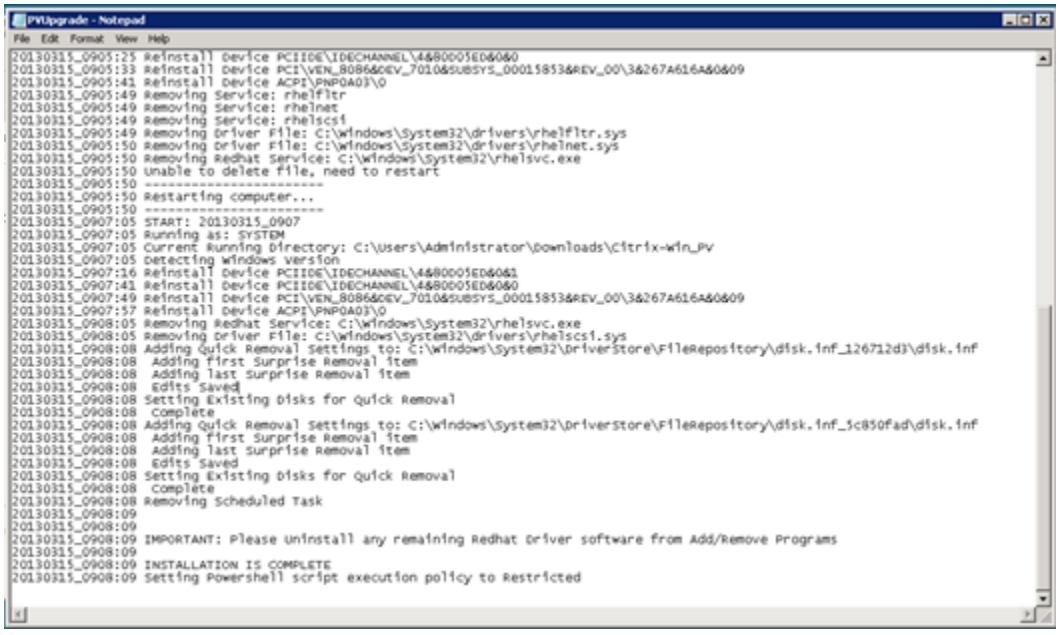
1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an. Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von RDP.
2. Laden Sie das Citrix PV-Upgrade-Paket in die Instance herunter.
3. Extrahieren Sie die Inhalte des Upgrade-Pakets an einem Speicherort Ihrer Wahl.
4. Doppelklicken Sie auf die Datei Upgrade.bat. Wenn eine Sicherheitswarnung angezeigt wird, wählen Sie Ausführen.
5. Prüfen Sie die Informationen im Dialogfeld Upgrade Drivers (Treiber upgraden) und klicken Sie auf Yes (Ja), wenn Sie bereit sind, das Upgrade zu starten.
6. Wählen Sie im Dialogfeld Deinstallationsprogramm für Red Hat Paravirtualized Xen Drivers für Windows die Option Ja, um die Red-Hat-Software zu entfernen. Ihre Instance wird neu gestartet.

> **Note**
>
> Wenn das Dialogfeld für das Deinstallationsprogramm nicht angezeigt wird, klicken Sie in der Windows-Taskleiste auf Red Hat Paravirtualize.

7. Prüfen Sie, ob die Instance neu gestartet wurde und einsatzbereit ist.
   a. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
   b. Wählen Sie auf der Seite Instances die Option Actions (Aktionen), dann Monitor and troubleshoot (Überwachung und Fehlerbehebung) aus und wählen Sie dann Get system log (Systemprotokoll abrufen) aus.
   c. Der Server sollte während des Upgrade-Vorgangs 3 oder 4 mal neu gestartet worden sein. Sie können das in der Protokolldatei daran erkennen, wie oft `Windows is Ready to use` angezeigt wird.

```
    Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
 Ec2Config service v2.1.9.0
  RedHat PV NIC Driver v1.3.10.0
2013/03/15 17:11:01Z: Waiting for meta-data accessibility...
2013/03/15 17:11:02Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BFD64F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
<Username>Administrator</Username>
<Password>
L79ThJPF8LyIL38IZht0FBrjet3vnT2csTiU/XGVMRCH7kQtBnznAnXrKd1sirXlxl9BwVMsd9b38jFJqv0lIUpgNNJRZoCDc7IbUw
</Password>
2013/03/15 17:11:30Z: Product activation was successful.
2013/03/15 17:11:32Z: Message: Windows is Ready to use
Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
 Ec2Config service v2.1.9.0
2013/03/15 21:04:24Z: There was an exception writing driver information to console: System.Exception:
   at Ec2Config.Service1.Go()
2013/03/15 21:04:35Z: Waiting for meta-data accessibility...
2013/03/15 21:04:40Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BFD64F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
2013/03/15 21:05:08Z: Product activation was successful.
2013/03/15 21:05:09Z: Message: Windows is Ready to use
Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
 Ec2Config service v2.1.9.0
  Citrix PV Ethernet Adapter v5.9.960.49119
2013/03/15 21:07:20Z: Waiting for meta-data accessibility...
2013/03/15 21:07:21Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BFD64F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
2013/03/15 21:07:27Z: Message: Windows is Ready to use
```

8. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
9. Schließen Sie das Dialogfeld Red Hat Paravirtualized Xen Drivers for Windows uninstaller.
10. Vergewissern Sie sich, dass die Installation abgeschlossen wurde. Navigieren Sie zu dem Ordner `Citrix-WIN_PV`, den Sie extrahiert haben, öffnen Sie die Datei `PVUpgrade.log` und suchen Sie nach dem Text `INSTALLATION IS COMPLETE`.



Upgrade des Citrix-Xen-Guest-Agent-Service

Wenn Sie Citrix PV-Treiber unter Windows-Server verwenden, können Sie ein Upgrade des Citrix Xen Guest Agent-Service durchführen. Dieser Windows-Service übernimmt Aufgaben wie das Beenden und erneute Starten von Ereignissen über die API. Sie können dieses Upgrade-Paket unter jeder Version von Windows Server ausführen, wenn in der Instance die Citrix PV-Treiber ausgeführt werden.

> **Important**
>
> Für Windows Server 2008 R2 und höher empfehlen wir die Aktualisierung auf AWS PV-Treiber mit der Guest Agent-Aktualisierung.

Erstellen Sie unbedingt ein Backup Ihrer wichtigen Daten in der Instance oder erstellen Sie ein AMI aus der Instance, bevor Sie mit dem Upgrade der Treiber beginnen. Weitere Informationen zum Erstellen eines AMI finden Sie unter Ein Amazon-EBS-gestütztes AMI erstellen.

> **Tip**
>
> Anstatt das AMI von der Amazon-EC2-Konsole aus zu erstellen, können Sie Systems Manager Automation verwenden, um das AMI mit dem `AWS-CreateImage`-Runbook zu erstellen. Weitere Informationen finden Sie unter AWS-CreateImage im Benutzerhandbuch zur AWS Systems Manager-Automatisierungs-Runbook-Referenz.

Wenn Sie ein AMI erstellen, sollten Sie unbedingt wie folgt vorgehen:

- Aktivieren Sie das Sysprep-Tool nicht mithilfe des EC2Config-Service.
- Notieren Sie sich Ihr Passwort.
- Stellen Sie Ihren Ethernet-Adapter auf DHCP ein.

So erstellen Sie ein Upgrade des Citrix Xen Guest Agent-Service

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an. Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von RDP.

2. Laden Sie das Citrix-Upgrade-Paket in die Instance herunter.
3. Extrahieren Sie die Inhalte des Upgrade-Pakets an einem Speicherort Ihrer Wahl.
4. Doppelklicken Sie auf die Datei Upgrade.bat. Wenn eine Sicherheitswarnung angezeigt wird, wählen Sie Ausführen.
5. Prüfen Sie die Informationen im Dialogfeld Upgrade Drivers (Treiber upgraden) und klicken Sie auf Yes (Ja), wenn Sie bereit sind, das Upgrade zu starten.
6. Wenn das Upgrade abgeschlossen ist, wird die Datei `PVUpgrade.log` geöffnet; diese enthält den Text `UPGRADE IS COMPLETE`.
7. Starten Sie Ihre Instance neu.

Fehler bei PV-Treibern auf Windows-Instances beheben

Nachstehend sind Lösungen für Probleme aufgeführt, auf die Sie möglicherweise mit älteren Amazon EC2-Images und PV-Treibern stoßen.

Inhalt

- Windows Server 2012 R2 verliert die Netzwerkverbindung und Speicheranbindung nach einem Neustart der Instance
- TCP-Offloading
- Zeitsynchronisierung
- Workloads, die mehr als 20 000 Festplatten-IOPS nutzen, führen zu einem Leistungsabfall aufgrund von CPU-Engpässen

Windows Server 2012 R2 verliert die Netzwerkverbindung und Speicheranbindung nach einem Neustart der Instance

> **Important**
>
> Dieses Problem tritt nur bei AMIs auf, die vor September 2014 zur Verfügung gestellt wurden.

Amazon Machine Images (AMIs) für Windows Server 2012 R2, die vor dem 10. September 2014 verfügbar gemacht wurden, können die Netzwerkverbindung und Speicheranbindung nach einem Neustart der Instance verlieren. Die Fehlermeldung im Systemprotokoll der AWS-

Managementkonsole lautet: "Difficulty detecting PV driver details for Console Output (Probleme beim Erkennen der PV-Treiberdetails für Konsolenausgabe)". Der Verlust der Verbindung wird durch das Feature "Plug & Play Cleanup" verursacht. Dieses Feature sucht alle 30 Tage nach inaktiven Systemgeräten und deaktiviert sie. Das Feature identifiziert das EC2-Netzwerkgerät irrtümlicherweise als inaktiv und entfernt es aus dem System. Wenn dies geschieht, verliert die Instance die Netzwerkverbindung nach einem Neustart.

Wenn Sie den Verdacht haben, dass ein System von diesem Problem betroffen ist, können Sie ein direktes Treiber-Upgrade herunterladen und ausführen. Wenn Sie das direkte Treiber-Upgrade nicht durchführen können, können Sie ein Hilfsskript ausführen. Das Skript ermittelt, ob Ihre Instance betroffen ist. Wenn das zutrifft und das Amazon EC2-Netzwerkgerät noch nicht entfernt wurde, wird die "Plug & Play Cleanup"-Suche durch das Skript deaktiviert. Wenn das Netzwerkgerät entfernt wurde, wird das Gerät von dem Skript repariert und die "Plug & Play Cleanup"-Suche deaktiviert. Anschließend kann Ihre Instance neu gestartet werden und die Netzwerkverbindung bleibt erhalten.

Inhalt

- Auswahl der Probleme, die behoben werden sollen
- Methode 1 – Enhanced Networking
- Methode 2 – Konfiguration der Registrierung
- Ausführen des Korrekturskripts

Auswahl der Probleme, die behoben werden sollen

Es gibt zwei Methoden zum Wiederherstellen der Netzwerkverbindung und Speicheranbindung für eine Instance, die von diesem Problem betroffen ist. Wählen Sie eine der folgenden Methoden:

Art	Voraussetzungen	Übersicht über das Verfahren
Methode 1 – Enhanced Networking	Enhanced Networking ist nur in einer Virtual Private Cloud (VPC) verfügbar und setzt den Instance-Typ C3 voraus. Wenn der Server aktuell nicht C3 als Instance-Typ verwendet, müssen Sie diesen temporär ändern.	Sie ändern den Instance-Typ des Servers in eine C3-Instance. Danach können Sie mit Enhanced Networking eine Verbindung mit der betroffenen Instance herstellen und das Problem beheben. Wenn Sie das Problem behoben haben,

Art	Voraussetzungen	Übersicht über das Verfahren
		ändern Sie den Instance-Typ wieder in den ursprünglichen Wert. Diese Methode ist in der Regel schneller als Methode 2 und es treten wahrscheinlich weniger Benutzerfehler auf. Solange die C3-Instance ausgeführt wird, werden Ihnen zusätzlich Kosten berechnet.
Methode 2 – Konfiguration der Registrierung	Möglichkeit, einen zweiten Server zu erstellen bzw. auf einen zuzugreifen. Möglichkeit, Registrierungseinstellungen zu ändern.	Sie trennen das Root-Volume von der betroffenen Instance, ordnen es einer anderen Instance zu, stellen eine Verbindung her und nehmen Änderungen an der Registrierung vor. Solange der zusätzliche Server ausgeführt wird, werden Ihnen zusätzlich Kosten berechnet. Diese Methode ist langsamer als Methode 1, funktioniert aber auch in Situationen, in denen Methode 1 das Problem nicht lösen konnte.

Methode 1 – Enhanced Networking

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Starten Sie die betroffene Instance. Wählen Sie die Instance und wählen Sie Instance state (Instance-Status) und dann Stop instance (Instance anhalten).

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

4. Wenn die Instance angehalten wurde, erstellen Sie ein Backup. Wählen Sie die Instance und wählen Sie Actions (Aktionen), dann Image und Templates (Image und Vorlagen) und dann Create image (Image erstellen).
5. Ändern Sie den Instance-Typ in eine C3-Instance.
6. Starten Sie die Instance.
7. Stellen Sie über Remote Desktop eine Verbindung mit der Instance her und laden Sie anschließend das Upgrade-Paket für die AWS PV-Treiber in die Instance herunter.
8. Extrahieren Sie den Inhalt des Ordners und führen Sie die Datei au `AWSPVDriverSetup.msi`.

   Wenn Sie die MSI-Datei ausgeführt haben, wird die Instance automatisch neu gestartet und das Upgrade der Treiber durchgeführt. Die Instance ist für die Dauer von bis zu 15 Minuten nicht verfügbar.
9. Wenn das Upgrade abgeschlossen wurde und die Instance beide Zustandsprüfungen in der Amazon EC2-Konsole bestanden hat, stellen Sie über Remote Desktop eine Verbindung mit der Instance her und prüfen Sie, ob die neuen Treiber installiert wurden. Suchen Sie im Geräte-Manager unter Storage Controllers den AWS PV Storage Host Adapter. Vergewissern Sie sich, dass die Treiberversion identisch mit der aktuellen Version in der Tabelle für den Treiber-Versionsverlauf ist. Weitere Informationen finden Sie unter AWS PV-Treiber – Paketverlauf.
10. Halten Sie die Instance an und ändern Sie den Instance-Typ wieder in den ursprünglichen Wert.
11. Starten Sie die Instance und fahren Sie mit der normalen Verwendung fort.

Methode 2 – Konfiguration der Registrierung

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Starten Sie die betroffene Instance. Wählen Sie die Instance, wählen Sie Instance state (Instance-Status) und dann Stop instance (Instance anhalten).

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

4. Wählen Sie die Option Launch instances (Instances starten) und erstellen Sie eine temporäre Windows-Server-2008- oder Windows-Server-2012-Instance in derselben Availability Zone wie die betroffene Instance. Erstellen Sie keine Windows Server 2012 R2-Instance.

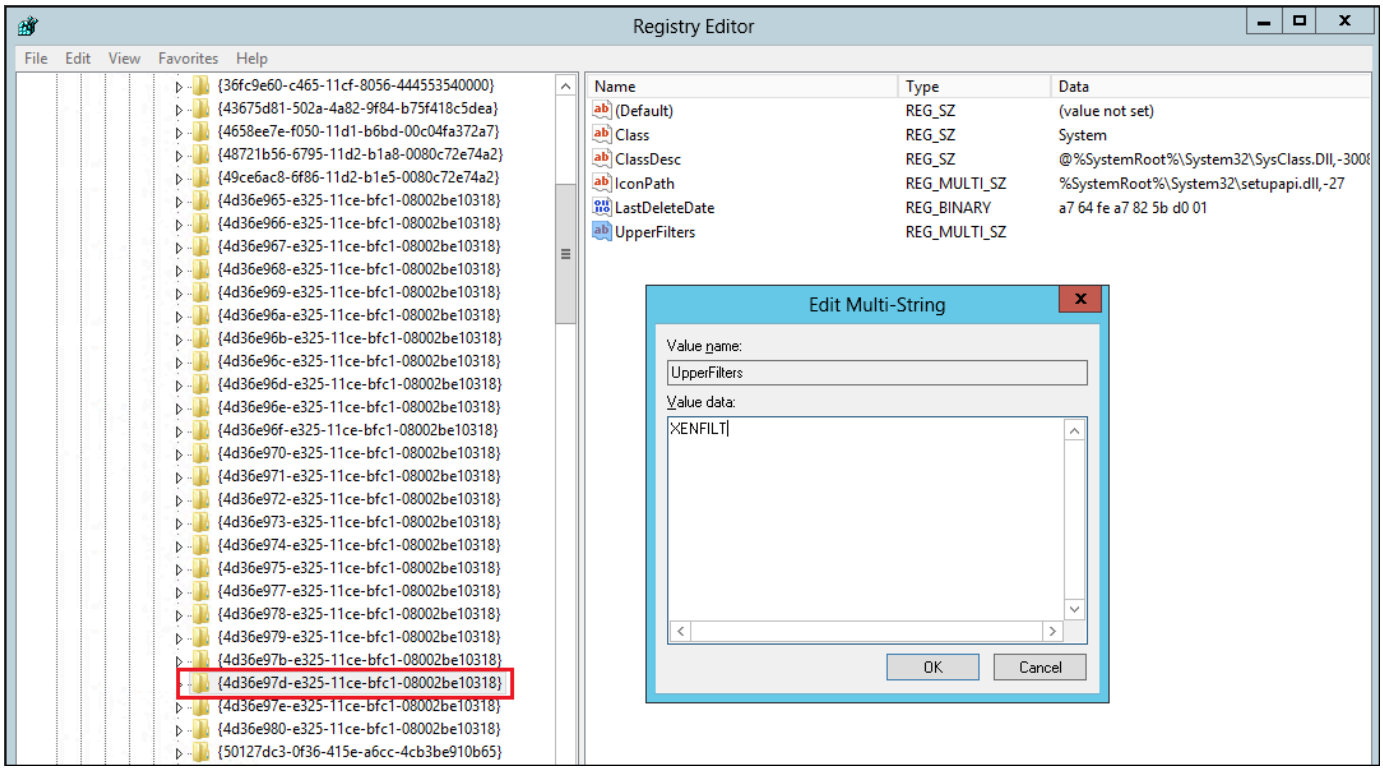
> **Important**
>
> Wenn Sie die Instance nicht in der gleichen Availability Zone wie die betroffene Instance erstellen, können Sie das Stamm-Volume der betroffenen Instance nicht der neuen Instance anfügen.

5. Wählen Sie im Navigationsbereich Volumes aus.
6. Lokalisieren Sie das Stamm-Volume der betroffenen Instance. Trennen Sie das Volume und fügen Sie das Volume anschließend der temporären Instance an, die Sie zuvor erstellt haben. Fügen Sie es dem standardmäßigen Gerätenamen (xvdf) an.
7. Stellen Sie über Remote Desktop eine Verbindung mit der temporären Instance her und verwenden Sie anschließend das Dienstprogramm für die Datenträgerverwaltung, um das Volume verfügbar zu machen und es zu verwenden.
8. Öffnen Sie in der temporären Instance das Dialogfeld Ausführen, geben Sie **`regedit`** ein und drücken Sie die Eingabetaste.
9. Wählen Sie im Navigationsbereich des Registrierungs-Editors die Option HKEY_LOCAL_MACHINE aus und wählen Sie dann im Menü File die Option Load Hive.
10. Navigieren Sie im Dialogfeld Load Hive zu Betroffenes Volume\Windows\System32\config \System" und geben Sie im Dialogfeld Key Name einen temporären Namen ein. z. B. „OldSys".
11. Suchen Sie im Navigationsbereich des Registrierungs-Editors die folgenden Schlüssel:

    HKEY_LOCAL_MACHINE***`Ihr_temporärer_Schlüsselname`***\ControlSet001\Control\Class \4d36e97d-e325-11ce-bfc1-08002be10318

    HKEY_LOCAL_MACHINE***`Ihr_temporärer_Schlüsselname`***\ControlSet001\Control\Class \4d36e96a-e325-11ce-bfc1-08002be10318

12. Doppelklicken Sie für jeden Schlüssel auf UpperFilters, geben Sie einen Wert für XENFILT ein und wählen Sie anschließend OK.



13. Suchen Sie den folgenden Schlüssel:

    HKEY_LOCAL_MACHINE***Ihr_temporärer_Schlüsselname***\ControlSet001\Services\XENBUS\Parameters

14. Erstellen Sie eine neue Zeichenfolge (REG_SZ) mit dem Namen „ActiveDevice” und dem folgenden Wert:

    PCI\VEN_5853&DEV_0001&SUBSYS_00015853&REV_01

15. Suchen Sie den folgenden Schlüssel:

    HKEY_LOCAL_MACHINE***Ihr_temporärer_Schlüsselname***\ControlSet001\Services\XENBUS

16. Ändern Sie den Wert unter Count von 0 in 1.

17. Suchen Sie die folgenden Schlüssel und löschen Sie sie:

    HKEY_LOCAL_MACHINE***Ihr_temporärer_Schlüsselname***\ControlSet001\Services\xenvbd\StartOverride

HKEY_LOCAL_MACHINE*Ihr_temporärer_Schlüsselname*\ControlSet001\Services\xenfilt\StartOverride

18. Wählen Sie im Navigationsbereich "Registry Editor" den temporären Schlüssel aus, den Sie beim ersten Öffnen des Registrierungs-Editors erstellt haben.
19. Wählen Sie im Menü File die Option Unload Hive aus.
20. Wählen Sie im Dienstprogramm für die Datenträgerverwaltung das Laufwerk aus, das Sie zugewiesen haben, öffnen Sie das Kontextmenü (rechte Maustaste) und wählen Sie die Option Offline aus.
21. Trennen Sie in der Amazon EC2-Konsole das betroffene Volume von der temporären Instance und ordnen Sie es wieder Ihrer Windows Server 2012 R2-Instance mit den Gerätenamen „/dev/sda1” zu. Sie müssen diesen Gerätenamen angeben, um das Volume als Stamm-Volume hinzufügen zu können.
22. Starten Sie die Instance.
23. Stellen Sie über Remote Desktop eine Verbindung mit der Instance her und laden Sie anschließend das Upgrade-Paket für die AWS PV-Treiber in die Instance herunter.
24. Extrahieren Sie den Inhalt des Ordners und führen Sie die Datei au `AWSPVDriverSetup.msi`.

    Wenn Sie die MSI-Datei ausgeführt haben, wird die Instance automatisch neu gestartet und das Upgrade der Treiber durchgeführt. Die Instance ist für die Dauer von bis zu 15 Minuten nicht verfügbar.
25. Wenn das Upgrade abgeschlossen wurde und die Instance beide Zustandsprüfungen in der Amazon EC2-Konsole bestanden hat, stellen Sie über Remote Desktop eine Verbindung mit der Instance her und prüfen Sie, ob die neuen Treiber installiert wurden. Suchen Sie im Geräte-Manager unter Storage Controllers den AWS PV Storage Host Adapter. Vergewissern Sie sich, dass die Treiberversion identisch mit der aktuellen Version in der Tabelle für den Treiber-Versionsverlauf ist. Weitere Informationen finden Sie unter AWS PV-Treiber – Paketverlauf.
26. Löschen Sie die in diesem Vorgang erstellte temporäre Instance bzw. beenden Sie sie.

Ausführen des Korrekturskripts

Wenn Sie kein direktes Upgrade der Treiber durchführen oder nicht in eine aktuelle Instance migrieren können, haben Sie die Möglichkeit, das Korrekturskript auszuführen, um die Probleme zu beheben, die von der „Plug & Play Cleanup”-Task verursacht wurden.

So führen Sie das Korrekturskript aus

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus, für die Sie das Korrekturskript ausführen möchten. Wählen Sie Instance state (Instance-Status) und dann Stop instance (Instance anhalten) aus.

   > **Warning**
   >
   > Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

4. Wenn die Instance angehalten wurde, erstellen Sie ein Backup. Wählen Sie die Instance, wählen Sie Actions (Aktionen), dann Image und Templates (Image und Vorlagen) und dann Create image (Image erstellen).
5. Wählen Sie Instance state (Instance-Status) und dann Start instance (Instance starten) aus.
6. Stellen Sie über Remote Desktop eine Verbindung mit der Instance her und laden Sie anschließend die Datei RemediateDriverIssue.zip in die Instance herunter.
7. Extrahieren Sie die Inhalte der Datei.
8. Führen Sie das Korrekturskript aus; befolgen Sie dazu die Anweisungen in der Datei Readme.txt. Die Datei befindet sich in dem Ordner, in den die Datei RemediateDriverIssue.zip extrahiert wurde.

TCP-Offloading

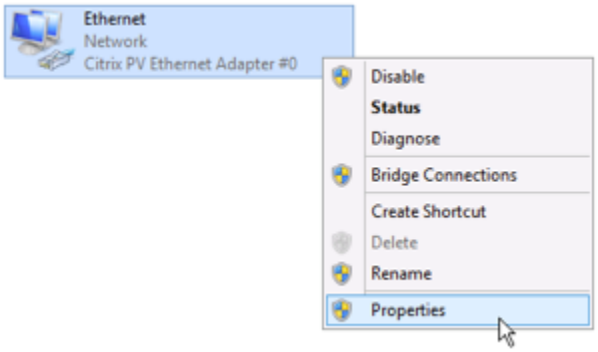
> **Important**
>
> Dieses Problem gilt nicht für Instances, auf denen AWS PV- oder Intel-Netzwerktreiber ausgeführt werden.

TCP-Offloading ist standardmäßig für Citrix PV-Treiber in Windows-AMIs aktiviert. Wenn Fehler auf der Transportebene oder bei der Übertragung von Paketen auftreten, bzw. in der Windows—Leistungsüberwachung angezeigt werden, z. B. wenn Sie bestimmte SQL—Workloads ausführen, dann müssen Sie dieses Feature möglicherweise deaktivieren.

> **Warning**
>
> Durch die Deaktivierung des TCP-Offloading verschlechtert sich möglicherweise die Netzwerkleistung Ihre Instance.

So deaktivieren Sie TCP-Offloading unter Windows Server 2012 und 2008

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
2. Wenn Sie Windows Server 2012 verwenden, drücken Sie Ctrl+Esc, um den Start-Bildschirm aufzurufen, und wählen Sie dann Control Panel (Systemsteuerung). Wenn Sie Windows Server 2008 verwenden, wählen Sie Start und dann die Option Control Panel (Systemsteuerung) aus.
3. Wählen Sie dann Netzwerk und Internet und anschließend Netzwerk- und Freigabecenter aus.
4. Wählen Sie Change adapter settings (Adapter-Einstellungen ändern) aus.
5. Klicken Sie mit der rechten Maustaste auf Citrix PV Ethernet Adapter #0 und wählen Sie die Option Properties.



6. Wählen Sie im Dialogfeld Eigenschaften der LAN-Verbindung die Option Konfigurieren aus, um das Dialogfeld Citrix PV Ethernet Adapter #0 Properties (Eigenschaften für Citrix PV Ethernet Adapter #0) zu öffnen.
7. Deaktivieren Sie auf der Registerkarte Erweitert jede der Eigenschaften, mit Ausnahme von Correct TCP/UDP Checksum Value (TCP/UDP-Prüfsummenwert korrigieren). Um eine Eigenschaft zu deaktivieren, wählen Sie sie unter Eigenschaft aus und wählen Sie unter dem Punkt Wert die Option Deaktiviert aus.
8. Klicken Sie auf OK.
9. Führen Sie die folgenden Befehle in einem Eingabeaufforderungsfenster aus.

```
netsh int ip set global taskoffload=disabled
netsh int tcp set global chimney=disabled
netsh int tcp set global rss=disabled
netsh int tcp set global netdma=disabled
```

10. Starten Sie die Instance neu.

Zeitsynchronisierung

Vor der Veröffentlichung der Windows-AMI 2013.02.13 konnte der Citrix Xen Guest Agent die Systemzeit falsch einstellen. Das kann dazu führen, dass Ihr DHCP-Lease abläuft. Wenn Sie Probleme mit der Verbindung zu Ihrer Instance haben, müssen Sie den Agent möglicherweise aktualisieren.

Sie können ermitteln, ob Sie bereits den aktualisierten Citrix Xen Guest Agent installiert haben, indem Sie prüfen, ob die Datei `C:\Program Files\Citrix\XenGuestAgent.exe` im März 2013 erstellt wurde. Wenn der Zeitstempel dieser Datei ein früheres Datum anzeigt, sollten sie den Citrix Xen Guest Agent-Service aktualisieren. Weitere Informationen finden Sie unter Upgrade des Citrix-Xen-Guest-Agent-Service.

Workloads, die mehr als 20 000 Festplatten-IOPS nutzen, führen zu einem Leistungsabfall aufgrund von CPU-Engpässen

Sie können von diesem Problem betroffen sein, wenn Sie Windows-Instances verwenden, auf denen AWS-PV-Treiber ausgeführt werden, die mehr als 20 000 IOPS nutzen, und es zu Fehlerprüfungscode `0x9E: USER_MODE_HEALTH_MONITOR` kommt.

Lese- und Schreibvorgänge (iOS) in den AWS PV-Treibern erfolgen in zwei Phasen: I/O-Vorbereitung und I/O-Abschluss. Standardmäßig läuft die Vorbereitungsphase auf einem einzelnen beliebigen Kern ab. Die Abschlussphase läuft auf Kern `0`. Die Menge an Berechnung, die für die Verarbeitung eines I/O erforderlich ist, hängt von der Größe und anderen Eigenschaften ab. Einige iOS verwenden in der Vorbereitungsphase mehr Berechnungen und andere in der Abschlussphase. Wenn eine Instance mehr als 20 000 IOPS steuert, kann die Vorbereitungs- oder Abschlussphase zu einem Engpass führen, bei dem die CPU, auf der sie läuft, eine Kapazität von 100% hat. Ob die Vorbereitungs- oder Abschlussphase zu einem Engpass wird oder nicht, hängt von den Eigenschaften des von der Anwendung verwendeten iOS ab.

Beginnend mit AWS PV-Treibern 8.4.0 kann die Last der Vorbereitungsphase und der Abschlussphase auf mehrere Kerne verteilt werden, wodurch Engpässe vermieden werden.

Jede Anwendung verwendet verschiedene I/O-Eigenschaften. Daher kann die Anwendung einer der folgenden Konfigurationen die Leistung Ihrer Anwendung erhöhen, verringern oder nicht beeinflussen. Nachdem Sie eine dieser Konfigurationen angewendet haben, überwachen Sie die Anwendung, um sicherzustellen, dass sie Ihre gewünschte Leistung erfüllt.

1. Voraussetzungen

   Bevor Sie mit diesem Fehlerbehebungsverfahren beginnen, sollten Sie die folgenden Voraussetzungen überprüfen:

   - Ihre Instance verwendet AWS PV-Treiber Version 8.4.0 oder höher. Informationen zum Upgrade finden Sie unter Upgrade von PV-Treibern auf EC2-Windows-Instances.
   - Sie haben RDP-Zugriff auf die Instance. Schritte zum Herstellen einer Verbindung mit Ihrer Windows-Instance über RDP finden Sie unter Verbindung zu Ihrer Windows-Instance mithilfe eines RDP-Clients herstellen.
   - Sie haben Administratorzugriff auf die Instance.

2. Beobachten Sie die CPU-Auslastung in Ihrer Instance

   Sie können den Windows Task-Manager verwenden, um die Auslastung jeder CPU anzuzeigen, um potenzielle Engpässe bei der Festplatten-I/O zu ermitteln.

   1. Stellen Sie sicher, dass Ihre Anwendung läuft und ähnlich wie Ihr Produktions-Workload Datenverkehr verarbeitet.
   2. Herstellen einer Verbindung mit Ihrer Instance über RDP.
   3. Wähle das Menü Start auf Ihrer Instance.
   4. Geben Sie `Task Manager` im Menü Start ein, um den Task-Manager zu öffnen.
   5. Wenn Task-Manager die Zusammenfassungsansicht anzeigt, wählen Sie More details (Weitere Einzelheiten), um die Detailansicht zu erweitern.
   6. Wählen Sie die Registerkarte Performance (Leistung) aus.
   7. Wählen Sie CPU im linken Bereich.
   8. Klicken Sie mit der rechten Maustaste auf das Diagramm im Hauptbereich und wählen Sie Change graph to (Diagramm ändern zu) > Logical processors (Logische Prozessoren), um jeden einzelnen Kern anzuzeigen.
   9. Je nachdem, wie viele Kerne sich auf Ihrer Instance befinden, sehen Sie möglicherweise Zeilen, die im Laufe der Zeit die CPU-Auslastung anzeigen oder Sie sehen nur eine Zahl.

- Wenn Sie Diagramme sehen, die die Last über die Zeit anzeigen, suchen Sie nach CPUs, bei denen das Kästchen fast vollständig schattiert ist.
- Wenn Sie auf jedem Kern eine Zahl sehen, suchen Sie nach Kernen, die durchweg 95% oder mehr anzeigen.

10 Beachten Sie, ob Kern `0` oder ein anderer Kern stark ausgelastet ist.

3. Wählen Sie, welche Konfiguration angewendet werden soll

Konfigurationsname	Wann diese Konfiguration angewendet werden	Hinweise
Default configuration	Workload verursacht weniger als 20 000 IOPS oder haben andere Konfigurationen die Leistung oder Stabilität nicht verbessert.	Für diese Konfiguration tritt I/O auf einigen Kernen auf, was kleineren Workloads zugute kommen kann, indem die Cache-Lokalität erhöht und der Kontextwechsel reduziert wird.
Allow driver to choose whether to distribute completion	Der Workload nutzt mehr als 20 000 IOPS, und eine moderate oder hohe Last wird im Kern `0` beobachten.	Diese Konfiguration wird für alle Xen-Instances empfohlen, die PV 8.4.0 oder höher verwenden und mehr als 20 000 IOPS nutzen, unabhängig davon, ob Probleme auftreten oder nicht.
Distribute both preparation and completion	Workload verursacht mehr als 20 000 IOPS, und entweder verbesserte die Erlaubnis für den Treiber, die Verteilung zu wählen, die Leistung nicht oder ein anderer Kern als `0` weit eine hohe Auslastung auf.	Diese Konfiguration ermöglicht die Verteilung sowohl der I/O-Vorbereitung als auch des I/O-Abschluss.

> **Note**
>
> Wir empfehlen, dass Sie die I/O-Vorbereitung nicht verteilen, ohne auch die I/O-Abschluss zu verteilen (Einstellung `DpcRedirection` ohne Einstellung `NotifierDistributed`), da die Abschlussphase empfindlich auf Überlastung durch die Vorbereitungsphase reagiert, wenn die Vorbereitungsphase parallel läuft.

Werte für Registrierungsschlüssel

- NotifierDistributed

  Wert `0` oder nicht vorhanden — Die Abschlussphase läuft auf Kern `0` .

  Wert `1` — Der Treiber entscheidet sich für die Durchführung der Abschlussphase oder Kern `0` oder einen zusätzlicher Kern pro angeschlossener Festplatte.

  Wert `2` — Der Treiber führt die Abschlussphase auf einem zusätzlichen Kern pro angeschlossener Festplatte aus.

- DpcRedirection

  Wert `0` oder nicht vorhanden — Die Vorbereitungsphase läuft auf einem einzigen, willkürlichen Kern.

  Wert `1` — Die Vorbereitungsphase ist auf mehrere Kerne verteilt.

Standardkonfiguration

Verwenden Sie die Standardkonfiguration mit AWS PV-Treiberversionen vor 8.4.0 oder wenn nach Anwendung einer der anderen Konfigurationen in diesem Abschnitt eine Leistungs- oder Stabilitätsverschlechterung beobachtet wird.

1. Herstellen einer Verbindung mit Ihrer Instance über RDP.
2. Öffnen Sie eine neue PowerShell-Eingabeaufforderung als Administrator.

3. Führen Sie die folgenden Befehle aus, um `NotifierDistributed` und `DpcRedirection`-Registrierungsschlüssel zu entfernen.

```
Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Name NotifierDistributed
```

```
Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Name DpcRedirection
```

4. Starten Sie Ihre Instance neu.

Treiber können auswählen, ob die Fertigstellung verteilt werden soll

Legen Sie den `NotiferDistributed`-Registrierungsschlüssel fest, damit der PV-Speichertreiber wählen kann, ob der I/O-Abschluss verteilt werden soll oder nicht.

1. Herstellen einer Verbindung mit Ihrer Instance über RDP.
2. Öffnen Sie eine neue PowerShell-Eingabeaufforderung als Administrator.
3. Führen Sie den folgenden Befehl aus, um den `NotiferDistributed`-Registrierungsschlüssel festzulegen:

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name NotifierDistributed
```

4. Starten Sie Ihre Instance neu.

Verteilen Sie sowohl Vorbereitung als auch Fertigstellung

Legen Sie `NotifierDistributed` und `DpcRedirection`-Registrierungsschlüssel fest, um immer sowohl die Vorbereitungs- als auch die Abschlussphase zu verteilen.

1. Herstellen einer Verbindung mit Ihrer Instance über RDP.
2. Öffnen Sie eine neue PowerShell-Eingabeaufforderung als Administrator.
3. Führen Sie die folgenden Befehle aus, um den `NotifierDistributed`- und `DpcRedirection`- Registrierungsschlüssel festzulegen.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000002 -Name NotifierDistributed
```

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name DpcRedirection
```

4. Starten Sie Ihre Instance neu.

AWS NVMe-Treiber

Amazon-EBS-und -Instance-Speicher-Volumes werden als NVMe-Blockgeräte auf Nitro-basierenden Instances angezeigt. Um die Leistung und die Funktionen der Amazon-EBS-Funktionen für Volumes, die als NVMe-Blockgeräte bereitgestellt werden, vollständig nutzen zu können, muss auf der Instance der AWS-NVMe-Treiber installiert sein. Auf allen AWS-Windows-AMIs der aktuellen Generation ist der AWS-NVMe-Treiber standardmäßig installiert.

Weitere Informationen finden Sie unter Amazon EBS und NVMe im Amazon-EBS-Benutzerhandbuch. Weitere Informationen über SSD-Instance-Speicher und NVMe finden Sie unter SSD-Instance-Speicher-Volumes für EC2-Instances.

Linux-Instances

Die folgenden AMIs enthalten die erforderlichen NVMe-Treiber:

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 oder höher mit `linux-aws`-Kernel

> **Note**
>
> AWS-Graviton-basierte Instance-Typen erfordern Ubuntu 18.04 oder höher mit `linux-aws`-Kernel

- Red Hat Enterprise Linux 7.4 oder höher
- SUSE Linux Enterprise Server 12 SP2 oder höher
- CentOS 7.4.1708 oder höher
- FreeBSD 11.1 oder höher

- Debian GNU/Linux 9 oder höher

So prüfen Sie, ob Ihre Instance über den NVMe-Treiber verfügt

Sie können mit dem folgenden Befehl bestätigen, dass Ihre Instance über den NVMe-Treiber verfügt.

- Amazon Linux, RHEL, CentOS und SUSE Linux Enterprise Server

```
$ modinfo nvme
```

  Wenn die Instance über den NVMe-Treiber verfügt, gibt der Befehl Informationen über den Treiber zurück.
- Amazon Linux 2 und Ubuntu

```
$ ls /sys/module/ | grep nvme
```

  Wenn die Instance über den NVMe-Treiber verfügt, gibt der Befehl die installierten Treiber zurück.

So aktualisieren Sie den NVMe-Treiber

Wenn Ihre Instance über den NVMe-Treiber verfügt, können Sie den Treiber mithilfe des folgenden Verfahrens auf die neueste Version aktualisieren.

1. Verbinden Sie sich mit der Instance.
2. Aktualisieren Sie den Cache der Paketverwaltung, um die erforderlichen Paketaktualisierungen herunterzuladen.
   - Für Amazon Linux 2, Amazon Linux, CentOS und Red Hat Enterprise Linux:

     ```
     [ec2-user ~]$ sudo yum update -y
     ```
   - Für Ubuntu und Debian:

     ```
     [ec2-user ~]$ sudo apt-get update -y
     ```
3. Ubuntu 16.04 und höher umfasst das `linux-aws`-Paket, das die von den Nitro-basierten Instances erforderten NVMe- und ENA-Treiber enthält. Aktualisieren Sie das `linux-aws`-Paket, um die aktuelle Version zu erhalten:

```
[ec2-user ~]$ sudo apt-get install --only-upgrade -y linux-aws
```

Für Ubuntu 14.04 können Sie das aktuelle `linux-aws`-Paket wie folgt installieren:

```
[ec2-user ~]$ sudo apt-get install linux-aws
```

4. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
sudo reboot
```

5. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.

Windows-Instances

PowerShell

Wenn Sie Ihre Instance nicht von einem der aktuellen, von Amazon bereitgestellten AWS-Windows-AMIs gestartet haben, gehen Sie wie folgt vor, um den aktuellen AWS-NVMe-Treiber auf Ihrer Instance zu installieren. Für diese Installation ist ein Neustart erforderlich. Entweder wird das Installationsskript Ihre Instance neu starten oder Sie müssen sie als letzten Schritt neu starten.

Voraussetzungen

- PowerShell Version 3.0 oder höher ist installiert.
- Die in diesem Abschnitt aufgeführten Befehle müssen in der 64-Bit-Version von PowerShell ausgeführt werden. Verwenden Sie nicht die x86-Version von PowerShell. Das ist die 32-Bit-Version der Shell und wird für diese Befehle nicht unterstützt.

So laden Sie den neuesten AWS NVMe-Treiber herunter und installieren ihn

1. Wir empfehlen Ihnen, ein AMI wie folgt als Backup zu erstellen, falls Sie Ihre Änderungen rückgängig machen müssen.

   a. Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Stellen Sie vor dem Anhalten einer Instance sicher, dass Sie alle benötigten Daten aus den Instance-Speicher-Volumes in den persistenten Speicher kopiert haben, z. B. Amazon EBS oder Amazon S3.

b. Wählen Sie im Navigationsbereich Instances aus.

c. Wählen Sie die Instance, die ein Treiberupgrade benötigt und wählen Sie Instance state (Instance-Zustand), Stop instance (Instance stoppen) aus.

d. Nachdem die Instance angehalten wurde, wählen Sie die Instance aus, wählen Sie Actions (Aktionen), Image and Templates (Image und Vorlagen) und dann Create image (Image erstellen) aus.

e. Wählen Sie Instance state (Instance-Status), Start instance (Instance starten).

2. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.

3. Laden Sie die Treiber mit einer der folgenden Optionen auf Ihre Instance herunter:

   - Browser – Download des neuesten Treiberpakets auf die Instance und Extrahieren des ZIP-Archivs.
   - PowerShell – Führen Sie die folgenden Befehle aus:

     ```
     Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/
     NVMe/Latest/AWSNVMe.zip -outfile $env:USERPROFILE\nvme_driver.zip
     Expand-Archive $env:userprofile\nvme_driver.zip -DestinationPath
      $env:userprofile\nvme_driver
     ```

     Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 oder früher verwenden, muss TLS 1.2 möglicherweise für Ihr PowerShell-Terminal aktiviert werden. Sie können TLS 1.2 für die aktuelle PowerShell-Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:

     ```
     [Net.ServicePointManager]::SecurityProtocol =
      [Net.SecurityProtocolType]::Tls12
     ```

4. Installieren Sie den Treiber auf Ihrer Instance, indem Sie das `install.ps1` PowerShell-Skript aus dem `nvme_driver`-Verzeichnis (`.\install.ps1`) ausführen. Wenn ein Fehler angezeigt wird, stellen Sie sicher, dass Sie PowerShell 3.0 oder höher verwenden.

   a. (Optional) Ab der AWS NVMe-Version `1.5.0` werden persistente Reservierungen für Small Computer System Interface (SCSI) für Windows Server 2016 und höher unterstützt. Dieses Feature fügt Unterstützung für Windows Server Failover Clustering mit gemeinsam genutztem Amazon EBS-Speicher hinzu. Dieses Feature ist bei der Installation standardmäßig nicht aktiviert.

Sie können das Feature aktivieren, wenn Sie das `install.ps1` Skript zur Installation des Treibers ausführen, indem Sie den `EnableSCSIPersistentReservations` Parameter mit dem Wert angeben`$true`.

```
PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $true
```

Sie können das Feature deaktivieren, wenn Sie das `install.ps1` Skript zur Installation des Treibers ausführen, indem Sie den `EnableSCSIPersistentReservations` Parameter mit dem Wert angeben`$false`.

```
PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $false
```

b. Beginnend mit AWS NVMe `1.5.0` installiert das `install.ps1` Skript das `ebsnvme-id` Tool immer zusammen mit dem Treiber.

   (Optional) Für die Versionen `1.4.0` `1.4.1` und `1.4.2` können Sie mit dem `install.ps1` Skript angeben, ob das `ebsnvme-id` Tool zusammen mit dem Treiber installiert werden soll.

   i. Um das `ebsnvme-id`-Tool zu installieren, geben Sie `InstallEBSNVMeIdTool 'Yes'` an.

   ii. Wenn Sie das Tool nicht installieren möchten, geben Sie `InstallEBSNVMeIdTool 'No'` an.

   Wenn Sie `InstallEBSNVMeIdTool` nicht angeben, und das Tool bereits bei `C:\ProgramData\Amazon\Tools` vorhanden ist, aktualisiert das Paket das Tool standardmäßig. Wenn das Tool nicht vorhanden ist, aktualisiert `install.ps1` das Tool standardmäßig nicht.

   Wenn Sie das Tool nicht als Teil des Pakets, sondern zu einem späteren Zeitpunkt, installieren möchten, finden Sie die neueste Version oder das Tool im Treiberpaket. Alternativ können Sie die Version `1.0.0` von Amazon S3 herunterladen:

   Laden Sie das `ebsnvme-id`-Tool herunter.

5. Wenn das Installationsprogramm Ihre Instance nicht neu startet, starten Sie die Instance neu.

Distributor

Das NVMe-Treiberpaket können Sie einmal mit Distributor, einer Funktion von AWS Systems Manager, oder mit geplanten Updates installieren.

So installieren Sie den AWS-NVMe-Treiber

1. Anweisungen zum Installieren des NVMe-Treiberpakets mit Distributor finden Sie in den Verfahren unter Installieren oder Aktualisieren von Paketen im Benutzerhandbuch für Amazon EC2 Systems Manager.
2. Wählen Sie für Installationstyp Deinstallieren und neu installieren aus.
3. Wählen Sie als Name AWSNVMe aus.
4. (Optional) Unter Zusätzliche Argumente können Sie die Installation durch Angabe von Werten anpassen. Die Werte müssen mit einer gültigen JSON-Syntax formatiert werden. Beispiele für die Übergabe zusätzlicher Argumente für das `aws configure`-Paket finden Sie in der Referenz zum Befehlsdokument-Plug-In.

   a. Ab AWS NVMe `1.5.0` unterstützt der Treiber persistente SCSI-Reservierungen für Windows Server 2016 und höher. Dieses Feature ist bei der Installation standardmäßig nicht aktiviert.

      - Um dieses Feature zu aktivieren, geben Sie an `{"SSM_EnableSCSIPersistentReservations": "true"}`.
      - Wenn Sie dieses Feature nicht aktivieren möchten, geben Sie an `{"SSM_EnableSCSIPersistentReservations": "false"}`.

   b. Beginnend mit AWS NVMe `1.5.0` installiert das `install.ps1`-Skript das `ebsnvme-id`-Tool immer.

      (Optional) Für die Versionen`1.4.0`, `1.4.1` und`1.4.2` können Sie mit dem `install.ps1`-Skript angeben, ob das Tool ebsnvme-id mit dem Treiber installiert werden soll.

      - Um das Tool ebsnvme-id zu installieren, geben Sie an `{"SSM_InstallEBSNVMeIdTool": "Yes"}`.
      - Wenn Sie das Tool nicht installieren möchten, geben Sie an `{"SSM_InstallEBSNVMeIdTool": "No"}`.

Wenn `SSM_InstallEBSNVMeIdTool` nicht für Zusätzliche Argumente angegeben ist und das Tool bereits bei `C:\ProgramData\Amazon\Tools` vorhanden ist, aktualisiert das Paket das Tool standardmäßig. Wenn das Tool nicht vorhanden ist, aktualisiert das Paket das Tool standardmäßig nicht.

Wenn Sie das Tool nicht als Teil des Pakets, sondern zu einem späteren Zeitpunkt, installieren möchten, finden Sie die neueste Version des Tools im Treiberpaket. Alternativ können Sie die Version `1.0.0` von Amazon S3 herunterladen:

Laden Sie das `ebsnvme-id`-Tool herunter.

5. Wenn das Installationsprogramm Ihre Instance nicht neu startet, starten Sie die Instance neu.

Persistente SCSI-Reservierungen für Windows-Instances konfigurieren

Nachdem die AWS NVMe-Treiberversion `1.5.0` oder höher installiert wurde, können Sie persistente SCSI-Reservierungen mithilfe der Windows-Registrierung für Windows Server 2016 und höher aktivieren oder deaktivieren. Sie müssen die Instance neu starten, damit die Registry-Änderungen übernommen werden.

Sie können persistente SCSI-Reservierungen mit dem folgenden Befehl aktivieren, der den Wert `EnableSCSIPersistentReservations` auf den Wert 1 setzt.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 1
```

Sie können persistente SCSI-Reservierungen mit dem folgenden Befehl deaktivieren, der den Wert `EnableSCSIPersistentReservations` auf den Wert `0` setzt.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 0
```

Versionsverlauf der AWS-NVMe-Windows-Treiber

Die folgende Tabelle zeigt, welche AWS-NVMe-Treiber Sie unter den einzelnen Versionen von Windows Server in Amazon EC2 verwenden sollten.

Windows Server Version	AWS-NVME-Treiberversionen
Windows Server 2025	Aktuelle Version
Windows Server 2022	Aktuelle Version
Windows Server 2019	Aktuelle Version
Windows Server 2016	Aktuelle Version
Windows Server 2012 R2	Version 1.5.1 und früher
Windows Server 2012	Version 1.5.1 und früher
Windows Server 2008 R2	Version 1.3.2 und früher
Windows Server 2008	Version 1.3.2 und früher

Die folgende Tabelle beschreibt die veröffentlichten Versionen des AWS NVMe-Treibers.

Paketversion	Treiberversion	Details	Datum der Veröffentlichung
1.7.0	1.7.0	• Unterstützung für den NVMe-Befehl Get Log Page hinzugefügt. • Unterstützung für detaillierte Leistungsstatistiken für EBS- und EC2-Instance-Speicher-Volumes hinzugefügt. • Fehlerkorrekturen für den Befehl Identify Namespace.	17. September 2025
1.6.0	1.6.0	• Das Installationsskript wurde aktualisiert, um PnPUtil zu verwenden. •	25. Oktober 2024

Paketversion	Treiberversion	Details	Datum der Veröffentlichung
		ebsnvme-id.exe wurde aktualisiert, um NVMe IOCTL zu verwenden.	
1.5.1	1.5.0	Das Installationsskript wurde korrigiert, um bei Bedarf einen Ordner für das `ebsnvme-id` -Tool zu erstellen.	17. November 2023
1.5.0	1.5.0	Unterstützung für persistente Reservierungen mit Small Computer System Interface (SCSI) für Instances hinzugefügt, auf denen Windows Server 2016 und höher ausgeführt wird. Das Tool ebsnvme-id (`ebsnvme-id.exe`) ist jetzt standardmäßig installiert.	31. August 2023
1.4.2	1.4.2	Es wurde ein Fehler behoben, bei dem AWS-NVMe-TreiberInstance-Speicher-Volumes auf D3-Instances nicht unterstützt hat.	16. März 2023
1.4.1	1.4.1	Meldet Namespace Preferred Write Granularity (NPGW) für EBS-Volumes, die dieses optionale NVMe-Feature unterstützen. Weitere Informationen finden Sie in Abschnitt 8.25, „Verbesserung der Leistung durch I/O-Größe und Ausrichtungsadhärenz“ in derNVMe Basisspezifikation, Version 1.4.	20. Mai 2022

Paketversion	Treiberversion	Details	Datum der Veröffentlichung
1.4.0	1.4.0	• Unterstützung für IoCTLs wurde hinzugefügt, mit denen Anwendungen mit NVMe-Geräten interagieren können. Diese Unterstützung ermöglicht es Anwendungen, `IdentifyController` -, `IdentifyNamespace` - und `NameSpace` -Listen vom NVMe-Gerät abzurufen. Weitere Informationen finden Sie unter Protokollspezifische Abfragen in der Microsoft-Dokumentation. • Die Treiberversion 1.4.0 und das neueste `ebsnvme-id` -Tool (`ebsnvme-id.exe`) sind in einem einzigen Paket vereint. Mit dieser Kombination können Sie sowohl Treiber als auch Tool aus einem einzigen Paket installieren. Weitere Details finden Sie unter . AWS NVMe-Treiber. • Fehlerbehebungen und verbesserte Zuverlässigkeit.	23. November 2021
1.3.2	1.3.2	Behebung eines Problems bei der Modifizierung von EBS-Volumes während einer aktiven I/O-Verarbeitung, das zu beschädigten Daten führen könnte. Kunden, die EBS-Online-Volumes nicht modifizieren (beispielsweise durch Ändern von Größe oder Typ) sind nicht betroffen. Dies ist die letzte Version, die auf Windows Server 2008 und 2008 R2 ausgeführt werden kann. Diese Version steht zum Download zur Verfügung, wird aber nicht mehr unterstützt. Windows Server 2008 und 2008 R2 haben das Ende ihrer Lebensdauer erreicht und werden von Microsoft nicht mehr unterstützt.	10. September 2019

Paketversion	Treiberversion	Details	Datum der Veröffentlichung
1.3.1	1.3.1	Verbesserung der Zuverlässigkeit.	21. Mai 2019
1.3.0	1.3.0	Verbesserungen der Geräteoptimierung.	31. August 2018
1.2.0	1.2.0	Eine verbesserte Leistung und Zuverlässigkeit für AWS NVMe-Geräte auf allen unterstützten Instances, einschließlich Bare-Metal-Instances.	13. Juni 2018
>1.0.0	>1.0.0	AWS NVMe-Treiber für unterstützte Instance-Typen unter Windows Server.	12. Februar 2018

Abonnieren von -Benachrichtigungen

Amazon SNS kann Sie benachrichtigen, wenn neue Versionen von EC2-Windows-Treibern veröffentlicht werden. Führen Sie die folgenden Schritte durch, um diese Benachrichtigungen zu abonnieren.

So abonnieren Sie EC2-Benachrichtigungen über die Konsole

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Ändern Sie, falls erforderlich, die Region in der Navigationsleiste zu US East (N. Virginia). Sie müssen diese Region auswählen, weil sich die SNS-Benachrichtigungen, die Sie abonnieren, in dieser Region befinden.
3. Wählen Sie im Navigationsbereich Subscriptions aus.
4. Wählen Sie Create subscription.
5. Führen Sie im Dialogfeld Create subscription Folgendes aus:
   a. Kopieren Sie den folgenden Amazon-Ressourcennamen (ARN) unter TopicARN:

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers

   b. Wählen Sie unter Protocol die Option `Email` aus.

c. Geben Sie unter Endpoint eine E-Mail-Adresse ein, um die Benachrichtigungen zu empfangen.

d. Wählen Sie Create subscription (Abonnement erstellen) aus.

6. Sie erhalten eine Bestätigungs-E-Mail. Öffnen Sie die E-Mail und befolgen Sie die Anweisungen, um Ihr Abonnement abzuschließen.

Jedes Mal wenn neue EC2-Treiber für Windows veröffentlicht werden, senden wir ein Benachrichtigung an die Abonnenten. Wenn Sie diese Benachrichtigungen nicht mehr erhalten möchten, führen Sie die folgenden Schritte aus, um sich abzumelden.

So kündigen Sie ein Abonnement der Benachrichtigungen zu Amazon EC2-Treibern für Windows

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie im Navigationsbereich Subscriptions aus.
3. Aktivieren Sie das Kontrollkästchen für das Abonnement und wählen Sie dann Actions und Delete subscriptions (Löschen) aus. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

Abonnieren von EC2-Benachrichtigungen über AWS CLI

Um EC2-Benachrichtigungen über AWS CLI zu abonnieren, verwenden Sie den folgenden Befehl.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers --
protocol email --notification-endpoint YourUserName@YourDomainName.ext
```

Abonnieren von EC2-Benachrichtigungen über AWS Tools for Windows PowerShell

Um EC2-Benachrichtigungen über AWS Tools for Windows PowerShell zu abonnieren, verwenden Sie den folgenden Befehl.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-
drivers' -Protocol email -Region us-east-1 -Endpoint 'YourUserName@YourDomainName.ext'
```

Ihre Amazon-EC2-Instance konfigurieren

Nachdem Sie eine Windows-Instance gestartet haben, können Sie sich als Administrator anmelden, um zusätzliche Konfigurationen für Windows-Feature und Systemeinstellungen vorzunehmen.

Hilfsprogramme zur Fehlerbehebung bei EC2 Windows kann Ihnen helfen, Probleme auf Ihrer Instance zu beheben.

Sie können Windows-Startagenten und andere Windows-spezifische Feature wie folgt konfigurieren.

Windows-Start-Agenten

Jedes AWS Windows-AMI (und viele andere AMIs, die auf dem AWS Marketplace verfügbar sind) enthält einen Windows-Startagent, der mit Standardeinstellungen vorkonfiguriert ist. Startagenten führen Aufgaben während des Starts einer Instance aus und werden ausgeführt, wenn eine Instance angehalten und später gestartet oder neu gestartet wird.

EC2-Schnellstart für Windows

Jede Windows-Instance von Amazon EC2 muss die Standardstartschritte des Windows-Betriebssystems (OS) durchlaufen, die mehrere Neustarts beinhalten und oft 15 Minuten oder länger dauern. Windows-Server-AMIs von Amazon EC2, bei denen das EC2-Schnellstart-Feature aktiviert ist, führen einige dieser Schritte durch und werden zuvor neu gestartet. Dadurch reduzieren sie die benötigte Zeit zum Starten einer Instance.

Windows-spezifische Systemeinstellungen

Die folgende Liste enthält einige Systemeinstellungen, die nur für Windows-Betriebssysteme gelten:

Das Windows-Administratorpasswort ändern

Wenn Sie eine Verbindung zu einer Windows-Instance herstellen, müssen Sie ein Benutzerkonto und Passwort angeben, das für den Zugriff auf die Instance berechtigt ist. Wenn Sie sich zum ersten Mal mit einer Instance verbinden, müssen Sie das Administratorkonto verwenden und das Standardpasswort angeben. Bei der ersten Anmeldung bei einer Instance empfehlen wir Ihnen, den Standardwert des Administratorpassworts zu ändern.

Windows-Komponenten hinzufügen

Windows Server-Betriebssysteme enthalten viele optionale Komponenten. Es ist nicht sinnvoll, alle optionalen Komponenten auf jedem AWS-Windows Server-AMI vorzuhalten. Stattdessen stellen wir Ihnen EBS-Snapshots als Installationsmedien zur Verfügung, die die erforderlichen Dateien zum Konfigurieren oder Installieren von Komponenten auf Ihrer Windows-Instance enthalten.

WSL in Windows installieren

Windows Subsystem for Linux (WSL) kann kostenlos heruntergeladen werden und kann auf Ihrer Windows-Instance installiert werden. Durch die Installation des WSL können Sie native Linux-Befehlszeilen-Tools direkt auf Ihrer Windows-Instance ausführen und die Linux-Tools neben Ihrem herkömmlichen Windows-Desktop für Skripts verwenden. Sie können auf einer einzigen Windows-Instance problemlos zwischen Linux und Windows wechseln, was in einer Entwicklungsumgebung sehr nützlich sein kann.

AWS-Gerätetreiber für Windows-Instances

Sie können die AWS-Gerätetreiber für Ihre Windows-Instances aktualisieren. Weitere Informationen finden Sie unter the section called “Gerätetreiber verwalten”.

In der folgenden Tabelle werden die unterstützten Treiber für Nitro-basierte Instances nach Windows-Version zusammengefasst.

Version	Speicher-Treiber	Erweitertes-Netzwerk-Treiber
Windows Server 2025	AWS-NVMe letzte Version	ENA letzte Version
Windows Server 2022	AWS-NVMe letzte Version	ENA letzte Version
Windows Server 2019	AWS-NVMe letzte Version	ENA letzte Version
Windows Server 2016	AWS-NVMe letzte Version	ENA letzte Version
Windows Server 2012 R2	AWS-NVMe Version 1.5.1	ENA-Version 2.6.0
Windows Server 2008 R2	AWS-NVMe Version 1.3.2	ENA Version 2.2.3

In der folgenden Tabelle werden die unterstützten Treiber für Xen-basierte Instances nach Windows-Version zusammengefasst.

Version	Speicher-Treiber	Erweitertes-Netzwerk-Treiber
Windows Server 2022	AWSAktuelle PV-Version	• ENA letzte Version [1]

Version	Speicher-Treiber	Erweitertes-Netzwerk-Treiber
		• Intel VF [2] • AWS PV letzte version [3]
Windows Server 2019	AWSAktuelle PV-Version	• ENA letzte Version [1] • Intel VF [2] • AWS PV letzte version [3]
Windows Server 2016	AWSAktuelle PV-Version	• ENA letzte Version [1] • Intel VF [2] • AWS PV letzte version [3]
Windows Server 2012 R2	AWS PV-Version 8.4.3	• ENA Version 2.6.0 [1] • Intel VF [2] • AWS PV Version 8.4.3 [3]
Windows Server 2008 R2	AWS-PV, Version 8.3.5	• ENA Version 2.2.3 [1] • Intel VF [2] • AWS PV Version 8.3.5 [3]

[1] Für Instance-Typen G3, H1, I3, `m4.16xlarge`, P2, P3, P3dn und R4.

[2] Für Instance-Typen C3, C4, D2, I2, M4 (außer `m4.16xlarge`) und R3.

[3] Für Instance-Typen C1, M1, M2, M3, T1, T2, X1 und X1e.

Windows-Start-Agenten auf Amazon-EC2-Windows-Instances

Jedes AWS-Windows-AMI enthält einen Windows-Start-Agent, der mit Standardeinstellungen vorkonfiguriert ist. Start-Agenten führen Aufgaben während des Starts einer Instance aus und werden ausgeführt, wenn eine Instance angehalten und später gestartet oder neu gestartet wird. Informationen zu einem bestimmten Agenten finden Sie auf den Detailseiten in der folgenden Liste.

Weitere Informationen zu AWS-Windows-AMIs finden Sie in der AWS-Windows AMI-Referenz.

- Den EC2Launch-v2-Agenten verwenden, um Aufgaben während des Starts einer EC2-Windows-Instance auszuführen
- Den EC2Launch-v1-Agenten verwenden, um Aufgaben während des Starts einer EC2-Windows-Instance auszuführen
- Den EC2Config-Service verwenden, um Aufgaben während des Starts der EC2-Legacy-Windows-Betriebssysteminstance auszuführen

Inhalt

- Amazon-EC2-Start-Agenten vergleichen
- Das DNS-Suffix für EC2-Windows-Start-Agenten konfigurieren
- Benachrichtigungen von EC2-Windows-Start-Agenten abonnieren
- Windows Service Administration für EC2Launch-v2- und EC2Config-Agents

Amazon-EC2-Start-Agenten vergleichen

Die folgende Tabelle zeigt die wichtigsten funktionalen Unterschiede zwischen EC2Config, EC2Launch v1 und EC2Launch v2.

Feature	EC2Config	EC2Launch v1	EC2Launch v2
Run as (Ausführen als)	Windows Service	PowerShell-Skripts	Windows Service
Unterstützt	Nur Legacy-Betriebssysteme	Windows-Server-Versionen: • 2016 • 2019 (LTSC und SAC)	Windows-Server-Versionen: • 2016 • 2019 (LTSC und SAC) • 2022 • 2025
Konfigurationsdatei	XML	JSON	JSON/YAML

Feature	EC2Config	EC2Launch v1	EC2Launch v2
Festgelegter Administratorbenutzername	Nein	Nein	Ja
Komprimierte Benutzerdaten	Nein	Nein	Ja
Erstellung lokaler Benutzereigen auf AMI	Nein	Nein	Ja, konfigurierbar.
Aufgabenkonfiguration in Benutzerdaten	Nein	Nein	Ja
Konfigurierbares Hintergrundbild	Nein	Nein	Ja
Reihenfolge der Aufgabenausführung anpassen	Nein	Nein	Ja
Konfigurierbare Aufgaben	15	9	20 bei Start
Unterstützt Windows Event Viewer	Ja	Nein	Ja
Anzahl der Event Viewer-Ereignistypen	2	0	30

> **Note**
>
> Die EC2Config-Dokumentation dient nur zu historischen Referenzzwecken. Die Betriebssystemversionen, auf denen es ausgeführt wird, werden von Microsoft nicht mehr unterstützt. Es wird dringend empfohlen, ein Upgrade auf den neuesten Startservice durchzuführen.

Das DNS-Suffix für EC2-Windows-Start-Agenten konfigurieren

Mit Amazon-EC2-Start-Agenten können Sie eine Liste von DNS-Suffixen konfigurieren, die Windows-Instances für die Auflösung von Domain-Namen verwenden. Die Start-Agenten überschreiben die Windows-Standardeinstellungen im `System\CurrentControlSet\Services\Tcpip\Parameters\SearchList`-Registrierungsschlüssel, indem sie der DNS-Suffix-Suchliste die folgenden Werte hinzufügen:

- Die Domain der Instance
- Die Suffixe, die sich aus der Devolution der Instance-Domain ergeben
- NV-Domain
- Die von den einzelnen Netzwerkschnittstellenkarten angegebenen Domains

Alle Start-Agenten unterstützen die DNS-Suffix-Konfiguration. Weitere Informationen finden Sie in Ihrer spezifischen Start-Agent-Version:

- Informationen zur `setDnsSuffix`-Aufgabe und zur Konfiguration von DNS-Suffixen in EC2Launch v2 finden Sie unter setDnsSuffix .
- Informationen zur Einrichtung der DNS-Suffixliste und zur Aktivierung oder Deaktivierung der Devolution für EC2Launch v1 finden Sie unter Den EC2Launch-v1-Agent in Ihrer Windows-Instance konfigurieren.
- Informationen zur Einrichtung der DNS-Suffixliste und zur Aktivierung oder Deaktivierung der Devolution für EC2Config finden Sie unter EC2Config-Einstellungsdateien.

Übertragung von Domain-Namen

Die Übertragung von Domain-Namen ist ein Active-Directory-Verhalten, das es Computern in einer untergeordneten Domain ermöglicht, auf Ressourcen in der übergeordneten Domain zuzugreifen, ohne einen vollständig qualifizierten Domain-Namen zu verwenden Standardmäßig wird die Übertragung von Domain-Namen so lange fortgesetzt, bis nur noch zwei Knoten in der Reihenfolge des Domain-Namens übrig sind.

Wenn die Instance mit einer Domain verbunden ist, führen die Start-Agenten eine Devolution des Domain-Namens durch und fügen die Ergebnisse der DNS-Suffix-Suchliste hinzu, die im **`System\CurrentControlSet\Services\Tcpip\Parameters\SearchList`**-Registrierungsschlüssel verwaltet wird. Die Agenten verwenden die Einstellungen der folgenden Registrierungsschlüssel, um das Devolutionsverhalten zu bestimmen.

- **`System\CurrentControlSet\Services\Tcpip\Parameters \UseDomainNameDevolution`**
  - Wenn nicht festgelegt, wird die Devolution deaktiviert
  - Wenn auf `1` gesetzt, wird die Devolution aktiviert (Standard)
  - Wenn auf `0` gesetzt, wird die Devolution deaktiviert
- **`System\CurrentControlSet\Services\Dnscache\Parameters \DomainNameDevolutionLevel`**
  - Wenn nicht gesetzt, verwenden Sie die Stufe von 2 (Standard)
  - Wenn der Wert auf `3` oder höher gesetzt ist, verwenden Sie den Wert, um den Wert festzulegen

Wenn Sie die Devolution deaktivieren oder Ihre Devolutionseinstellungen auf eine höhere Ebene ändern, enthält der `System\CurrentControlSet\Services\Tcpip\Parameters \SearchList`-Registrierungsschlüssel immer noch die Suffixe, die zuvor hinzugefügt wurden. Sie werden nicht automatisch entfernt. Sie können die Liste manuell aktualisieren, oder Sie können die Liste löschen und Ihren Agenten den Vorgang zur Einrichtung der neuen Liste durchführen lassen.

> **Note**
>
> Um die DNS-Suffixliste aus der Registrierung zu löschen, können Sie den folgenden Befehl ausführen.
>
> ```
> PS C:\> Invoke-CimMethod -ClassName Win32_NetworkAdapterConfiguration -
> MethodName "SetDNSSuffixSearchOrder" -Arguments @{ DNSDomainSuffixSearchOrder =
>  $null } | Out-Null
> ```

Devolutionsbeispiele

Die folgenden Beispiele zeigen die Entwicklung von Domain-Namen während des Übertragungsprozesses.

`corp.example.com`

- Fährt fort zu `example.com`

`locale.region.corp.example.com`

1. Fährt fort zu `region.corp.example.com`
2. Fährt fort zu `corp.example.com`
3. Fährt fort zu `example.com`

`locale.region.corp.example.com` mit einer Einstellung von `DomainNameDevolutionLevel=3`

1. Fährt fort zu `region.corp.example.com`
2. Fährt fort zu `corp.example.com` Der Fortschritt hört hier aufgrund der Ebeneneinstellung auf.

Benachrichtigungen von EC2-Windows-Start-Agenten abonnieren

Amazon SNS kann Sie benachrichtigen, wenn neue Versionen des EC2-Windows-Start-Agenten veröffentlicht werden. Führen Sie die folgenden Schritte durch, um diese Benachrichtigungen zu abonnieren.

EC2Config-Benachrichtigungen abonnieren

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Ändern Sie, falls erforderlich, die Region in der Navigationsleiste zu US East (N. Virginia). Sie müssen diese Region auswählen, da die SNS-Benachrichtigungen, die Sie abonnieren, in dieser Region erstellt wurden.
3. Wählen Sie im Navigationsbereich Subscriptions aus.
4. Wählen Sie Create subscription.
5. Führen Sie im Dialogfeld Create subscription Folgendes aus:

   a. Verwenden Sie für Thema-ARN den folgenden Amazon-Ressourcennamen (ARN), der zu dem Agenten passt, für den Sie Benachrichtigungen erhalten möchten:

      - EC2Launch v2:

        ```
        arn:aws:sns:us-east-1:309726204594:amazon-ec2launch-v2
        ```

      - EC2Launch oder EC2Config:

```
arn:aws:sns:us-east-1:801119661308:ec2-windows-ec2config
```

b. Wählen Sie unter Protocol die Option `Email` aus.

c. Geben Sie als Endpunkt die E-Mail-Adresse ein, an welche die Benachrichtigungen gesendet werden sollen.

d. Wählen Sie Create subscription.

6. Sie erhalten eine E-Mail, in der Sie aufgefordert werden, Ihr Abonnement zu bestätigen. Öffnen Sie die E-Mail und befolgen Sie die Anweisungen, um Ihr Abonnement abzuschließen.

Sobald eine neue Version des Staragenten veröffentlicht wird, senden wir den Abonnenten Benachrichtigungen. Wenn Sie diese Benachrichtigungen nicht mehr erhalten möchten, führen Sie die folgenden Schritte aus, um sich abzumelden.

So melden Sie sich von den Start-Agenten-Benachrichtigungen ab

1. Öffnen Sie die Amazon SNS-Konsole.
2. Wählen Sie im Navigationsbereich Subscriptions aus.
3. Wählen Sie das Abonnement und dann Actions (Aktionen), Delete subscriptions (Abonnements löschen) aus. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

Windows Service Administration für EC2Launch-v2- und EC2Config-Agents

Wenn Sie sich als Benutzer mit Administratorrechten bei Ihrer Instance angemeldet haben, können Sie die Start-Agenten von EC2Launch v2 und EC2Config genauso verwalten wie jeden anderen Windows-Service. EC2Launch v1 ist eine Reihe von PowerShell-Skripten, die standardmäßig über geplante Aufgaben verwaltet werden. Dieser Abschnitt behandelt die Verwaltung der Services für EC2Launch v2 und EC2Config.

Um aktualisierte Einstellungen auf Ihre Instance anzuwenden, können Sie den EC2Launch-v2-Agent oder den EC2Config-Sercicestart-Agent über die Microsoft Management Console (MMC)-Schnittstelle für Services beenden und neu starten. Ebenso müssen Sie bei der Installation einer neuen Version des Start-Agenten den Agenten zuerst beenden und ihn dann neu starten, wenn die Installation abgeschlossen ist.

> **Note**
>
> Sie müssen die MMC-Services-Oberfläche als Administrator öffnen, um diese Aktionen auswählen zu können. Dazu können Sie im Kontextmenü die Option Als Administrator ausführen auswählen. Gehen Sie alternativ wie folgt vor, um die Benutzeroberfläche über Ihre Tastatur zu öffnen:
>
> 1. Wählen Sie mit der `Tab`-Taste oder den Pfeiltasten im Menü Verwaltung den Menüpunkt Services aus.
> 2. Verwenden Sie die folgende Tastenkombination, um das Programm als Administrator zu öffnen: `Ctrl` + `Shift` + `Enter`.

In den folgenden Verfahren werden die Schritte zum Stoppen und Starten des Start-Agenten auf Ihrer Instance aufgeführt.

Start-Agenten stoppen

1. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
2. Wählen Sie im Windows-Startmenü die Option Verwaltungstools aus.
3. Öffnen Sie die Services-Konsole als Administrator, wie am Anfang dieses Abschnitts beschrieben.
4. Wählen Sie in der Liste der Services den Agenten aus, der auf Ihrer Instance ausgeführt wird (EC2Launch oder EC2Config) und wählen Sie dann im Menü Aktion die Option Anhalten aus. Alternativ können Sie das Kontextmenü verwenden, um den Agenten zu beenden.

Neustart des Start-Agenten

1. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
2. Wählen Sie im Windows-Startmenü die Option Verwaltungstools aus.
3. Öffnen Sie die Services-Konsole als Administrator, wie am Anfang dieses Abschnitts beschrieben.
4. Wählen Sie in der Liste der Services den Agenten aus, der auf Ihrer Instance ausgeführt wird (EC2Launch oder EC2Config), und wählen Sie dann im Menü Aktion die Option Start oder Neustart aus. Alternativ können Sie das Kontextmenü verwenden, um den Agenten zu beenden.

Wenn Sie weder die Konfigurationseinstellungen aktualisieren, Ihr eigenes AMI erstellen oder AWS Systems Manager verwenden müssen, können Sie den Start-Agenten löschen oder deinstallieren.

Löschen

Durch das Löschen eines Services wird der Registrierungsunterschlüssel entfernt.

Deinstallieren

Durch die Deinstallation eines Services werden die Dateien, der Registrierungsunterschlüssel und alle Shortcuts zum Service entfernt.

Start-Agenten löschen

1. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
2. Starten Sie ein Fenster der Windows-Eingabeaufforderung.
3. Führen Sie einen der folgenden Befehle aus, um den Start-Agenten zu löschen.
   - Führen Sie den folgenden Befehl aus, um EC2Launch oder EC2Launch v2 zu löschen:

     ```
     sc delete ec2launch
     ```

   - Führen Sie den folgenden Befehl aus, um den EC2Config-Service zu löschen:

     ```
     sc delete ec2config
     ```

Start-Agenten deinstallieren

1. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
2. Wählen Sie im Windows-Startmenü Windows System und dann Systemsteuerung.
3. Wählen Sie Programme und Feature, um die Liste der Programme zu öffnen, die auf Ihrer Instance installiert sind.
4. Wählen Sie Ihren Start-Agenten aus der Liste aus (Amazon EC2Launch oder EC2ConfigService) und wählen Sie anschließend im Menü Datei die Option Deinstallieren. Alternativ können Sie auch das Kontextmenü verwenden.

> **Note**
>
> In der Spalte Version können Sie sehen, welche Start-Agent-Version installiert ist.

Den EC2Launch-v2-Agenten verwenden, um Aufgaben während des Starts einer EC2-Windows-Instance auszuführen

Alle unterstützten Instances von Amazon EC2, die von AWS-Windows-Server-2022- und Windows-Server-2025-AMIs gestartet werden, enthalten standardmäßig den EC2Launch-v2-Start-Agenten (`EC2Launch.exe`). Darüber hinaus bieten wir AMIs für Windows Server 2016 und 2019 an, bei denen EC2Launch v2 als Standard-Launch-Agent installiert ist. Diese AMIs werden zusätzlich zu den AMIs für Windows Server 2016 und 2019 bereitgestellt, die EC2Launch v1 enthalten. Sie können nach Windows-AMIs suchen, die standardmäßig EC2Launch v2 enthalten, indem Sie in der Suche auf der Seite AMIs in der Amazon-EC2-Konsole das folgende Präfix eingeben: `EC2LaunchV2-Windows_Server-*`.

Einen Vergleich der Feature der Start-Agent-Version finden Sie unter Amazon-EC2-Start-Agenten vergleichen.

EC2Launch v2 ist ein Service, der während des Instance-Startups Aufgaben ausführt und ausgeführt wird, wenn eine Instance gestoppt und später gestartet oder neu gestartet wird. Außerdem kann EC2Launch v2 nach Bedarf Aufgaben ausführen. Einige dieser Aufgaben sind automatisch aktiviert, während andere manuell aktiviert werden müssen. Der EC2Launch v2-Service unterstützt alle Features von EC2Config und EC2Launch.

Dieser Service verwendet eine Konfigurationsdatei zur Steuerung seines Betriebs. Sie können die Konfigurationsdatei entweder mit einem grafischen Tool aktualisieren oder direkt als einzelne .yml-Datei () bearbei (`agent-config.yml`). Weitere Informationen zu den Datei-Speicherorten finden Sie unter EC2Launch v2-Verzeichnisstruktur.

EC2Launch v2 veröffentlicht Windows-Ereignisprotokolle, um Ihnen bei der Fehlerbehebung und beim Festlegen von Auslösern zu helfen. Weitere Informationen finden Sie unter Windows-Ereignisprotokolle.

Unterstützte OS-Versionen

Der EC2Launch-v2-Agent unterstützt die folgenden Versionen für das Betriebssystem Windows Server (OS):

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019 (Langzeitwartungskanal und halbjährlicher Kanal)
- Windows Server 2016

Aufgaben, die standardmäßig ausgeführt werden

Der EC2Launch-v2-Agent führt die folgenden Aufgaben beim ersten Starten einer Instance standardmäßig nur einmal aus. Die Aufgaben werden in der Reihenfolge organisiert, in der sie in der Startphase ausgeführt werden.

`Boot`-Phase

- extendRootPartition

`PreReady`-Phase

- activateWindows
- setDnsSuffix
- setAdminAccount
- setWallpaper

`PostReady`-Phase

- startSsm

Konzepte für EC2Launch v2

Die folgenden Konzepte sind nützlich für die Verwendung von EC2Launch v2.

agent-config

`agent-config` ist eine Datei, die sich im Konfigurationsordner für EC2Launch v2 befindet. Diese umfasst die Konfiguration für die Start-, Netzwerk-, PreReady- und PostReady-Stufen. Diese Datei wird verwendet, um die Instance-Konfiguration für Aufgaben festzulegen, die beim ersten oder späteren Start des AMI ausgeführt werden sollen.

Standardmäßig wird bei der EC2Launch v2-Installation eine `agent-config`-Datei installiert, die empfohlene Konfigurationen enthält, die in Standard-Amazon-Windows-AMIs verwendet werden. Sie können die Konfigurationsdatei aktualisieren, um die Standardstartumgebung für Ihr AMI zu ändern, die EC2Launch v2 angibt. Weitere Informationen zu den Datei-Speicherorten finden Sie unter EC2Launch v2-Verzeichnisstruktur.

Häufigkeit

Die Frequenz der Aufgaben bestimmt, wann Aufgaben ausgeführt werden sollen, abhängig vom Startkontext. Die meisten Aufgaben haben nur eine zulässige Frequenz. Sie können eine Frequenz für `executeScript`-Aufgaben festlegen.

Sie können die folgenden Frequenzen in der Aufgabenkonfiguration in EC2Launch v2 anzeigen.

- Einmal – Die Aufgabe wird einmal ausgeführt, wenn das AMI zum ersten Mal gestartet wurde (Sysprep abgeschlossen).
- Immer – Die Aufgabe wird jedes Mal ausgeführt, wenn der Startagent ausgeführt wird. Der Launch-Agent wird ausgeführt, wenn:
  - eine Instance startet oder neu startet
  - der EC2Launch-Service läuft
  - `EC2Launch.exe run` wird aufgerufen

Stufe

Eine Stufe ist eine logische Gruppierung von Aufgaben, die vom EC2Launch-v2-Agenten ausgeführt werden. Einige Aufgaben können nur in einer bestimmten Phase ausgeführt werden. Andere können in mehreren Phasen ausgeführt werden. Bei der Verwendung von `agent-config.yml` müssen Sie eine Liste von Stufen und eine Liste von Aufgaben angeben, die innerhalb jeder Stufe ausgeführt werden sollen.

Der Service führt die Phasen in der folgenden Reihenfolge aus:

Phase 1: Boot

Phase 2: Netzwerk

Phase 3: PreReady

Windows ist bereit

Nach Abschluss der PreReady-Phase sendet der Service die `Windows is ready`-Nachricht an die Amazon-EC2-Konsole.

Stufe 4: PostReady

Benutzerdaten werden während der PostReady-Stufe ausgeführt. Einige Skriptversionen werden vor der `agent-config.yml`-Datei in der PostReady-Stufe ausgeführt, andere danach, wie folgt:

Vor `agent-config.yml`

- YAML-Benutzerdaten-Version 1.1
- XML-Benutzerdaten

Nach `agent-config.yml`

- YAML-Benutzerdatenversion 1.0 (Legacy-Version für Abwärtskompatibilität)

Beispiele für Phasen und Aufgaben finden Sie unter Beispiel: `agent-config.yml`.

Wenn Sie Benutzerdaten verwenden, müssen Sie eine Liste von Aufgaben angeben, die der Startagent ausführen soll. Die Phase ist impliziert. Beispiele für Aufgaben finden Sie unter Beispiel: Benutzerdaten.

EC2Launch v2 führt die Liste der Aufgaben in der Reihenfolge aus, die Sie in `agent-config.yml` und in den Benutzerdaten angeben. Die Phasen werden der Reihe nach ausgeführt. Die nächste Phase beginnt, nachdem die vorherige Phase abgeschlossen ist. Aufgaben werden nacheinander ausgeführt.

Aufgabe

Sie können eine Aufgabe aufrufen, um eine Aktion für eine Instance durchzuführen. Sie können Aufgaben in der `agent-config.yml`-Datei oder über Benutzerdaten konfigurieren. Eine Liste der verfügbaren Aufgaben für EC2Launch v2 finden Sie unter EC2Launch v2-Aufgaben. Schemata und Einzelheiten zur Aufgabenkonfiguration finden Sie unter Aufgabenkonfiguration in EC2Launch v2.

Benutzerdaten

Benutzerdaten sind Daten, die beim Starten einer Instance konfiguriert werden können. Sie können Benutzerdaten aktualisieren, um dynamisch zu ändern, wie benutzerdefinierte AMIs oder Schnellstart-AMIs konfiguriert werden. EC2Launch-v2-unterstützt eine Eingabelänge von 60 KB. Benutzerdaten beinhalten nur die UserData-Phase und werden daher nach der `agent-config`-Datei ausgeführt. Sie können Benutzerdaten eingeben, wenn Sie eine Instance mit dem Launch Instance Wizard starten oder Sie können Benutzerdaten über die EC2-Konsole ändern. Weitere Informationen zum Arbeiten mit Benutzerdaten finden Sie unter Wie Amazon EC2 mit Benutzerdaten für Windows-Instances umgeht.

Überblick über EC2Launch-v2-Aufgaben

EC2Launch v2 kann bei jedem Start die folgenden Aufgaben ausführen:

- Einrichten eines neuen und optional angepassten Hintergrundbildes, das Informationen über die Instance wiedergibt.
- Festlegen der Attribute für das Administratorkonto, das auf dem lokalen Computer erstellt wird.
- Hinzufügen von DNS-Suffixen zur Liste der Suffixe. Nur Suffixe, die noch nicht vorhanden sind, werden der Liste hinzugefügt.
- Festlegen von Laufwerkbuchstaben für zusätzliche Volumes und deren Erweiterung, um den verfügbaren Speicherplatz zu nutzen.
- Schreiben Sie Dateien aus der Konfiguration auf die Festplatte.
- Führen Sie die in der EC2Launch-v2-Konfigurationsdatei angegebenen Skripts oder von `user-data` aus. Skripts von `user-data` können Klartext oder gezippt sein und als Base64-Format bereitgestellt werden.
- Führen Sie ein Programm mit angegebenen Argumenten aus.
- Erstellen des Computer-Namens.
- Senden von Instance-Informationen an die Amazon EC2-Konsole.
- Senden Sie den Fingerabdruck des RDP-Zertifikats an die Amazon-EC2-Konsole.
- Erweiterung der Betriebssystempartition, um den gesamten nicht partitionierten Speicherplatz mit einzuschließen.
- Führen Sie Benutzerdaten aus. Weitere Informationen zur Angabe von Benutzerdaten finden Sie unter Aufgabenkonfiguration in EC2Launch v2.
- Legen Sie nicht-persistente statische Routen fest, um den Metadatendienst und die AWS KMS-Server zu erreichen.
- Festlegen von Nicht-Boot-Partitionen auf `mbr` oder `gpt`.
- Starten Sie den Systems-Manager-Service nach Sysprep.
- Optimieren der ENA-Einstellungen.
- Aktivieren von OpenSSH für spätere Windows-Versionen.
- Aktivieren von Jumbo-Frames.
- Einstellen von Sysprep so ein, dass es mit EC2Launch v2 ausgeführt wird.
- Veröffentlichen von Windows-Ereignisprotokollen.

EC2Launch v2-Verzeichnisstruktur

EC2Launch v2 sollte in den folgenden Verzeichnissen installiert werden:

- Service-Binärdateien: `%ProgramFiles%\Amazon\EC2Launch`
- Servicedaten (Einstellungen, Protokolldateien und Statusdateien): `%ProgramData%\Amazon\EC2Launch`

> **Note**
>
> Windows blendet Dateien und Ordner unter standardmäßig au `C:\ProgramData`. Um die EC2Launch v2-Verzeichnisse und -Dateien anzuzeigen, müssen Sie entweder den Pfad im Windows Explorer eingeben oder die Ordnereigenschaften so ändern, dass ausgeblendete Dateien und Ordner angezeigt werden.

Das `%ProgramFiles%\Amazon\EC2Launch`-Verzeichnis enthält Binärdateien und unterstützende Bibliotheken. Es enthält die folgenden Unterverzeichnisse:

- `settings`
  - `EC2LaunchSettingsUI.exe` – Benutzeroberfläche zum Ändern der `agent-config.yml`-Datei
  - `YamlDotNet.dll` – DLL zur Unterstützung einiger Vorgänge in der Benutzeroberfläche
- `tools`
  - `ebsnvme-id.exe` – Tool zum Überprüfen der Metadaten der EBS-Volumes auf der Instance
  - `AWSAcpiSpcrReader.exe` – Tool zur Bestimmung des korrekten zu verwendenden COM-Ports
  - `EC2LaunchEventMessage.dll` – DLL zur Unterstützung der Windows-Ereignisprotokollierung für EC2Launch
- `service`
  - `EC2LaunchService.exe` – Ausführbare Windows-Servicedatei, die gestartet wird, wenn der Launch-Agent als Service ausgeführt wird.
- `EC2AgentTelemetry.dll` – DLL zur Unterstützung der EC2-Agenten-Telemetrie
- `EC2Launch.exe` – zentrale ausführbare EC2Launch-Datei
- `EC2LaunchAgentAttribution.txt` – Zuweisung für Code, der innerhalb von EC2 Launch verwendet wird

Das Verzeichnis `%ProgramData%\Amazon\EC2Launch` enthält die folgenden Unterverzeichnisse. Alle von dem Service erzeugten Daten, einschließlich Protokolle, Konfiguration und Status, werden in diesem Verzeichnis gespeichert.

- `config` – Konfiguration

  Die Servicekonfigurationsdatei wird in diesem Verzeichnis als gespeicher `agent-config.yml`. Diese Datei kann aktualisiert werden, um Standardaufgaben zu ändern, hinzuzufügen oder zu entfernen, die von dem Service ausgeführt werden. Die Berechtigung zum Erstellen von Dateien in diesem Verzeichnis ist auf das Administratorkonto beschränkt, um die Eskalation von Berechtigungen zu verhindern.

- `log` – Instance-Protokolle

  Protokolle für den Service (`agent.log`), die Konsole (`console.log`), die Leistung (`bench.log`), Fehler (`err.log`) und Telemetrie (`telemetry.log`) werden in diesem Verzeichnis gespeichert. Protokolldateien werden bei nachfolgenden Ausführungen des Services angehängt.

- `state` – Servicestatusdaten

  Hier wird der Status gespeichert, mit dem der Service ermittelt wird, welche Aufgaben ausgeführt werden sollen. Es gibt eine `.run-once`-Datei, die angibt, ob der Service bereits nach Sysprep ausgeführt wurde (so dass Aufgaben mit der Häufigkeit "einmal" bei der nächsten Ausführung übersprungen werden). Dieses Unterverzeichnis enthält ein `state.json` und `previous-state.json`, um den Status jeder Aufgabe zu verfolgen.

- `sysprep` – Sysprep

  Dieses Verzeichnis enthält Dateien, die verwendet werden, um zu bestimmen, welche Operationen von Sysprep ausgeführt werden sollen, wenn ein angepasstes Windows-AMI erstellt wird, das wiederverwendet werden kann.

- `wallpaper` – Hintergrundbild

  Diese Hintergrundbilder werden in diesem Verzeichnis gespeichert.

Telemetrie

Bei Telemetrie handelt es sich um zusätzliche Informationen, die AWS dabei helfen, Ihre Anforderungen besser zu verstehen, Probleme zu diagnostizieren und Features bereitzustellen, um Ihre Erfahrung mit AWS-Services zu verbessern.

EC2Launch v2-Version `2.1.592` und später sammeln Telemetrie, wie Nutzungsmetriken und Fehler. Diese Daten werden von der Amazon-EC2-Instance erfasst, auf der EC2Launch v2 ausgeführt wird. Dies umfasst alle Windows-AMIs, die gehören AWS.

EC2Launch v2 bietet folgende Telemetrie-Typen:

- Nutzungsinformationen – Agent-Befehle, Installationsmethode und geplante Ausführungsfrequenz.
- Fehler und Diagnoseinformationen – Agent-Installation-Fehlercodes, Ausführungs-Fehlercodes und Fehleraufrufstapel.

Beispiele für gesammelte Daten aus den Versionen 2.0.592 bis 2.1.1:

```
2025/07/18 22:38:52Z: EC2LaunchTelemetry: IsTelemetryEnabled=true
2025/07/18 22:38:52Z: EC2LaunchTelemetry: AgentOsArch=windows_amd64
2025/07/18 22:38:52Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2025/07/18 22:38:52Z: EC2LaunchTelemetry: AgentCommandErrorCode=0
2025/07/18 22:38:52Z: EC2LaunchTelemetry: AdminPasswordTypeCode=0
2025/07/18 22:38:52Z: EC2LaunchTelemetry: IpConflictDetectionCode=0
2025/07/18 22:38:52Z: EC2LaunchTelemetry: AgentErrorLocation=addroutes.go:49
```

Ab Version 2.2.63 werden die Telemetriedaten des EC2-Agenten als JSON-Objekt formatiert:

```
{"type":"EC2AgentTelemetry","agentId":"WindowsLaunchAgentV2" ... }
```

Die Telemetrie ist standardmäßig aktiviert. Sie können die Telemetriesammlung jederzeit deaktivieren.

Deaktivieren der Telemetrie auf einer Instance

Um die Telemetrie für eine einzelne Instance zu deaktivieren, können Sie entweder eine Systemumgebungsvariable festlegen oder die Installation mit dem MSI ändern.

Um Telemetrie durch Festlegen einer Systemumgebungsvariablen zu deaktivieren, führen Sie den folgenden Befehl als Administrator aus.

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Um die Telemetrie mithilfe der MSI zu deaktivieren, führen Sie den folgenden Befehl aus, nachdem Sie die MSI-Datei herunterladen.

```
msiexec /i ".\AmazonEC2Launch.msi" Remove="Telemetry" /q
```

Weitere Themen für EC2Launch v2

- Installieren der neuesten Version von EC2Launch v2
- EC2Launch-v2-Einstellungen für Windows-Instances konfigurieren
- Aufgabendefinitionen für EC2Launch v2-Startaufgaben
- Problembehandlung beim EC2Launch-v2-Agent
- EC2Versionsverläufe von Launch v2

Installieren der neuesten Version von EC2Launch v2

Sie können eine der folgenden Methoden verwenden, um den EC2Launch v2-Agenten auf Ihrer EC2-Instance zu installieren:

- Laden Sie den Agenten von Amazon S3 herunter und installieren Sie ihn mit Windows PowerShell. Download-URLs finden Sie unter EC2Launch v2 kann auf Amazon S3 heruntergeladen werden.
- Installation mit SSM-Distributor.
- Installation von einer EC2-Image-Builder-Komponente, wenn Sie ein benutzerdefiniertes Image erstellen.
- Starten Sie Ihre Instance über ein AMI, auf dem EC2Launch v2 vorinstalliert ist.

> **Warning**
>
> AmazonEC2Launch.msi deinstalliert frühere Versionen der EC2-Startservices, z. B. EC2Launch (v1) oder EC2Config.

Wählen Sie für die Installationsschritte die Registerkarte aus, die Ihrer bevorzugten Methode entspricht.

PowerShell

Um die neueste Version des EC2Launch v2-Agenten mit Windows PowerShell zu installieren, führen Sie die folgenden Schritte aus.

1. Erstellen Sie Ihr lokales Verzeichnis.

```
New-Item -Path "$env:USERPROFILE\Desktop\EC2Launchv2" -ItemType Directory
```

2. Legen Sie die URL für Ihren Download-Speicherort fest. Führen Sie den folgenden Befehl mit der von Ihnen verwendeten Amazon-S3-URL aus. Download-URLs finden Sie unter EC2Launch v2 kann auf Amazon S3 heruntergeladen werden

```
$Url = "Amazon S3 URL/AmazonEC2Launch.msi"
```

3. Verwenden Sie den folgenden zusammengesetzten Befehl, um den Agenten herunterzuladen und die Installation auszuführen

```
$DownloadFile = "$env:USERPROFILE\Desktop\EC2Launchv2\" + $(Split-Path -Path
 $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadFile
msiexec /i "$DownloadFile"
```

> **Note**
>
> Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 oder früher verwenden, muss TLS 1.2 möglicherweise für Ihr PowerShell-Terminal aktiviert werden. Sie können TLS 1.2 für die aktuelle PowerShell-Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

4. Der msiexec-Befehl installiert EC2Launch v2 auf Windows-Server-Instances am folgenden Speicherort: `%ProgramFiles%\Amazon\EC2Launch`. Um zu überprüfen, ob die Installation ausgeführt wurde, können Sie das lokale Dateisystem auf Ihrer Instance überprüfen.

AWS Systems Manager Distributor

Informationen zur Konfiguration automatischer Updates für EC2Launch v2 mit AWS Systems Manager Quick Setup finden Sie unter Automatische Installation und Aktualisierung mit Distributor Quick Setup.

Sie können auch eine einmalige Installation des`AWSEC2Launch-Agent`-Pakets vom AWS Systems Manager-Distributor durchführen. Anweisungen zum Installieren eines Pakets vom Systems Manager Distributor finden Sie unter Installieren oder Aktualisieren von Paketen im AWS Systems Manager-Benutzerhandbuch.

EC2 Image Builder component

Sie können die Komponente `ec2launch-v2-windows` installieren, wenn Sie ein benutzerdefiniertes Image mit EC2 Image Builder erstellen. Anweisungen zum Erstellen eines benutzerdefinierten Image mit EC2 Image Builder finden Sie unterErstellen einer Image-Pipeline mithilfe des EC2-Image-Builder-Konsolenassistenten im Benutzerhandbuch für EC2 Image Builder.

AMI

EC2Launch v2 ist auf AMIs für Betriebssysteme mit Windows Server 2022 und höher standardmäßig vorinstalliert:

- Windows_Server-*`version`*-English-Full-Base
- Windows_Server-*`version`*-English-Core-Base
- Windows_Server-*`version`*-English-Core-EKS_Optimized
- Windows Server-*`version`*-AMIs mit allen anderen Sprachen
- Windows Server *`version`* AMIs mit SQL installiert

EC2Launch v2 ist ebenfalls auf den folgenden Windows-Server-AMIs vorinstalliert. Sie können diese AMIs über die Amazon-EC2-Konsole oder mithilfe des folgenden Suchpräfixes finden: `EC2LaunchV2-` in der AWS CLI.

- EC2LaunchV2-Windows_Server-2019-English-Core-Base
- EC2LaunchV2-Windows_Server-2019-English-Full-Base
- EC2LaunchV2-Windows_Server-2016-English-Core-Base
- EC2LaunchV2-Windows_Server-2016-English-Full-Base

Automatische Installation und Aktualisierung von EC2Launch v2 mit AWS Systems Manager Distributor Quick Setup

Mit AWS Systems Manager Distributor Quick Setup können Sie automatische Updates für EC2Launch v2 einrichten. Der folgende Prozess richtet eine Systems Manager Association auf

Ihrer Instance ein, die den EC2Launch-v2-Agenten automatisch mit einer von Ihnen angegebenen Frequenz aktualisiert. Die Zuordnung, die der Distributor Quick Setup erstellt, kann Instances innerhalb eines AWS-Konto und Region oder Instances innerhalb einer AWS-Organisation umfassen. Weitere Informationen finden Sie unter Anleitung: Erstellen und Konfigurieren einer Organisation im Benutzerhandbuch für AWS Organizations.

Stellen Sie vor Beginn sicher, dass Ihre Instances alle Voraussetzungen erfüllen.

Voraussetzungen

Um automatische Updates mit Distributor Quick Setup einzurichten, müssen Ihre Instances die folgenden Voraussetzungen erfüllen.

- Sie haben mindestens eine laufende Instance, die EC2Launch v2 unterstützt. Sehen Sie unterstützte Betriebssysteme für EC2Launch v2.
- Sie haben die Systems-Manager-Einrichtungsaufgaben auf Ihren Instances ausgeführt. Weitere Informationen finden Sie unter System Manager einrichten im AWS Systems Manager-Benutzerhandbuch.
- EC2Launch v2 muss der einzige Start-Agent sein, der auf Ihrer Instance installiert ist. Wenn Sie mehr als einen Start-Agenten installiert haben, schlägt die Konfiguration der Distributor Quick Setup fehl. Bevor Sie EC2Launch v2 mit einem Distributor Quick Setup konfigurieren, deinstallieren Sie EC2Config- oder EC2Launch-v1-Start-Agenten, falls diese vorhanden sind.

Konfigurieren von Distributor Quick Setup für EC2Launch v2

Um eine Konfiguration für EC2Launch v2 mit Distributor Quick Setup zu erstellen, verwenden Sie die folgenden Einstellungen, wenn Sie die Schritte für die Bereitstellung des Distributor-Pakets abschließen:

- Softwarepakete: Amazon EC2Launch-v2-agent.
- Aktualisierungshäufigkeit: Wählen Sie eine Frequenz aus der Liste aus.
- Ziele: Wählen Sie aus den verfügbaren Bereitstellungsoptionen.

Um den Status Ihrer Konfiguration zu überprüfen, navigieren Sie zur Registerkarte Konfigurationen des Systems Manager Quick Setup in der AWS-Managementkonsole.

1. Öffnen Sie die AWS Systems Manager-Konsole unter https://console.aws.amazon.com/systems-manager/.

2. Wählen Sie im Navigationsbereich Quick Setup aus.
3. Wählen Sie auf der Registerkarte Konfigurationen die Zeile aus, die mit der von Ihnen erstellten Konfiguration verknüpft ist. Die Registerkarte Konfigurationen listet Ihre Konfigurationen auf und enthält eine Zusammenfassung der wichtigsten Details wie Region, Bereitstellungsstatus und Zuordnungsstatus.

   > **Note**
   >
   > Der Zuordnungsname für jede EC2Launch-v2-Verteilerkonfiguration beginnt mit dem folgenden Präfix: `AWS-QuickSetup-Distributor-EC2Launch-Agent-`.

4. Um Details anzuzeigen, wählen Sie die Konfiguration aus und klicken Sie auf Details anzeigen.

Weitere Informationen und Schritte zur Fehlerbehebung finden Sie unter Problembehandlung bei Ergebnissen von Quick Setup im AWS Systems Manager-Benutzerhandbuch.

EC2Launch v2 kann auf Amazon S3 heruntergeladen werden

Um die neueste Version von EC2Launch v2 zu installieren, laden Sie die Installationsdatei vom folgenden Standort herunter:

- https://s3.amazonaws.com/amazon-ec2launch-v2/windows/amd64/latest/AmazonEC2Launch.msi

Installationsoptionen konfigurieren

Wenn Sie EC2Launch v2 installieren oder aktualisieren, können Sie Installationsoptionen mit dem Installationsdialogfeld von EC2Launch v2 oder mit dem msiexec-Befehl in einer Befehlszeilen-Shell konfigurieren.

Wenn das EC2Launch-v2-Installationsprogramm zum ersten Mal auf einer Instance ausgeführt wird, initialisiert es die Einstellungen des Startagenten auf Ihrer Instance wie folgt:

- Es erstellt den lokalen Pfad und schreibt die Datei des Startagenten dorthin. Dies wird manchmal als Neuinstallation bezeichnet.
- Es erstellt die Umgebungsvariable `EC2LAUNCH_TELEMETRY`, sofern diese noch nicht vorhanden ist, und legt sie basierend auf Ihrer Konfiguration fest.

Wählen Sie für Konfigurationsdetails die Registerkarte aus, die der von Ihnen verwendeten Konfigurationsmethode entspricht.

Amazon EC2Launch Setup dialog

Wenn Sie EC2Launch v2 installieren oder aktualisieren, können Sie die folgenden Installationsoptionen über den EC2Launch-v2-Installationsdialog konfigurieren.

Optionen der Grundlegende Installation

Telemetrie senden

Wenn Sie dieses Feature in den Einrichtungsdialog aufnehmen, legt das Installationsprogramm die Umgebungsvariable `EC2LAUNCH_TELEMETRY` auf einen Wert von 1 fest. Wenn Sie Telemetrie senden deaktivieren, legt das Installationsprogramm die Umgebungsvariable auf den Wert `0` fest.

Wenn der EC2Launch-v2-Agent ausgeführt wird, liest er die Umgebungsvariable `EC2LAUNCH_TELEMETRY`, um festzustellen, ob Telemetriedaten hochgeladen werden sollen. Wenn der Wert gleich 1 ist, werden die Daten hochgeladen. Andernfalls wird der Upload nicht durchgeführt.

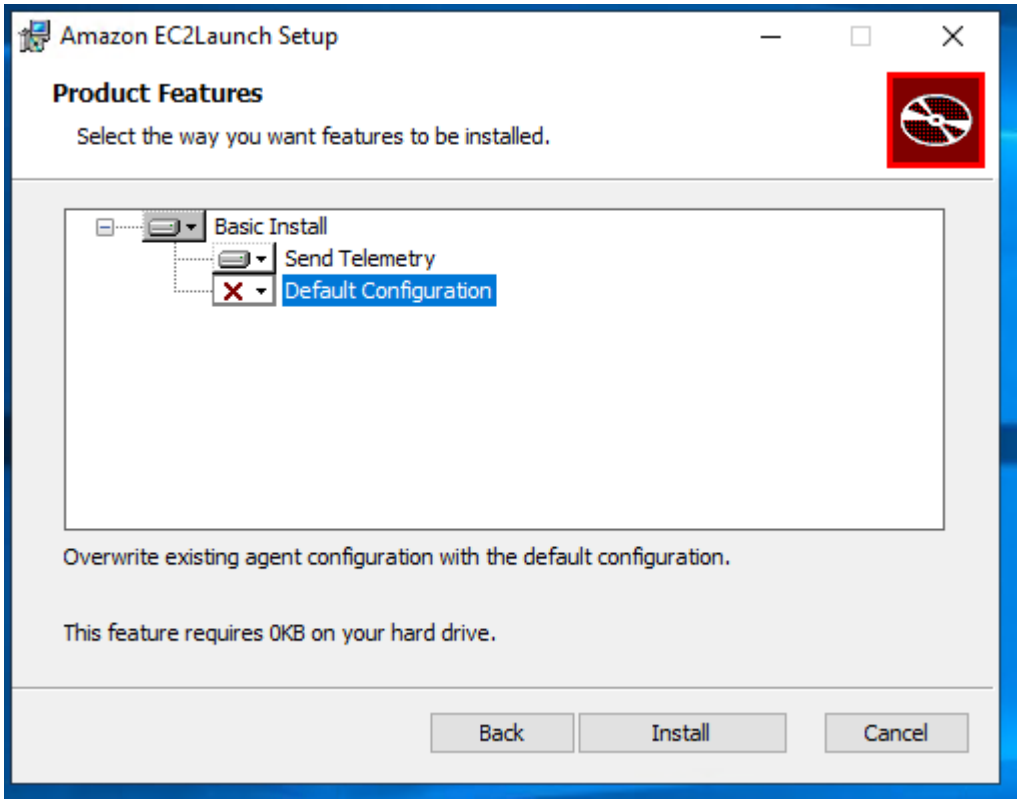
Standardkonfiguration

Die Standardkonfiguration für EC2Launch v2 besteht darin, den lokalen Startagenten zu überschreiben, falls dieser bereits vorhanden ist. Wenn Sie zum ersten Mal eine Installation auf einer Instance ausführen, wird in der Standardkonfiguration eine Neuinstallation durchgeführt. Wenn Sie die Standardkonfiguration bei der Erstinstallation deaktivieren, schlägt die Installation fehl.

Wenn Sie die Installation auf der Instance erneut ausführen, können Sie die Standardkonfiguration deaktivieren, um ein Upgrade durchzuführen, bei dem die `%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`-Datei nicht ersetzt wird.

Beispiel: Upgrade von EC2Launch v2 mit Telemetrie

Das folgende Beispiel zeigt das EC2Launch-v2-Einrichtungsdialog, das zum Aktualisieren der aktuellen Installation und zum Aktivieren der Telemetrie konfiguriert ist. Diese Konfiguration führt eine Installation durch, ohne die Agent-Konfigurationsdatei zu ersetzen, und legt die Umgebungsvariable `EC2LAUNCH_TELEMETRY` auf den Wert 1 fest.



Command line

Wenn Sie EC2Launch v2 installieren oder aktualisieren, können Sie die folgenden Installationsoptionen mit dem msiexec-Befehl in einer Befehlszeilen-Shell konfigurieren.

`ADDLOCAL`-Parameterwerte

Grundlegend (erforderlich)

Installieren Sie den Start-Agenten. Wenn dieser Wert im `ADDLOCAL`-Parameter nicht vorhanden ist, wird die Installation beendet.

Bereinigen

Wenn Sie den `Clean`-Wert in den `ADDLOCAL`-Parameter einbeziehen, schreibt das Installationsprogramm die Agent-Konfigurationsdatei an den folgenden Speicherort: `%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`. Wenn die Agent-Konfigurationsdatei bereits vorhanden ist, wird die Datei überschrieben.

Wenn Sie den `Clean`-Wert im `ADDLOCAL`-Parameter weglassen, führt das Installationsprogramm ein Upgrade durch, das die Agent-Konfigurationsdatei nicht ersetzt.

Telemetrie

Wenn Sie den `Telemetry`-Wert in den `ADDLOCAL`-Parameter einbeziehen, legt das Installationsprogramm die Umgebungsvariable `EC2LAUNCH_TELEMETRY` auf den Wert 1 fest.

Wenn Sie den `Telemetry`-Wert in den `ADDLOCAL`-Parameter einbeziehen, legt das Installationsprogramm die Umgebungsvariable auf den Wert `0` fest.

Wenn der EC2Launch-v2-Agent ausgeführt wird, liest er die Umgebungsvariable `EC2LAUNCH_TELEMETRY`, um festzustellen, ob Telemetriedaten hochgeladen werden sollen. Wenn der Wert gleich 1 ist, werden die Daten hochgeladen. Andernfalls wird der Upload nicht durchgeführt.

Beispiel: EC2Launch v2 mit Telemetrie installieren

```
& msiexec /i "C:\Users\Administrator\Desktop\EC2Launchv2\AmazonEC2Launch.msi"
 ADDLOCAL="Basic,Clean,Telemetry" /q
```

Prüfen der Version EC2Launch v2

Überprüfen Sie mithilfe eines der folgenden Verfahren, welche Version von EC2Launch v2 in Ihren Instances installiert ist.

PowerShell

Überprüfen Sie die installierte Version von EC2Launch v2 mit Windows PowerShell wie folgt.

1. Starten Sie eine Instance von Ihrem AMI und stellen Sie eine Verbindung damit her.
2. Führen Sie den folgenden PowerShell-Befehl zur Prüfung der installierten Version von EC2Launch v2 aus:

   ```
   & "C:\Program Files\Amazon\EC2Launch\EC2Launch.exe" version
   ```

Windows Control Panel

Überprüfen Sie die installierte Version von EC2Launch v2 in der Windows-Systemsteuerung wie folgt.

1. Starten Sie eine Instance von Ihrem AMI und stellen Sie eine Verbindung damit her.
2. Öffnen Sie die Windows-Systemsteuerung und wählen Sie Programme und Features.
3. Suchen Sie in der Liste mit den installierten Programmen nach `Amazon EC2Launch`. Die Versionsnummer wird in der Spalte Version angegeben.

Die neuesten Updates für die AWS-Windows-AMIs finden Sie im Windows-AMI-Versionsverlauf in der AWS-Windows-AMI-Referenz.

Die neueste Version von EC2Launch v2 finden Sie unter EC2Versionsverlauf für Version 2 starten.

Sie können benachrichtigt werden, wenn neue Versionen des EC2Launch v2-Services veröffentlicht werden. Weitere Informationen finden Sie unter Benachrichtigungen von EC2-Windows-Start-Agenten abonnieren.

EC2Launch-v2-Einstellungen für Windows-Instances konfigurieren

Dieser Abschnitt enthält Informationen zum Konfigurieren von Einstellungen für EC2Launch v2.

Zu den Themen gehören:

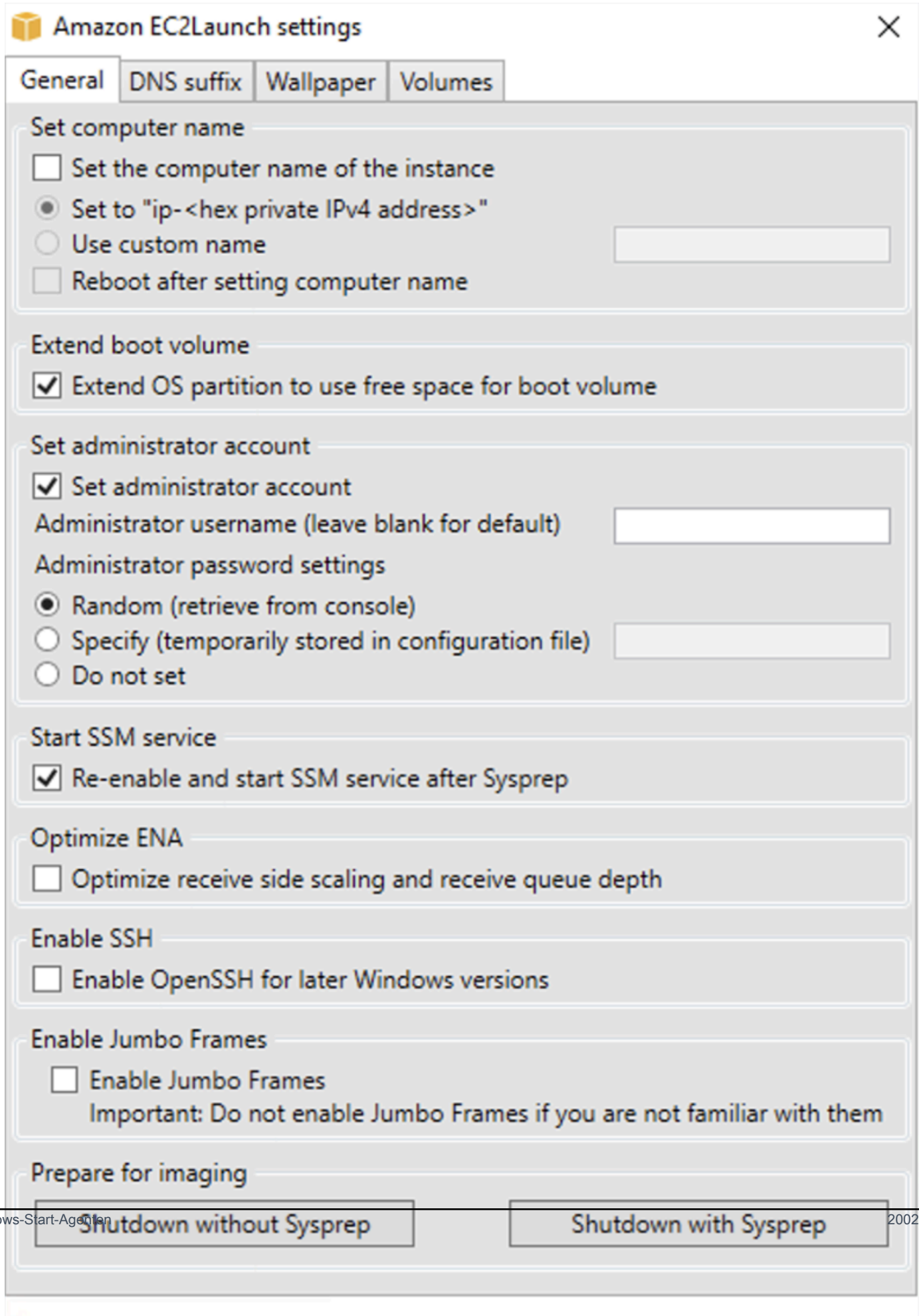
- Ändern der Einstellungen mithilfe des Dialogfelds für EC2Launch v2-Einstellungen
- Konfigurieren von EC2Launch v2 mit der CLI
- Aufgabenkonfiguration in EC2Launch v2
- Exit-Codes und Neustarts für EC2Launch v2
- EC2Launch v2 und Sysprep

Ändern der Einstellungen mithilfe des Dialogfelds für EC2Launch v2-Einstellungen

Der folgende Vorgang beschreibt, wie die Einstellungen anhand des Dialogfelds für EC2Launch v2-Einstellungen aktiviert bzw. deaktiviert werden.

> **Note**
>
> Wenn Sie benutzerdefinierte Aufgaben in der Datei agent-config.yml falsch konfigurieren und versuchen, das Dialogfeld mit den Amazon-EC2Launch-Einstellungen zu öffnen, erhalten Sie eine Fehlermeldung. Ein Beispielschema finden Sie unter Beispiel: `agent-config.yml`.

1. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
2. Wählen Sie im Startmenü All Programs (Alle Programme) und navigieren Sie zu den EC2Launch settings (Einstellungen). Bevor Sie Herunterfahren mit Sysprep oder Herunterfahren ohne Sysprep wählen, stellen Sie sicher, dass Sie alle Änderungen speichern, die Sie während des Herunterfahrens übernehmen möchten.


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Set computer name
Set the computer name of the instance
Set to "ip-<hex private IPv4 address>"
Use custom name
Reboot after setting computer name
Extend boot volume
Extend OS partition to use free space for boot volume
Set administrator account
Set administrator account
Administrator username (leave blank for default)
Administrator password settings
Random (retrieve from console)
Specify (temporarily stored in configuration file)
Do not set
Start SSM service
Re-enable and start SSM service after Sysprep
Optimize ENA
Optimize receive side scaling and receive queue depth
Enable SSH
Enable OpenSSH for later Windows versions
Enable Jumbo Frames
Enable Jumbo Frames
Important: Do not enable Jumbo Frames if you are not familiar with them
Prepare for imaging
Shutdown without Sysprep
Shutdown with Sysprep

3. Aktivieren bzw. deaktivieren Sie auf der Registerkarte General (Allgemeines) im Dialogfeld EC2Launch Service Properties (EC2Launch-Service-Eigenschaften) die folgenden Einstellungen.

   a. Set Computer Name

      Wenn diese Einstellung aktiviert ist (standardmäßig deaktiviert), wird der aktuelle Hostname bei jedem Start mit dem gewünschten Host-Namen verglichen. Wenn die Host-Namen nicht übereinstimmen, wird der Host-Name zurückgesetzt, und das System wird optional neu gestartet, um den neuen Host-Namen aufzunehmen. Wenn kein benutzerdefinierter Host-Name angegeben wird, wird er mit der hexadezimalformatierten privaten IPv4-Adresse generiert, beispielsweis, `ip-AC1F4E6`. Um zu verhindern, dass Ihr bestehender Hostname geändert wird, aktivieren Sie diese Einstellung nicht.

   b. Extend Boot Volume (Erweitern des Start-Volumes

      Diese Einstellung erweitert Festplatte `Disk 0`/`Volume 0` dynamisch so, dass der gesamte nicht partitionierte Speicherplatz eingeschlossen ist. Dies ist nützlich, wenn die Instance von einem Root-Volume gestartet wird, das eine benutzerdefinierte Größe hat.

   c. Set Administrator Account (Festlegen des Administratorkontos

      Wenn diese Option aktiviert ist, können Sie die Attribute „Username (Benutzername)“ und „Password (Passwort)“ für das Administratorkonto festlegen, das auf Ihrem lokalen Computer erstellt wird. Wenn dieses Feature nicht aktiviert ist, wird auf dem System nach Sysprep kein Administratorkonto erstellt. Geben Sie in `adminPassword` nur dann ein Passwort an, wenn `adminPasswordtype` `Specify` ist.

      Die Passworttypen sind wie folgt definiert:

      i. `Random`

         EC2Launch generiert ein Passwort und verschlüsselt es mit dem Schlüssel des Benutzers: Die Einstellung wird vom System nach dem Start der Instance deaktiviert, so dass das Passwort weiterhin gilt, wenn die Instance neu gestartet bzw. angehalten und gestartet wird.

      ii. `Specify`

         EC2Launch verwendet das Passwort, das Sie unter angeben `adminPassword`. Wenn das Passwort nicht den Systemanforderungen entspricht, erstellt EC2Launch stattdessen ein zufälliges Passwort. Das Passwort wird in `agent-config.yml` im

Klartext gespeichert und gelöscht, wenn Sysprep das Administratorpasswort einstellt. EC2Launch verschlüsselt das Passwort mit dem Schlüssel des Benutzers.

iii. `Do not set`

EC2Launch verwendet das Passwort, das Sie in der Datei unattend.xml angeben. Wenn Sie in der Datei unattend.xml kein Passwort angeben, ist das Administratorkonto deaktiviert.

d. Start SSM Service (Starten des SSM-Services

Wenn diese Option ausgewählt ist, wird der Systems Manager Dienst aktiviert, um nach Sysprep zu starten. EC2Launch v2 führt alle zuvor beschriebenen Aufgaben aus und SSM Agent verarbeitet Anforderungen für Systems Manager-Funktionen wie Run Command und Statusmanager.

Sie können über Run Command Ihre vorhandenen Instances upgraden, damit diese die aktuelle Version des EC2Launch v2-Service und von SSM Agent verwenden. Weitere Informationen finden Sie unter Aktualisieren des SSM-Agent mit Run Command im Benutzerhandbuch für AWS Systems Manager.

e. Optimize ENA (Optimieren von ENA

Wenn diese Option ausgewählt ist, werden die ENA-Einstellungen so konfiguriert, dass die Einstellungen für ENA Receive Side Scaling und Receive Queue Depth für optimiert sin AWS. Weitere Informationen finden Sie unter Konfiguration der CPU-Affinität für empfangsseitige Skalierung.

f. Enable SSH (Aktivieren von SSH

Diese Einstellung aktiviert OpenSSH für spätere Windows-Versionen, um die Remote-Systemverwaltung zu ermöglichen.

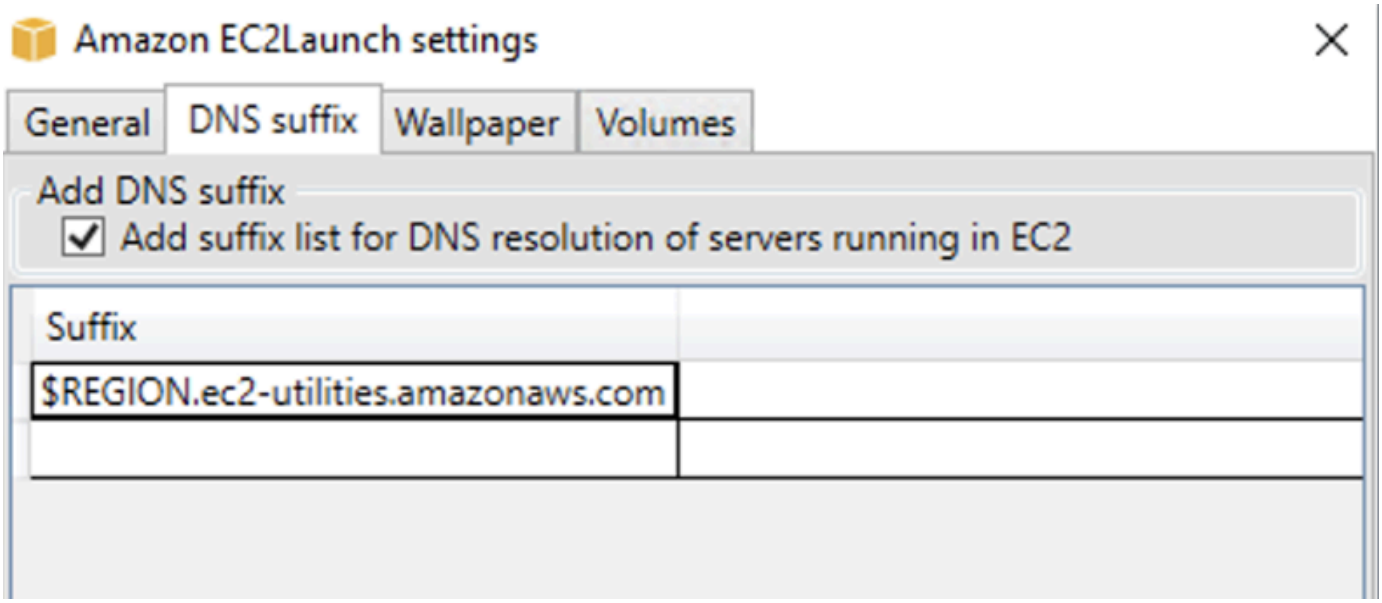
g. Enable Jumbo Frames (Aktivieren von Jumbo Frames

Wählen Sie diese Option aus, um Jumbo Frames zu aktivieren. Jumbo Frames können unbeabsichtigte Auswirkungen auf Ihre Netzwerkkommunikation haben. Stellen Sie also sicher, dass Sie wissen, wie sich Jumbo Frames auf Ihr System auswirken, bevor Sie diese aktivieren. Weitere Informationen zu Jumbo Frames finden Sie unter Jumbo-Frames (9001 MTU).

h. Prepare for Imaging (Vorbereitung zum Imaging

Wählen Sie aus, ob Ihre EC2-Instance mit oder ohne Sysprep heruntergefahren werden soll. Wenn Sie Sysprep mit EC2Launch v2 ausführen möchten, wählen Sie Shutdown with Sysprep (Mit Sysprep herunterfahren).

4. Auf der Registerkarte DNS Suffix (DNS-Suffix) können Sie auswählen, ob Sie eine DNS-Suffixliste für die DNS-Auflösung von Servern mit EC2 hinzufügen möchten, ohne den vollqualifizierten Domain-Namen anzugeben. DNS-Suffixe können die Variablen `$REGION` und `$AZ` enthalten. Nur Suffixe, die noch nicht vorhanden sind, werden der Liste hinzugefügt.



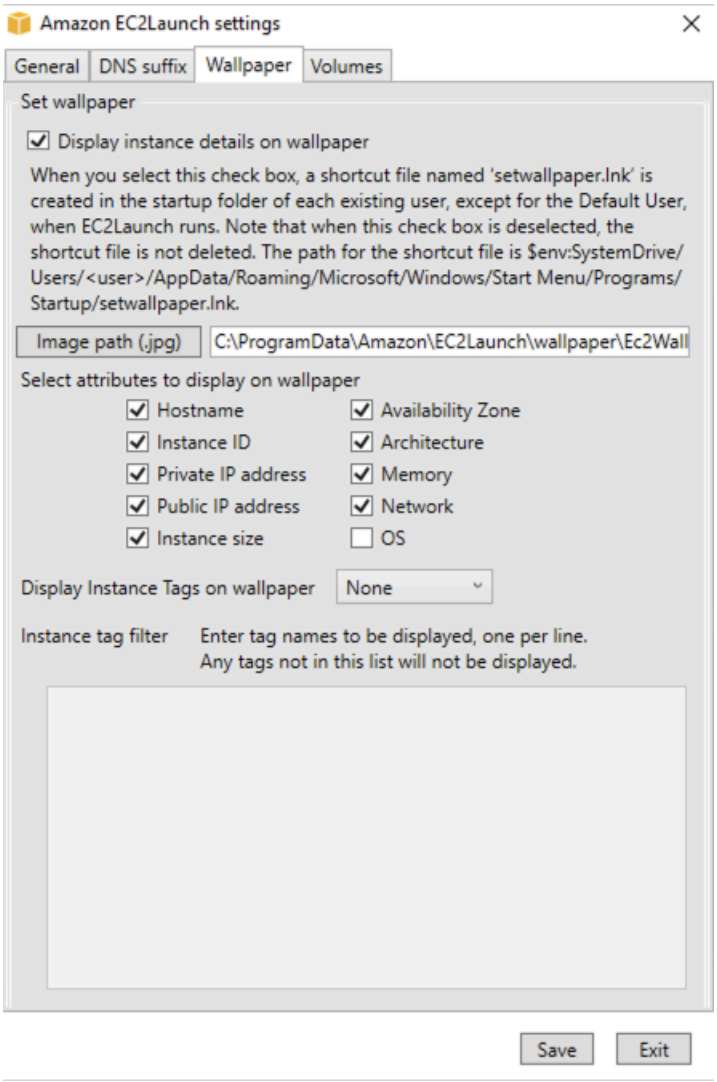
5. Auf der Registerkarte Hintergrundbild können Sie Ihr Instance-Hintergrundbild mit einem Hintergrundbild konfigurieren und Instance-Details für das anzuzeigende Hintergrundbild angeben. Amazon EC2 generiert die Details bei jeder Anmeldung.

   Sie können Ihr Hintergrundbild mit den folgenden Steuerelementen konfigurieren.

   - Instance-Details auf dem Hintergrundbild anzeigen – Dieses Kontrollkästchen aktiviert oder deaktiviert die Anzeige von Instance-Details auf dem Hintergrundbild.
   - Image-Pfad (.jpg) – Geben Sie den Pfad zu dem Image an, das als Hintergrundhintergrund verwendet werden soll.
   - Auf Hintergrund anzuzeigende Attribute auswählen – Aktivieren Sie die Kontrollkästchen für die Instance-Details, die auf dem Hintergrund angezeigt werden sollen. Deaktivieren Sie die Kontrollkästchen für zuvor ausgewählte Instance-Details, die Sie aus dem Hintergrundbild entfernen möchten.
   - Instance-Tags auf Hintergrundbild anzeigen – Wählen Sie eine der folgenden Einstellungen aus, um Instance-Tags auf dem Hintergrundbild anzuzeigen:

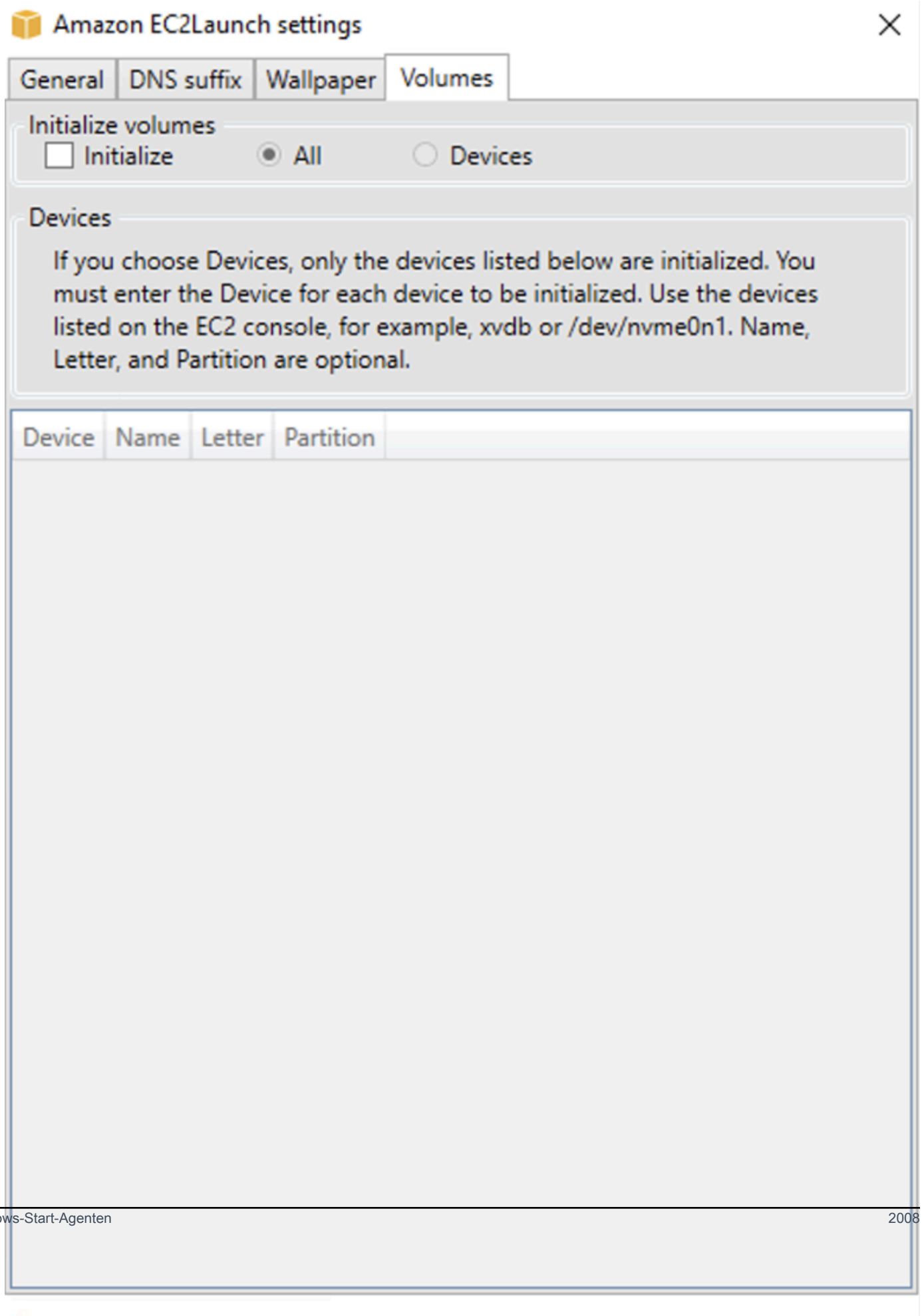
- Keine – Keine Instance-Tags auf dem Hintergrundbild anzeigen.
- Alles anzeigen – Alle Instance-Tags auf dem Hintergrund anzeigen.
- Gefiltert anzeigen – Angegebene Instance-Tags auf dem Hintergrundbild anzeigen. Wenn Sie diese Einstellung wählen, können Sie die Instance-Tags, die Sie auf Ihrem Hintergrundbild anzeigen möchten, zum Feld Instance-Tag-Filter hinzufügem.

> **Note**
>
> Sie müssen Tags in Metadaten aktivieren, um Tags auf dem Hintergrundbild anzuzeigen. Weitere Informationen zu Instance-Tags und Metadaten finden Sie unter Zeigen Sie Tags für Ihre EC2 Instances mithilfe von Instanz-Metadaten an.



6. Wählen Sie auf der Registerkarte Volumes aus, ob Sie die Volumes initialisieren möchten, die der Instance angefügt sind. Durch die Aktivierung werden Laufwerkbuchstaben für zusätzliche Volumes festgelegt und diese erweitert, um verfügbaren Speicherplatz zu nutzen. Wenn Sie All (Alle) auswählen, werden alle Speicher-Volumes initialisiert. Wenn Sie Devices (Geräte) auswählen, werden nur Geräte initialisiert, die in der Liste angegeben sind. Sie müssen jedes zu initialisierende Gerät eingeben. Verwenden Sie beispielsweise die Geräte, die auf der EC2-Konsole aufgeführt sind, `xvdb` oder `/dev/nvme0n1`. In der Dropdown-Liste werden die Speicher-Volumes angezeigt, die der Instance zugeordnet sind. Um ein Gerät einzugeben, das nicht an die Instance angefügt ist, geben Sie es in das Textfeld ein.

   Name, Letter (Buchstabe) und Partition sind optionale Felder. Wenn für Partition kein Wert angegeben wird, werden Speichermedien, die größer als 2 TB sind, mit dem Partitionstyp `gpt` initialisiert, und solche, die kleiner als 2 TB sind, mit dem Partitionstyp `mbr` initialisiert. Wenn Geräte konfiguriert sind und ein Nicht-NTFS-Gerät entweder eine Partitionstabelle enthält oder die ersten 4 KB des Datenträgers Daten enthalten, wird der Datenträger übersprungen und die Aktion protokolliert.


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Initialize volumes
Initialize
All
Devices
Devices
If you choose Devices, only the devices listed below are initialized. You must enter the Device for each device to be initialized. Use the devices listed on the EC2 console, for example, xvdb or /dev/nvme0n1. Name, Letter, and Partition are optional.
Device
Name
Letter
Partition

Nachfolgend finden Sie ein Beispiel für eine YAML-Konfigurationsdatei, die aus den Einstellungen erstellt wurde, die im EC2Launch-Dialog eingegeben wurden.

```
version: 1.0
config:
  - stage: boot
 tasks:
      - task: extendRootPartition
  - stage: preReady
    tasks:
      - task: activateWindows
        inputs:
          activation:
            type: amazon
      - task: setDnsSuffix
        inputs:
          suffixes:
            - $REGION.ec2-utilities.amazonaws.com
      - task: setAdminAccount
        inputs:
          password:
            type: random
      - task: setWallpaper
        inputs:
          path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
          attributes:
            - hostName
            - instanceId
            - privateIpAddress
            - publicIpAddress
            - instanceSize
            - availabilityZone
            - architecture
            - memory
            - network
  - stage: postReady
    tasks:
      - task: startSsm
```

Konfigurieren von EC2Launch v2 mit der CLI

Sie können die Befehlszeilenschnittstelle (CLI) verwenden, um Ihre EC2Launch-Einstellungen zu konfigurieren und den Service zu verwalten. Der folgende Abschnitt enthält Beschreibungen

und Verwendungsinformationen für die CLI-Befehle, die Sie zum Verwalten von EC2Launch v2 verwenden können.

Befehle

- collect-logs
- get-agent-config
- list-Volumes
- reset
- run
- Status
- sysprep
- validieren
- version
- Hintergrundbild

collect-logs

Erfasst Protokolldateien für EC2Launch, komprimiert die Dateien und speichert sie in einem angegebenen Verzeichnis.

Beispiel

```
ec2launch collect-logs -o C:\Mylogs.zip
```

Verwendung

```
ec2launch collect-logs [flags]
```

Flags

`-h, --help`

Hilfe für `collect-logs`

`-o, --output string`

Pfad zu komprimierten Ausgabe-Protokolldateien

get-agent-config

Druckt `agent-config.yml` im angegebenen Format (JSON oder YAML). Wenn kein Format angegeben ist, wird `agent-config.yml` in dem zuvor angegebenen Format gedruckt.

Beispiel

```
ec2launch get-agent-config -f json
```

Verwendung

`ec2launch get-agent-config [flags]`

Flags

`-h`, `--help`

Hilfe für `get-agent-config`

`-f`, `--format string`

Ausgabeformat der `agent-config`-Datei: `json`, `yaml`

list-Volumes

Listet alle Speicher-Volumes auf, die der Instance zugeordnet sind, einschließlich flüchtiger und EBS-Volumes.

Beispiel

```
ec2launch list-volumes
```

Verwendung

`ec2launch list-volumes`

Flags

`-h`, `--help`

Hilfe für `list-volumes`

reset

Das Hauptziel dieser Aufgabe besteht darin, den Agenten für die nächste Ausführung zurückzusetzen. Dazu löscht der reset-Befehl alle Statusdaten des Agenten für EC2Launch v2 aus dem lokalen `EC2Launch`-Verzeichnis (weitere Informationen unter EC2Launch v2-Verzeichnisstruktur). Beim Zurücksetzen werden optional die Service- und Sysprep-Protokolle gelöscht.

Das Verhalten des Skripts hängt davon ab, in welchem Modus der Agent die Skripte ausführt – inline oder getrennt.

Inline (Standard)

Der EC2Launch-v2-Agent führt die Skripte nacheinander aus (`detach: false`). Dies ist die Standardeinstellung.

> **Note**
>
> Wenn Ihr Inline-Skript einen reset- oder sysprep-Befehl ausgibt, wird es sofort ausgeführt und setzt den Agenten zurück. Die aktuelle Aufgabe wird beendet, dann wird der Agent heruntergefahren, ohne weitere Aufgaben auszuführen.
> Wenn beispielsweise auf die Aufgabe, die den Befehl ausgibt, eine `startSsm`-Aufgabe folgen würde (die standardmäßig nach der Ausführung der Benutzerdaten enthalten ist), wird die Aufgabe nicht ausgeführt und der Systems-Manager-Service nicht gestartet.

Getrennt

Der EC2Launch-v2-Agent führt Skripte gleichzeitig mit anderen Aufgaben aus (`detach: true`).

> **Note**
>
> Wenn Ihr abgetrenntes Skript einen reset- oder sysprep-Befehl ausgibt, warten diese Befehle, bis der Agent fertig ist, bevor sie ausgeführt werden. Aufgaben nach dem executeScript werden weiterhin ausgeführt.

Beispiel

```
ec2launch reset -c
```

Verwendung

`ec2launch reset [flags]`

Flags

`-c`, `--clean`

bereinigt Instance-Protokolle vor `reset`

`-h`, `--help`

Hilfe für `reset`

run

Führt EC2Launch v2 aus.

Beispiel

```
ec2launch run
```

Verwendung

`ec2launch run [flags]`

Flags

`-h`, `--help`

Hilfe für `run`

Status

Ruft den Status eines EC2Launch-v2-Agents ab. Blockiert optional den Prozess, bis der Agent beendet ist. Der Prozess-Beendigungscode bestimmt den Agentenstatus:

- `0` – der Agent wurde ausgeführt und war erfolgreich.

- 1 – der Agent wurde ausgeführt und ist fehlgeschlagen.
- 2 – der Agent wird noch ausgeführt.
- 3 – der Agent befindet sich in einem unbekannten Status. Der Agentenstatus wird nicht ausgeführt oder ist beendet.
- 4 – beim Versuch, den Agentenstatus abzurufen, ist ein Fehler aufgetreten.
- 5 – der Agent wird nicht ausgeführt und der Status der letzten bekannten Ausführung ist unbekannt. Dies könnte eines der folgenden bedeuten:
  - Sowohl `state.json` und `previous-state.json` werden gelöscht.
  - `previous-state.json` ist beschädigt.

  Dies ist der Agentenstatus nach dem Ausführen des `reset`-Befehls.

Beispiel:

```
ec2launch status -b
```

Verwendung

`ec2launch status [flags]`

Flags

`-b,--block`

blockiert den Prozess, bis die Ausführung des Agenten beendet ist

`-h,--help`

Hilfe für `status`

sysprep

Das Hauptziel dieser Aufgabe besteht darin, den Agenten für die nächste Ausführung zurückzusetzen. Dazu setzt der sysprep-Befehl den Agentenstatus zurück, aktualisiert die `unattend.xml`-Datei, deaktiviert RDP und führt Sysprep aus.

Das Verhalten des Skripts hängt davon ab, in welchem Modus der Agent die Skripte ausführt – inline oder getrennt.

Inline (Standard)

Der EC2Launch-v2-Agent führt die Skripte nacheinander aus (`detach: false`). Dies ist die Standardeinstellung.

> **Note**
>
> Wenn Ihr Inline-Skript einen reset- oder sysprep-Befehl ausgibt, wird es sofort ausgeführt und setzt den Agenten zurück. Die aktuelle Aufgabe wird beendet, dann wird der Agent heruntergefahren, ohne weitere Aufgaben auszuführen.
> Wenn beispielsweise auf die Aufgabe, die den Befehl ausgibt, eine `startSsm`-Aufgabe folgen würde (die standardmäßig nach der Ausführung der Benutzerdaten enthalten ist), wird die Aufgabe nicht ausgeführt und der Systems-Manager-Service nicht gestartet.

Getrennt

Der EC2Launch-v2-Agent führt Skripte gleichzeitig mit anderen Aufgaben aus (`detach: true`).

> **Note**
>
> Wenn Ihr abgetrenntes Skript einen reset- oder sysprep-Befehl ausgibt, warten diese Befehle, bis der Agent fertig ist, bevor sie ausgeführt werden. Aufgaben nach dem executeScript werden weiterhin ausgeführt.

Beispiel:

```
ec2launch sysprep
```

Verwendung

`ec2launch sysprep [flags]`

Flags

`-c,--clean`

bereinigt Instance-Protokolle vor `sysprep`

`-h,--help`

Hilfe für Sysprep

`-s,--shutdown`

fährt die Instance nach herunte `sysprep`

validieren

Validiert die `agent-config`-Datei `C:\ProgramData\Amazon\EC2Launch\config\agent-config.yml`.

Beispiel

```
ec2launch validate
```

Verwendung

`ec2launch validate [flags]`

Flags

`-h , --help`

Hilfe für `validate`

version

Ruft die ausführbare Version ab.

Beispiel

```
ec2launch version
```

Verwendung

`ec2launch version [flags]`

Flags

`-h, --help`

Hilfe für `version`

Hintergrundbild

Legt das bereitgestellte Hintergrundbild für den Hintergrundbildpfad fest (JPG-Datei) und zeigt die ausgewählten Instance-Details an.

Syntax

```
ec2launch wallpaper ^
--path="C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg" ^
--all-tags ^
--
attributes=hostName,instanceId,privateIpAddress,publicIpAddress,instanceSize,availabilityZone,a
```

Eingaben

Parameter

--allowed-tags [***`tag-name-1`***, ***`tag-name-n`***]

(Optional) Base64-codiertes JSON-Array von Instance-Tag-Namen zur Anzeige auf dem Hintergrundbild. Sie können dieses Tag oder das `--all-tags` verwenden, aber nicht beides.

--attributes ***`attribute-string-1`***, ***`attribute-string-n`***

(Optional) Eine durch Kommas getrennte Liste von `wallpaper`-Attributzeichenfolgen zum Anwenden von Einstellungen auf das Hintergrundbild.

[--path | -p] ***`path-string`***

(Erforderlich) Gibt den `wallpaper`-Dateipfad für das Hintergrundbild an.

Flags

--all-tags

(Optional) Zeigt alle Instance-Tags auf dem Hintergrund an. Sie können dieses Tag oder das `--allowed-tags` verwenden, aber nicht beides.

[--help | -h]

Zeigt Hilfe für den wallpaper-Befehl an.

Aufgabenkonfiguration in EC2Launch v2

Dieser Abschnitt enthält das Konfigurationsschema, Aufgaben, Details und Beispiele für `agent-config.yml` und Benutzerdaten.

Aufgaben und Beispiele

- Schema: agent-config.yml
- EC2Launch-v2-Skripts für Benutzerdaten, die beim Starten oder Neustarten ausgeführt werden, konfigurieren

Schema: **`agent-config.yml`**

Die Struktur der `agent-config.yml`-Datei wird unten gezeigt. Beachten Sie, dass eine Aufgabe nicht in derselben Phase wiederholt werden kann. Informationen zu den Aufgabeneigenschaften finden Sie in den folgenden Aufgabenbeschreibungen.

Dokumentstruktur: agent-config.yml

JSON

```
{
 "version": "1.1",
 "config": [
  {
   "stage": "string",
   "tasks": [
    {
     "task": "string",
     "inputs": {
      ...
     }
    },
    ...
   ]
  },
  ...
```

```
 ]
}
```

YAML

```
version: 1.1
config:
- stage: string
  tasks:
  - task: string
 inputs:
   ...
  ...
...
```

Beispiel: **`agent-config.yml`**

Das folgende Beispiel zeigt die Einstellungen für die `agent-config.yml`-Konfigurationsdatei.

```
version: 1.1
config:
- stage: boot
  tasks:
  - task: extendRootPartition
- stage: preReady
  tasks:
  - task: activateWindows
    inputs:
      activation:
        type: amazon
  - task: setDnsSuffix
    inputs:
      suffixes:
      - $REGION.ec2-utilities.amazonaws.com
  - task: setAdminAccount
    inputs:
      password:
        type: random
  - task: setWallpaper
    inputs:
      path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
      attributes:
      - hostName
```

```
      - instanceId
      - privateIpAddress
      - publicIpAddress
      - instanceSize
      - availabilityZone
      - architecture
      - memory
      - network
- stage: postReady
  tasks:
  - task: startSsm
```

EC2Launch-v2-Skripts für Benutzerdaten, die beim Starten oder Neustarten ausgeführt werden, konfigurieren

Die folgenden JSON- und YAML-Beispiele zeigen die Dokumentstruktur für Benutzerdaten. Amazon EC2 analysiert jede Aufgabe, die im `tasks`-Array genannt wird, das Sie im Dokument angeben. Jede Aufgabe hat ihre eigenen Eigenschaften und Anforderungen. Einzelheiten finden Sie im Aufgabendefinitionen für EC2Launch v2-Startaufgaben.

> **Note**
>
> Eine Aufgabe darf nur einmal im Array mit Benutzerdatenaufgaben vorkommen.

Dokumentenstruktur: Benutzerdaten

JSON

```
{
 "version": "1.1",
 "tasks": [
  {
   "task": "string",
   "inputs": {
    ...
   },
  },
  ...
 ]
}
```

YAML

```
version: 1.1
tasks:
- task: string
  inputs:
    ...
...
```

Beispiel: Benutzerdaten

Weitere Informationen zu Benutzerrollen finden Sie unter Wie Amazon EC2 mit Benutzerdaten für Windows-Instances umgeht.

Das folgende Beispiel eines YAML-Dokuments zeigt ein PowerShell-Skript, das EC2Launch v2 als Benutzerdaten ausführt, um eine Datei zu erstellen.

```
version: 1.1
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: powershell
    runAs: localSystem
    content: |-
      New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
```

Sie können ein XML-Format für die Benutzerdaten verwenden, das mit früheren Versionen des Startagenten kompatibel ist. EC2Launch v2 führt das Skript als `executeScript`-Aufgabe in der `UserData`-Stufe aus. Um dem EC2Launch-v1- und EC2Config-Verhalten zu entsprechen, wird das Benutzerdatenskript standardmäßig als angefügter/Inline-Prozess ausgeführt.

Sie können optionale Tags hinzufügen, um die Ausführung Ihres Skripts anzupassen. Um beispielsweise das Benutzerdatenskript beim Neustart der Instance zusätzlich zum einmaligen Starten der Instance auszuführen, können Sie das folgende Tag verwenden:

`<persist>true</persist>`

Beispiel:

```
<powershell>
```

```
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Sie können ein oder mehrere PowerShell-Argumente mit dem `<powershellArguments>`-Tag angeben. Wenn keine Argumente übergeben werden, fügt EC2Launch v2 standardmäßig das folgende Argument hinzu: `-ExecutionPolicy Unrestricted`.

Beispiel:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

Um ein XML-Benutzerdatenskript als getrennten Prozess auszuführen, fügen Sie Ihren Benutzerdaten das folgende Tag hinzu.

`<detach>true</detach>`

Beispiel:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<detach>true</detach>
```

> **Note**
>
> Das Abtrennungs-Tag wird auf früheren Startagenten nicht unterstützt.

Änderungsprotokoll: Benutzerdaten

In der folgenden Tabelle sind die Änderungen für Benutzerdaten aufgeführt und sie werden mit der jeweiligen Version des EC2Launch-v2-Agents verglichen.

Benutzerdatenversion	Details	Eingeführt in
1.1	• Benutzerdatenaufgaben werden vor der `PostReady` -Phase in der Agentenkonfigurationsdatei ausgeführt. • Führt Benutzerdaten aus, bevor der Systems Manager Agent gestartet wird (gleiches Verhalten wie EC2Launch v1 und EC2Config).*	EC2Launch -v2-Version 2.0.1245
1,0	• Wird veraltet sein. • Benutzerdatenaufgaben werden nach der `PostReady` -Phase in der Agentenkonfigurationsdatei ausgeführt. Dies ist nicht abwärtskompatibel mit EC2Launch-v1. • Wirkt sich auf eine Race-Bedingung zwischen dem Start des Systems Manager Agents und den Benutzerdatenaufgaben aus.	EC2Launch -v2-Version 2.0.0

* Bei Verwendung mit der `agent-config.yml`-Standarddatei.

Exit-Codes und Neustarts für EC2Launch v2

Sie können EC2Launch v2 verwenden, um zu definieren, wie Beendigungscodes in Ihren Skripts gehandhabt werden. Standardmäßig wird der Beendigungscode des letzten in einem Skript ausgeführten Befehls als Beendigungscode für das gesamte Skript gemeldet. Wenn ein Skript beispielsweise drei Befehle enthält und der erste Befehl fehlschlägt, aber die folgenden erfolgreich sind, wird der Ausführungsstatus als `success` gemeldet, da der endgültige Befehl erfolgreich war.

Wenn Sie möchten, dass ein Skript eine Instance neu startet, müssen Sie `exit 3010` in Ihrem Skript angeben, auch wenn der Neustart der letzte Schritt in Ihrem Skript ist. `exit 3010` weist EC2Launch v2 an, die Instance neu zu starten und das Skript erneut aufzurufen, bis ein Beendigungscode zurückgegeben wird, der nicht `3010` ist oder bis die maximale Neustartanzahl erreicht ist. EC2Launch v2 erlaubt maximal 5 Neustarts pro Aufgabe. Wenn Sie versuchen, eine Instance aus einem Skript mit einem anderen Mechanismus wie `Restart-Computer` neu zu starten, ist der

Skriptausführungsstatus inkonsistent. Er kann beispielsweise in einer Neustartschleife stecken bleiben oder den Neustart nicht durchführen.

Wenn Sie ein XML-Benutzerdatenformat verwenden, das mit älteren Agenten kompatibel ist, werden die Benutzerdaten möglicherweise öfter ausgeführt, als Sie beabsichtigen. Weitere Informationen finden Sie im Abschnitt zur Fehlerbehebung unter Der Service führt Benutzerdaten mehr als einmal aus.

EC2Launch v2 und Sysprep

Der EC2Launch v2-Service führt Sysprep aus, ein Microsoft-Tool, mit dem Sie ein benutzerdefiniertes Windows-AMI erstellen können, das wiederverwendet werden kann. Wenn EC2Launch v2 Sysprep aufruft, verwendet es die Dateien in `%ProgramData%\Amazon\EC2Launch`, um zu bestimmen, welche Operationen ausgeführt werden sollen. Sie können diese Dateien indirekt über das EC2Launch settings (Einstellungen)-Dialogfeld oder direkt über einen YAML-Editor oder einen Texteditor bearbeiten. Es gibt jedoch einige erweiterte Einstellungen, die nicht im Dialogfeld EC2Launch settings (Einstellungen) verfügbar sind. Diese Einträge müssen Sie direkt bearbeiten.

Wenn Sie ein AMI aus einer Instance erstellen, nachdem Sie deren Einstellungen aktualisiert haben, werden die neuen Einstellungen auf alle Instances angewandt, die von diesem AMI gestartet werden. Weitere Informationen über die Erstellung eines AMI finden Sie unter Ein Amazon-EBS-gestütztes AMI erstellen.

Aufgabendefinitionen für EC2Launch v2-Startaufgaben

Jede Aufgabe, die EC2Launch v2 während des Starts oder Hochfahrens ausführt, hat ihre eigenen Eigenschaften und Anforderungen. Zu den Aufgabendetails gehören Einstellungen dafür, wie oft eine Aufgabe ausgeführt wird – einmal oder immer –, in welcher Phase des Startvorgangs des Agenten sie ausgeführt wird, Syntax und Beispiele für YAML-Dokumente. Weitere Informationen finden Sie in den Aufgabendetails in dieser Referenz.

EC2Launch-v2-Aufgaben

- activateWindows
- enableJumboFrames
- enableOpenSsh
- executeProgram
- executeScript
- extendRootPartition

- initializeVolume
- optimizeEna
- setAdminAccount
- setDnsSuffix
- setHostName
- setWallpaper
- startSsm
- sysprep
- writeFile

activateWindows

Aktiviert Windows für einen Satz von AWS KMS-Servern. Die Aktivierung wird übersprungen, wenn die Instance als Bring-Your-Own-License (BYOL) erkannt wird.

Häufigkeit - einmal

AllowedStages — `[PreReady]`

Eingaben —

`activation`: (Zuordnung)

`type`: (Zeichenfolge) Aktivierungstyp, der verwendet werden soll, auf gesetzt `amazon`

Beispiel

```
task: activateWindows
  inputs:
    activation:
    type: amazon
```

enableJumboFrames

Aktiviert Jumbo Frames, die die Maximum Transmission Unit (MTU) des Netzwerkadapters erhöhen. Weitere Informationen finden Sie unter Jumbo-Frames (9001 MTU).

Häufigkeit — immer

AllowedStages — `[PostReady, UserData]`

Eingaben — keine

Beispiel

```
task: enableJumboFrames
```

enableOpenSsh

Aktiviert Windows OpenSSH und fügt den öffentlichen Schlüssel für die Instance dem Ordner für autorisierte Schlüssel hinzu.

Häufigkeit - einmal

AllowedStages — `[PreReady, UserData]`

Eingaben — keine

Beispiel

Im folgenden Beispiel wird gezeigt, wie OpenSSH für eine Instance aktiviert und der öffentliche Schlüssel für die Instance dem Ordner für autorisierte Schlüssel hinzugefügt wird. Diese Konfiguration funktioniert nur auf Instances, auf denen Windows Server 2019 ausgeführt wird.

```
task: enableOpenSsh
```

executeProgram

Führt ein Programm mit optionalen Argumenten und einer angegebenen Häufigkeit aus.

Phasen: Sie können die Aufgabe `executeProgram` während der Phasen `PreReady`, `PostReady` und `UserData` ausführen.

Frequenz: konfigurierbar, siehe Eingänge.

Eingaben

> Dieser Abschnitt enthält ein oder mehrere Programme, mit denen die executeProgram-Aufgabe ausgeführt werden kann (Eingaben). Jede Eingabe kann die folgenden konfigurierbaren Einstellungen enthalten:

Frequenz (Zeichenfolge)

(Erforderlich) Geben Sie genau einen der folgenden Werte an:

- `once`
- `always`

Pfad (Zeichenfolge)

(Erforderlich) Der Dateipfad für die auszuführende Datei.

Argumente (Liste von Zeichenfolgen)

(Optional) Eine durch Kommas getrennte Liste von Argumenten, die dem Programm als Eingabe zur Verfügung gestellt werden sollen.

runAs (Zeichenfolge)

(Erforderlich) Muss auf `localSystem` gesetzt sein

Output

Alle Aufgaben schreiben Logfile-Einträge in die `agent.log`-Datei. Zusätzliche Ausgaben der Aufgabe `executeProgram` werden wie folgt separat in einem dynamisch benannten Ordner gespeichert:

`%LocalAppData%\Temp\`*`EC2Launch#########\outputfilename.tmp`*

Der genaue Pfad zu den Ausgabedateien ist in der `agent.log`-Datei enthalten, zum Beispiel:

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\ExecuteProgramInputs.tmp
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

Ausgabedateien für die Aufgabe **`executeProgram`**

`ExecuteProgramInputs.tmp`

Enthält den Pfad für die ausführbare Datei und alle Eingabeparameter, die die Aufgabe `executeProgram` bei der Ausführung an sie übergibt.

`Output.tmp`

Enthält die Laufzeitausgabe des Programms, das die Aufgabe `executeProgram` ausführt.

`Err.tmp`

Enthält die Laufzeit-Fehlermeldungen des Programms, das die Aufgabe `executeProgram` ausführt.

Beispiele

Die folgenden Beispiele zeigen, wie eine ausführbare Datei aus einem lokalen Verzeichnis auf einer Instance mit der Aufgabe `executeProgram` ausgeführt wird.

Beispiel 1: Setup Executable mit einem Argument

Dieses Beispiel zeigt eine `executeProgram`-Aufgabe, die eine Setup Executable im Modus „Quiet“ ausführt.

```
task: executeProgram
  inputs:
    - frequency: always
      path: C:\Users\Administrator\Desktop\setup.exe
      arguments: ['-quiet']
```

Beispiel 2: VLC-Executable mit zwei Argumenten

Dieses Beispiel zeigt eine `executeProgram`-Aufgabe, die eine VLC-Executable-Datei mit zwei als Eingabeparameter übergebenen Argumenten ausführt.

```
task: executeProgram
  inputs:
    - frequency: always
      path: C:\vlc-3.0.11-win64.exe
      arguments: ['/L=1033','/S']
      runAs: localSystem
```

executeScript

Führt ein Skript mit optionalen Argumenten und einer angegebenen Häufigkeit aus. Das Verhalten des Skripts hängt davon ab, in welchem Modus der Agent die Skripte ausführt – inline oder getrennt.

Inline (Standard)

Der EC2Launch-v2-Agent führt die Skripte nacheinander aus (`detach: false`). Dies ist die Standardeinstellung.

> **Note**
>
> Wenn Ihr Inline-Skript einen reset- oder sysprep-Befehl ausgibt, wird es sofort ausgeführt und setzt den Agenten zurück. Die aktuelle Aufgabe wird beendet, dann wird der Agent heruntergefahren, ohne weitere Aufgaben auszuführen.
> Wenn beispielsweise auf die Aufgabe, die den Befehl ausgibt, eine `startSsm`-Aufgabe folgen würde (die standardmäßig nach der Ausführung der Benutzerdaten enthalten ist), wird die Aufgabe nicht ausgeführt und der Systems-Manager-Service nicht gestartet.

Getrennt

Der EC2Launch-v2-Agent führt Skripte gleichzeitig mit anderen Aufgaben aus (`detach: true`).

> **Note**
>
> Wenn Ihr abgetrenntes Skript einen reset- oder sysprep-Befehl ausgibt, warten diese Befehle, bis der Agent fertig ist, bevor sie ausgeführt werden. Aufgaben nach dem executeScript werden weiterhin ausgeführt.

Phasen: Sie können die Aufgabe `executeScript` während der Phasen `PreReady`, `PostReady` und `UserData` ausführen.

Frequenz: konfigurierbar, siehe Eingänge.

Eingaben

Dieser Abschnitt enthält ein oder mehrere Skripte, mit denen die executeScript-Aufgabe ausgeführt werden kann (Eingaben). Jede Eingabe kann die folgenden konfigurierbaren Einstellungen enthalten:

Frequenz (Zeichenfolge)

(Erforderlich) Geben Sie genau einen der folgenden Werte an:

- `once`

- `always`

Typ (Zeichenfolge)

(Erforderlich) Geben Sie genau einen der folgenden Werte an:

- `batch`
- `powershell`

Argumente (Liste von Zeichenfolgen)

(Optional) Eine Liste von Zeichenfolgenargumenten, die an die Shell übergeben werden sollen (nicht das PowerShell-Skript). Dieser Parameter wird nicht für `type: batch` unterstützt. Wenn keine Argumente übergeben werden, fügt EC2Launch v2 standardmäßig das folgende Argument hinzu: `-ExecutionPolicy Unrestricted`.

Inhalt (Zeichenfolge)

(Erforderlich) Skriptinhalt.

runAs (Zeichenfolge)

(Erforderlich) Geben Sie genau einen der folgenden Werte an:

- `admin`
- `localSystem`

trennen (Boolean)

(Optional) Der EC2Launch v2-Agent führt standardmäßig Skripts einzeln aus (`detach: false`). Um das Skript gleichzeitig mit anderen Aufgaben auszuführen, setzen Sie den Wert auf `true` (`detach: true`).

> **Note**
>
> Skript-Exitcodes (einschließlich `3010`) haben keine Wirkung, wenn `detach` auf `true` festgelegt wird.

Output

Alle Aufgaben schreiben Logfile-Einträge in die `agent.log`-Datei. Zusätzliche Ausgaben von Skripten, die die Aufgabe `executeScript` ausführt, werden wie folgt separat in einem dynamisch benannten Ordner gespeichert:

`%LocalAppData%\Temp\EC2Launch#########\outputfilename.ext`

Der genaue Pfad zu den Ausgabedateien ist in der `agent.log`-Datei enthalten, zum Beispiel:

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\UserScript.ps1
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

Ausgabedateien für die Aufgabe **`executeScript`**

`UserScript.ext`

Enthält das Skript, das die Aufgabe `executeScript` ausgeführt hat. Die Dateierweiterung hängt wie folgt von der Art des Skripts ab, das Sie im `type`-Parameter für die `executeScript`-Aufgabe angegeben haben:

- Wenn der Typ `batch` ist, dann ist die Dateierweiterung `.bat`.
- Wenn der Typ `powershell` ist, dann ist die Dateierweiterung `.ps1`.

`Output.tmp`

Enthält die Laufzeitausgabe des Skripts, das die Aufgabe `executeScript` ausführt.

`Err.tmp`

Enthält die Laufzeit-Fehlermeldungen des Skripts, das die Aufgabe `executeScript` ausführt.

Beispiele

Die folgenden Beispiele zeigen, wie Sie ein Inline-Skript mit der Aufgabe `executeScript` ausführen.

Beispiel 1: Hello World Ausgabetextdatei

Dieses Beispiel zeigt eine Aufgabe `executeScript`, die ein PowerShell-Skript ausführt, um eine „Hello World“-Textdatei auf dem `C:`-Laufwerk zu erstellen.

```
task: executeScript
  inputs:
    - frequency: always
      type: powershell
```

```
      runAs: admin
      content: |-
        New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
        Set-Content 'C:\PowerShellTest.txt' "Hello world"
```

Beispiel 2: Zwei Skripts ausführen

Dieses Beispiel zeigt, dass die Aufgabe `executeScript` mehr als ein Skript ausführen kann und der Skripttyp nicht unbedingt übereinstimmen muss.

Das erste Skript (`type: powershell`) schreibt eine Zusammenfassung der Prozesse, die derzeit auf der Instance ausgeführt werden, in eine Textdatei auf dem `C:`-Laufwerk.

Das zweite Skript (`batch`) schreibt die Systeminformationen in die `Output.tmp`-Datei.

```
task: executeScript
  inputs:
    - frequency: always
      type: powershell
      runAs: localSystem
      content: |
        Get-Process | Out-File -FilePath C:\Process.txt
    - frequency: always
      type: batch
      runAs: localSystem
      content: |
        systeminfo
```

Beispiel 3: Idempotenz-Systemkonfiguration mit Neustarts

Dieses Beispiel zeigt eine Aufgabe `executeScript`, die ein idempotentes Skript ausführt, um die folgende Systemkonfiguration mit einem Neustart zwischen den einzelnen Schritten durchzuführen:

- Den Computer umbenennen.
- Den Computer mit der Domain verbinden.
- Aktivieren von Telnet.

Das Skript stellt sicher, dass jede Operation nur einmal ausgeführt wird. Dies verhindert eine Neustartschleife und macht das Skript idempotent.

```
task: executeScript
```

```
inputs:
  - frequency: always
    type: powershell
    runAs: localSystem
    content: |-
      $name = $env:ComputerName
      if ($name -ne $desiredName) {
        Rename-Computer -NewName $desiredName
        exit 3010
      }
      $domain = Get-ADDomain
      if ($domain -ne $desiredDomain)
      {
        Add-Computer -DomainName $desiredDomain
        exit 3010
      }
      $telnet = Get-WindowsFeature -Name Telnet-Client
      if (-not $telnet.Installed)
      {
        Install-WindowsFeature -Name "Telnet-Client"
        exit 3010
      }
```

extendRootPartition

Erweitert das Stammvolume, um den gesamten verfügbaren Speicherplatz auf der Festplatte zu nutzen.

Häufigkeit - einmal

AllowedStages — `[Boot]`

Eingaben — keine

Beispiel

```
task: extendRootPartition
```

initializeVolume

Initialisiert leere Volumes, die an die Instance angefügt sind, sodass diese aktiviert und partitioniert werden. Der Startagent überspringt die Initialisierung, wenn er erkennt, dass das Volume nicht leer

ist. Ein Volume gilt als leer, wenn die ersten 4 KiB des Volumes leer sind oder wenn das Volume kein von Windows erkennbares Laufwerkslayout aufweist.

Der Eingabeparameter wird `letter` immer angewendet, wenn diese Aufgabe ausgeführt wird, unabhängig davon, ob das Laufwerk bereits initialisiert ist.

Das `initializeVolume` führt die folgenden Aktionen aus.

- Setzen Sie die Festplattenattribute `offline` und `readonly` auf false.
- Erstellen Sie eine Partition. Wenn im Eingabeparameter `partition` kein Partitionstyp angegeben ist, gelten die folgenden Standardwerte:
  - Wenn die Festplattengröße kleiner als 2 TB ist, legen Sie den Partitionstyp auf fest `mbr`.
  - Wenn die Festplattengröße 2 TB oder größer ist, legen Sie den Partitionstyp auf fest `gpt`.
- Formatieren Sie das Volume als NTFS.
- Legen Sie die Volume-Bezeichnung wie folgt fest:
  - Verwenden Sie den Wert des Eingabeparameters `name`, falls angegeben.
  - Wenn es sich um ein kurzlebiges Volume handelt und kein Name angegeben wurde, legen Sie die Volume-Bezeichnung auf `Temporary Storage Z` fest.
- Wenn das Volume kurzlebig ist (SSD oder HDD – nicht Amazon EBS), erstellen Sie im Stammverzeichnis des Volumes eine `Important.txt`-Datei mit dem folgenden Inhalt:

```
This is an 'Instance Store' disk and is provided at no additional charge.

*This disk offers increased performance since it is local to the host
*The number of Instance Store disks available to an instance vary by instance type
*DATA ON THIS DRIVE WILL BE LOST IN CASES OF IMPAIRMENT OR STOPPING THE INSTANCE.
 PLEASE ENSURE THAT ANY IMPORTANT DATA IS BACKED UP FREQUENTLY

For more information, please refer to: Instance-Speicher temporärer Speicher auf
 Blockebene für EC2-Instances.
```

- Legen Sie den Laufwerkbuchstaben auf den im Eingabeparameter `letter` angegebenen Wert fest.

Phasen: Sie können die Aufgabe `initializeVolume` während der Phasen `PostReady` und `UserData` ausführen.

Häufigkeit: immer.

Eingaben

Sie können Laufzeitparameter wie folgt konfigurieren:

Geräte (Liste der Zuordnungen)

(Bedingt) Konfiguration für jedes Gerät, das vom Startagenten initialisiert wird. Dies ist erforderlich, wenn der Eingabeparameter `initialize` auf `devices` festgelegt ist.

- Gerät (Zeichenfolge, erforderlich) – Identifiziert das Gerät während der Instance-Erstellung. Beispiel: `xvdb`, `xvdf` oder `\dev\nvme0n1`.
- Buchstabe (Zeichenfolge, optional) – Ein Zeichen. Der Laufwerkbuchstabe, der zugewiesen werden soll.
- Name (Zeichenfolge, optional) – Der zuzuweisende Volume-Name.
- Partition (Zeichenfolge, optional) – Geben Sie einen der folgenden Werte für den Typ der zu erstellenden Partition an oder lassen Sie den Startagenten basierend auf der Volume-Größe als Standard festlegen:
  - mbr
  - gpt

initialisieren (Zeichenfolge)

(Erforderlich) Geben Sie genau einen der folgenden Werte an:

- `all`
- `devices`

Beispiele

Die folgenden Beispiele zeigen Beispiele für Eingabekonfigurationen für die `initializeVolume`-Aufgabe.

Beispiel 1: Initialisieren von zwei Volumes auf einer Instance

Dieses Beispiel zeigt eine `initializeVolume`-Aufgabe, die zwei sekundäre Volumes auf einer Instance initialisiert. Das Gerät mit dem Namen `DataVolume2` im Beispiel ist kurzlebig.

```
task: initializeVolume
inputs:
```

```
  initialize: devices
  devices:
  - device: xvdb
    name: DataVolume1
    letter: D
    partition: mbr
  - device: /dev/nvme0n1
    name: DataVolume2
    letter: E
    partition: gpt
```

Beispiel 2: Initialisieren von EBS-Volumes, die an eine Instance angefügt sind

Dieses Beispiel zeigt eine `initializeVolume`-Aufgabe, die alle leeren EBS-Volumes initialisiert, die an die Instance angefügt sind.

```
task: initializeVolume
inputs:
  initialize: all
```

optimizeEna

Optimiert ENA-Einstellungen basierend auf dem aktuellen Instance-Typ. Möglicherweise wird die Instance neu gestartet.

Häufigkeit — immer

AllowedStages — `[PostReady, UserData]`

Eingaben — keine

Beispiel

```
task: optimizeEna
```

setAdminAccount

Legt Attribute für das Standardadministratorkonto fest, das auf dem lokalen PC erstellt wird.

Häufigkeit - einmal

AllowedStages — `[PreReady]`

Eingaben —

`name`: (Zeichenfolge) Name des Administratorkontos

`password`: (Zuordnung)

`type`: (Zeichenfolge) Strategie zum Setzen des Passworts, entweder als `static`, `random` oder `doNothing`

`data`: (Zeichenfolge) speichert Daten, wenn das Feld `type` statisch ist

Beispiel

```
task: setAdminAccount
inputs:
  name: Administrator
  password:
  type: random
```

setDnsSuffix

Fügt DNS-Suffixe zur Liste der Suchsuffixe hinzu. Nur Suffixe, die noch nicht vorhanden sind, werden der Liste hinzugefügt. Weitere Informationen zur Einrichtung von DNS-Suffixen durch Start-Agenten finden Sie unter Das DNS-Suffix für EC2-Windows-Start-Agenten konfigurieren.

Häufigkeit — immer

AllowedStages — `[PreReady]`

Eingaben —

`suffixes`: (Liste von Zeichenfolgen) Liste mit einem oder mehreren gültigen DNS-Suffixen; gültige Substitutionsvariablen sind `$REGION` und `$AZ`

Beispiel

```
task: setDnsSuffix
inputs:
  suffixes:
```

```
  - $REGION.ec2-utilities.amazonaws.com
```

setHostName

Setzt den Host-Namen des Computers auf eine benutzerdefinierte Zeichenfolge oder, falls `hostName`, die private IPv4-Adresse, nicht angegeben ist.

Häufigkeit — immer

AllowedStages — `[PostReady, UserData]`

Eingaben —

`hostName`: (Zeichenfolge) optionaler Host-Name, der wie folgt formatiert werden muss.

- Muss 15 Zeichen oder weniger haben
- Muss nur alphanumerische (a-z, A-Z, 0-9) und Bindestriche (-) enthalten.
- Darf nicht ausschließlich aus numerischen Zeichen bestehen.

`reboot`: (boolescher Wert) gibt an, ob ein Neustart zulässig ist, wenn der Hostname geändert wird

Beispiel

```
task: setHostName
inputs:
  reboot: true
```

setWallpaper

Erstellt die Verknüpfungsdatei `setwallpaper.lnk` im Startup-Ordner jedes vorhandenen Benutzers, mit Ausnahme von `Default User`. Diese Verknüpfungsdatei wird ausgeführt, wenn sich der Benutzer nach dem Start der Instance zum ersten Mal anmeldet. Hiermit wird die Instance mit einem benutzerdefinierten Hintergrundbild eingerichtet, auf dem die Instance-Attribute zu sehen sind.

Der Pfad der Verknüpfungsdatei lautet:

```
$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/
Startup/setwallpaper.lnk
```

> **Note**
>
> Wenn Sie die `setWallpaper`-Aufgabe entfernen, wird diese Verknüpfungsdatei nicht gelöscht. Weitere Informationen finden Sie unter `setWallpaper`Die Aufgabe ist nicht aktiviert, aber das Hintergrundbild wird beim Neustart zurückgesetzt.

Phasen: Sie können das Hintergrundbild während der Phasen `PreReady` und `UserData` konfigurieren.

Häufigkeit: `always`

Konfiguration des Hintergrundbilds

Sie können Ihr Hintergrundbild mit den folgenden Steuerelementen konfigurieren.

Eingaben

Von Ihnen bereitgestellte Eingabeparameter und Attribute, die Sie zum Konfigurieren Ihres Hintergrundbilds festlegen können:

Attribute (Liste von Zeichenfolgen)

(Optional) Sie können Ihrem Hintergrundbild eines oder mehrere der folgenden Attribute hinzufügen:

- `architecture`
- `availabilityZone`
- `hostName`
- `instanceId`
- `instanceSize`
- `memory`
- `network`
- `privateIpAddress`
- `publicIpAddress`

instanceTags

(Optional) Sie können genau eine der folgenden Optionen für diese Einstellung verwenden.

- AllTags (Zeichenfolge) – Fügen Sie Ihrem Hintergrundbild alle Instance-Tags hinzu.

```
instanceTags: AllTags
```

- instanceTags (Liste von Zeichenfolgen) – Geben Sie eine Liste mit Instance-Tag-Namen an, die Ihrem Hintergrundbild hinzugefügt werden sollen. Zum Beispiel:

```
instanceTags:
  - Tag 1
  - Tag 2
```

Pfad (Zeichenfolge)

(Erforderlich) Der Dateinamenspfad der lokalen Bilddatei im .jpg-Format, die für Ihr Hintergrundbild verwendet werden soll.

Beispiel

Das folgende Beispiel zeigt Hintergrundkonfigurationseingaben, die den Dateipfad für das Hintergrundbild festlegen, zusammen mit Instance-Tags mit den Namen `Tag 1` und `Tag 2` und Attributen, die den Hostnamen, die Instance-ID und die privaten und öffentlichen IP-Adressen für die Instance enthalten.

```
task: setWallpaper
inputs:
  path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
  attributes:
  - hostName
  - instanceId
  - privateIpAddress
  - publicIpAddress
instanceTags:
  - Tag 1
  - Tag 2
```

> **Note**
>
> Sie müssen Tags in Metadaten aktivieren, um Tags auf dem Hintergrundbild anzuzeigen. Weitere Informationen zu Instance-Tags und Metadaten finden Sie unter Zeigen Sie Tags für Ihre EC2 Instances mithilfe von Instanz-Metadaten an.

startSsm

Starten des Systems Manager-Services (SSM) nach Sysprep.

Häufigkeit — immer

AllowedStages — `[PostReady, UserData]`

Eingaben — keine

Beispiel

```
task: startSsm
```

sysprep

Setzt den Servicestatus zurück, aktualisiert `unattend.xml`, deaktiviert RDP und führt Sysprep aus. Diese Aufgabe wird erst ausgeführt, wenn alle anderen Aufgaben abgeschlossen sind.

Häufigkeit - einmal

AllowedStages — `[UserData]`

Eingaben —

`clean`: (boolescher Wert) bereinigt Instance-Protokolle vor dem Ausführen von Sysprep

`shutdown`: (boolescher Wert) fährt die Instance nach dem Ausführen von Sysprep herunter

Beispiel

```
task: sysprep
inputs:
clean: true
shutdown: true
```

writeFile

Schreibt eine Datei in ein Ziel.

Häufigkeit — siehe Eingaben

AllowedStages — `[PostReady, UserData]`

Eingaben —

`frequency`: (Zeichenfolge) `once` oder `always`

`destination`: (Zeichenfolge) Pfad, in den der Inhalt geschrieben werden soll

`content`: (Zeichenfolge) Text, der an das Ziel geschrieben werden soll

Beispiel

```
task: writeFile
inputs:
  - frequency: once
  destination: C:\Users\Administrator\Desktop\booted.txt
  content: Windows Has Booted
```

Problembehandlung beim EC2Launch-v2-Agent

In diesem Abschnitt werden allgemeine Problembehandlungsszenarien für EC2Launch v2, Informationen zum Anzeigen von Windows-Ereignisprotokollen sowie die Konsolenprotokollausgabe und -meldungen aufgeführt.

Themen zur Fehlerbehebung

- Allgemeine Problembehandlungsszenarien
- Windows-Ereignisprotokolle
- EC2Launch v2-Konsolenprotokollausgabe

Allgemeine Problembehandlungsszenarien

In diesem Abschnitt werden allgemeine Problembehandlungsszenarien und Lösungsschritte aufgeführt.

Szenarien

- Der Service kann das Hintergrundbild nicht festlegen
- Service kann Benutzerdaten nicht ausführen
- Der Service führt eine Aufgabe nur einmal aus
- Service kann eine Aufgabe nicht ausführen
- Der Service führt Benutzerdaten mehr als einmal aus

- Geplante Aufgaben von EC2Launch-v1 werden nach der Migration zu EC2Launch v2 nicht ausgeführt
- Der Service initialisiert ein EBS-Volume, das nicht leer ist
- setWallpaperDie Aufgabe ist nicht aktiviert, aber das Hintergrundbild wird beim Neustart zurückgesetzt
- Der Dienst hängt im laufenden Status fest
- Ungültige agent-config.yml verhindert das Öffnen des Dialogfelds für EC2Launch-v2-Einstellungen
- task:executeScript should be unique and only invoked once

Der Service kann das Hintergrundbild nicht festlegen

Auflösung

1. Überprüfen Sie, ob `%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\setwallpaper.lnk` vorhanden ist.
2. Überprüfen Sie `%ProgramData%\Amazon\EC2Launch\log\agent.log` darauf, ob Fehler aufgetreten sind.

Service kann Benutzerdaten nicht ausführen

Mögliche Ursache: Der Service ist möglicherweise fehlgeschlagen, bevor Benutzerdaten ausgeführt werden konnten.

Auflösung

1. Überprüfen Sie `%ProgramData%\Amazon\EC2Launch\state\previous-state.json`.
2. Sehen Sie nach, ob `boot`, `network`, `preReady` und `postReadyLocalData` wurden alle als erfolgreich markiert wurden.
3. Wenn eine der Phasen fehlgeschlagen ist, überprüfen Sie `%ProgramData%\Amazon\EC2Launch\log\agent.log` auf bestimmte Fehler.

Der Service führt eine Aufgabe nur einmal aus

Auflösung

1. Überprüfen Sie die Häufigkeit der Aufgabe.

2. Wenn der Service bereits nach Sysprep ausgeführt wurde und die Aufgabenhäufigkeit auf `once` festgelegt ist, wird die Aufgabe nicht erneut ausgeführt.
3. Legen Sie die Häufigkeit der Aufgabe auf `always` fest, wenn die Aufgabe bei jeder Ausführung von EC2Launch v2 ausgeführt werden soll.

Service kann eine Aufgabe nicht ausführen

Auflösung

1. Überprüfen Sie die neuesten Einträge in `%ProgramData%\Amazon\EC2Launch\log\agent.log`.
2. Wenn keine Fehler aufgetreten sind, versuchen Sie, den Service manuell von `"%ProgramFiles%\Amazon\EC2Launch\EC2Launch.exe" run` auszuführen, um festzustellen, ob die Aufgaben ausgeführt werden.

Der Service führt Benutzerdaten mehr als einmal aus

Auflösung

Benutzerdaten werden von EC2Launch v1 und EC2Launch v2 unterschiedlich behandelt. EC2Launch v1 führt Benutzerdaten als geplante Aufgabe auf der Instance aus, wenn `persist` auf `true` gesetzt ist. Wenn `persist` auf `false` festgelegt ist, wird die Aufgabe nicht geplant, selbst wenn sie mit einem Neustart beendet wird oder während der Ausführung unterbrochen wird.

EC2Launch v2 führt Benutzerdaten als Agentenaufgabe aus und verfolgt deren Ausführungsstatus. Wenn Benutzerdaten einen Neustart des Computers ausstellen oder Benutzerdaten während der Ausführung unterbrochen wurden, bleibt der Ausführungsstatus als `pending` bestehen und die Benutzerdaten werden beim nächsten Instance-Start erneut ausgeführt. Wenn Sie verhindern möchten, dass das Benutzerdatenskript mehr als einmal ausgeführt wird, machen Sie das Skript idempotent.

Das folgende Beispiel für ein idempotentes Skript legt den Computer-Namen fest und schließt sich einer Domain an.

```
<powershell>
  $name = $env:computername
  if ($name -ne $desiredName) {
 Rename-Computer -NewName $desiredName
```

```
  }
  $domain = Get-ADDomain
  if ($domain -ne $desiredDomain)
  {
 Add-Computer -DomainName $desiredDomain
  }
  $telnet = Get-WindowsFeature -Name Telnet-Client
  if (-not $telnet.Installed)
  {
 Install-WindowsFeature -Name "Telnet-Client"
  }
</powershell>
<persist>false</persist>
```

Geplante Aufgaben von EC2Launch-v1 werden nach der Migration zu EC2Launch v2 nicht ausgeführt

Auflösung

Das Migrationstool erkennt keine geplanten Aufgaben, die mit EC2Launch-v1-Skripten verknüpft sind. Daher richtet es diese Aufgaben in EC2Launch v2 nicht automatisch ein. Um diese Aufgaben zu konfigurieren, bearbeiten Sie die `agent-config.yml`-Datei oder verwenden Sie das EC2Launch v2-Einstellungsdialogfeld. Wenn eine Instance beispielsweise eine geplante Aufgabe umfasst, die `InitializeDisks.ps1` ausführt, müssen Sie nach dem Ausführen des Migrationstools die Volumes angeben, die Sie im Einstellungsdialogfeld von EC2Launch v2 initialisieren möchten. Siehe Schritt 6 des Verfahrens zu Ändern der Einstellungen mithilfe des Dialogfelds für EC2Launch v2-Einstellungen.

Der Service initialisiert ein EBS-Volume, das nicht leer ist

Auflösung

Bevor ein Volume initialisiert wird, versucht EC2Launch v2 zu erkennen, ob es leer ist. Wenn ein Volume nicht leer ist, überspringt es die Initialisierung. Alle Volumes, die als nicht leer erkannt werden, werden nicht initialisiert. Ein Volume gilt als leer, wenn die ersten 4 KiB eines Volumes leer sind oder wenn ein Volume kein Windows-erkennbares Laufwerkslayout hat. Ein Volume, das auf einem Linux-System initialisiert und formatiert wurde, hat kein Windows-erkennbares Laufwerkslayout, zum Beispiel MBR oder GPT. Daher wird es als leer und initialisiert betrachtet. Wenn Sie diese Daten beibehalten möchten, verlassen Sie sich nicht auf die Erkennung leerer Laufwerke durch EC2Launch v2. Geben Sie stattdessen Volumes an, die Sie im EC2Launch v2-Einstellungsdialogfeld (siehe Schritt 6) oder in `agent-config.yml` initialisieren möchten.

`setWallpaper`Die Aufgabe ist nicht aktiviert, aber das Hintergrundbild wird beim Neustart zurückgesetzt

Die Aufgabe `setWallpaper` erstellt die Verknüpfungsdatei `setwallpaper.lnk` im Startup-Ordner jedes vorhandenen Benutzers. Diese Verknüpfungsdatei wird ausgeführt, wenn sich der Benutzer nach dem Start der Instance zum ersten Mal anmeldet. Hiermit wird die Instance mit einem benutzerdefinierten Hintergrundbild eingerichtet, auf dem die Instance-Attribute zu sehen sind. Durch das Entfernen der Aufgabe `setWallpaper` wird diese Verknüpfungsdatei nicht gelöscht. Sie müssen die Datei manuell oder mithilfe eines Skripts löschen.

Der Verknüpfungspfad lautet:

`$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/setwallpaper.lnk`

Auflösung

Löschen Sie die Datei manuell oder mithilfe eines Skripts.

PowerShell-Beispielskript zum Löschen der Verknüpfungsdatei

```
foreach ($userDir in (Get-ChildItem "C:\Users" -Force -Directory).FullName)
{
 $startupPath = Join-Path $userDir -ChildPath "AppData\Roaming\Microsoft\Windows\Start
 Menu\Programs\Startup"
 if (Test-Path $startupPath)
 {
  $wallpaperSetupPath = Join-Path $startupPath -ChildPath "setwallpaper.lnk"
  if (Test-Path $wallpaperSetupPath)
  {
   Remove-Item $wallpaperSetupPath -Force -Confirm:$false
  }
 }
}
```

Der Dienst hängt im laufenden Status fest

Beschreibung

EC2Launch v2 ist blockiert, mit Protokollmeldungen (`agent.log`) ähnlich der folgenden:

```
2022-02-24 08:08:58 Info:
 ********************************************************************************
```

```
2022-02-24 08:08:58 Info: EC2Launch Service starting
2022-02-24 08:08:58 Info: Windows event custom log exists: Amazon EC2Launch
2022-02-24 08:08:58 Info: ACPI SPCR table not supported. Bailing Out
2022-02-24 08:08:58 Info: Serial port is in use. Waiting for Serial Port...
2022-02-24 08:09:00 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:02 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:04 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:06 Info: ACPI SPCR table not supported. Use default console port.
```

Mögliche Ursache

SAC ist aktiviert und verwendet die serielle Schnittstelle. Weitere Informationen finden Sie unter SAC zur Fehlerbehhebung von Windows-Instances verwenden.

Auflösung

Versuchen Sie, das Problem wie folgt zu beheben:

- Deaktivieren Sie den Dienst, der den seriellen Port verwendet.
- Wenn Sie möchten, dass der Dienst weiterhin den seriellen Port verwendet, schreiben Sie benutzerdefinierte Skripte, um Launch-Agent-Aufgaben auszuführen, und rufen Sie diese als geplante Aufgaben auf.

Ungültige **`agent-config.yml`** verhindert das Öffnen des Dialogfelds für EC2Launch-v2-Einstellungen

Beschreibung

Die Einstellungen für EC2Launch v2 versuchen, dieselbe `agent-config.yml`-Datei zu analysieren, bevor sie das Dialogfeld öffnen. Wenn die YAML-Konfigurationsdatei nicht dem unterstützten Schema folgt, zeigt das Dialogfeld den folgenden Fehler an:

```
Unable to parse configuration file agent-config.yml. Review configuration file. Exiting application.
```

Auflösung

1. Stellen Sie sicher, dass die Konfigurationsdatei dem unterstützten Schema entspricht.
2. Wenn Sie von vorne anfangen möchten, kopieren Sie die Standardkonfigurationsdatei in `agent-config.yml`. Sie können das Beispiel`agent-config.yml` im Abschnitt „Aufgabenkonfiguration“ verwenden.

3. Sie können auch von vorne beginnen, indem Sie `agent-config.yml` löschen. Die Einstellungen für EC2Launch v2 generieren eine leere Konfigurationsdatei.

`task:executeScript should be unique and only invoked once`

Beschreibung

Eine Aufgabe nicht in derselben Phase wiederholt werden kann.

Auflösung

Einige Aufgaben müssen als Array eingegeben werden, z. B. executeScript und executeProgram. Ein Beispiel für das Schreiben des Skripts als Array finden Sie unter executeScript.

Windows-Ereignisprotokolle

EC2Launch v2 veröffentlicht Windows-Ereignisprotokolle für wichtige Ereignisse, z. B. Servicestart, Windows ist bereit und Erfolg und Misserfolg von Aufgaben. Ereignis-IDs identifizieren eindeutig ein bestimmtes Ereignis. Jedes Ereignis enthält Informationen zu Phase, Aufgabe und Ebene sowie eine Beschreibung. Sie können mithilfe der Ereignis-ID Auslöser für bestimmte Ereignisse festlegen.

Event-IDs liefern Informationen über ein Ereignis und identifizieren einige Ereignisse eindeutig. Die am wenigsten signifikante Ziffer einer Ereignis-ID gibt den Schweregrad eines Ereignisses an.

Veranstaltung	Am wenigsten bedeutende Ziffer
`Success`	`. . .0`
`Informational`	`. . .1`
`Warning`	`. . .2`
`Error`	`. . .3`

Dienstbezogene Ereignisse, die beim Start oder Ende des Dienstes generiert werden, enthalten eine einstellige Ereigniskennung.

Veranstaltung	Einstellige ID
`Success`	`0`

Veranstaltung	Einstellige ID
`Informational`	1
`Warning`	2
`Error`	3

Die Ereignisnachrichten für `EC2LaunchService.exe`-Ereignisse beginnen mit `Service:`. Die Ereignisnachrichten für `EC2Launch.exe`-Ereignisse beginnen nicht mit `Service:`.

Vierstellige Ereignis-IDs enthalten Informationen über die Phase, Aufgabe und den Schweregrad eines Ereignisses.

Themen

- Format der Ereignis-ID
- Beispiele für Ereignis-IDs
- Windows-Ereignisprotokollschema

Format der Ereignis-ID

Die folgende Tabelle zeigt das Format einer EC2Launch v2-Ereignis-ID.

3	2 1	0
S	T	L

Die Buchstaben und Zahlen in der Tabelle stehen für die folgenden Ereignistypen und Definitionen.

Ereignistyp	Definition
S (Stage)	0 - Nachricht auf Service-Ebene 1 - Boot 2 - Netzwerk

Ereignistyp	Definition
	3 - PreReady 5 - Windows ist bereit 6 - PostReady 7 - Benutzerdaten
T (Aufgabe)	Die Aufgaben, die durch die entsprechenden beiden Werte dargestellt werden, sind für jede Phase unterschiedlich. Informationen zur vollständigen Liste der Ereignisse finden Sie unter Windows-Ereignisprotokollschema.
L (Ebene des Ereignisses)	0 - Erfolg 1 - Informativ 2 - Warnung 3 - Fehler

Beispiele für Ereignis-IDs

Nachfolgend finden Sie Beispiele für Ereignis-IDs.

- `5000` - Windows ist einsatzbereit
- `3010` - Aktivieren der Windows-Aufgabe in der PreReady-Phase war erfolgreich
- `6013` - Beim Festlegen der Hintergrundbildaufgabe in PostReady Local Data Stadium ist ein Fehler aufgetreten

Windows-Ereignisprotokollschema

MessageID/Ereignis-ID	Ereignismeldung
. . .0	Success
. . .1	Informational
. . .2	Warning
. . .3	Error
x	EC2Launch service-level logs
0	EC2Launch service exited successfully
1	EC2Launch service informational logs
2	EC2Launch service warning logs
3	EC2Launch service error logs
10	Replace state.json with previous-state.json
100	Serial Port
200	Sysprep
300	PrimaryNic
400	Metadata
x000	Stage (1 digit), Task (2 digits), Status (1 digit)
1000	Boot
1010	Boot - extend_root_partition

MessageID/Ereignis-ID	Ereignismeldung
2000	Network
2010	Network - add_routes
3000	PreReady
3010	PreReady - activate_windows
3020	PreReady - install_egpu_manager
3030	PreReady - set_monitor_on
3040	PreReady - set_hibernation
3050	PreReady - set_admin_account
3060	PreReady - set_dns_suffix
3070	PreReady - set_wallpaper
3080	PreReady - set_update_schedule
3090	PreReady - output_log
3100	PreReady - enable_open_ssh
5000	Windows is Ready to use
6000	PostReadyLocalData
7000	PostReadyUserData
6010/7010	PostReadyLocal/UserData - set_wallpaper
6020/7020	PostReadyLocal/UserData - set_update_schedule

MessageID/Ereignis-ID	Ereignismeldung
6030/7030	PostReadyLocal/UserData - set_hostname
6040/7040	PostReadyLocal/UserData - execute_program
6050/7050	PostReadyLocal/UserData - execute_script
6060/7060	PostReadyLocal/UserData - manage_package
6070/7070	PostReadyLocal/UserData - initialize_volume
6080/7080	PostReadyLocal/UserData - write_file
6090/7090	PostReadyLocal/UserData - start_ssm
7100	PostReadyUserData - enable_open_ssh
6110/7110	PostReadyLocal/UserData - enable_jumbo_frames

EC2Launch v2-Konsolenprotokollausgabe

Dieser Abschnitt enthält eine Beispielausgabe des Konsolenprotokolls für EC2Launch v2 und führt alle Fehlermeldungen des EC2Launch v2-Konsolenprotokolls auf, mit denen Sie Probleme beheben können. Weitere Informationen über die Ausgabe der Instance-Konsole und wie Sie darauf zugreifen können, finden Sie unter the section called “Instance-Konsolenausgabe”.

Outputs

- EC2Launch v2-Konsolenprotokollausgabe

- EC2Launch v2-Konsolenprotokollmeldungen

EC2Launch v2-Konsolenprotokollausgabe

Im Folgenden finden Sie eine Beispiel-Konsolenprotokollausgabe für EC2Launch v2. Einige Werte in diesem Beispiel werden durch repräsentativen Text ersetzt, der von geschweiften Klammern umgeben ist.

```
2025/07/22 21:26:53Z: Windows sysprep configuration complete.
2025/07/22 21:26:53Z: Message: Waiting for access to metadata...
2025/07/22 21:26:53Z: Message: Meta-data is now available.
2025/07/22 21:26:53Z: AMI Origin Version: 2024.12.13
2025/07/22 21:26:53Z: AMI Origin Name: Windows_Server-2022-English-Full-Base
2025/07/22 21:26:53Z: OS: Microsoft Windows NT 10.0.20348
2025/07/22 21:26:53Z: OsVersion: 10.0
2025/07/22 21:26:53Z: OsProductName: Windows Server 2022 Datacenter
2025/07/22 21:26:53Z: OsBuildLabEx: 20348.1.amd64fre.fe_release.210507-1500
2025/07/22 21:26:53Z: OsCurrentBuild: 20348
2025/07/22 21:26:53Z: OsReleaseId: 2009
2025/07/22 21:26:53Z: Language: en-US
2025/07/22 21:26:53Z: TimeZone: UTC
2025/07/22 21:26:53Z: Offset: UTC +0000
2025/07/22 21:26:53Z: Launch: EC2 Launch v2.2.63
2025/07/22 21:26:53Z: AMI-ID: ami-1234567890abcdef1
2025/07/22 21:26:53Z: Instance-ID: i-1234567890abcdef0
2025/07/22 21:26:54Z: Instance Type: t3.xlarge
2025/07/22 21:26:54Z: Driver: AWS NVMe Driver v1.6.0.35
2025/07/22 21:26:54Z: SubComponent: 1.6.0.35; EnableSCSIPersistentReservations: 0
2025/07/22 21:26:54Z: Driver: AWS PV Driver Package v8.5.0
2025/07/22 21:26:55Z: Driver: Amazon Elastic Network Adapter v2.8.0.0
2025/07/22 21:26:55Z: HOSTNAME: EC2AMAZ-9FJG5CC
2025/07/22 21:26:55Z: RDPCERTIFICATE-SUBJECTNAME: {certificate subject name}
2025/07/22 21:26:55Z: RDPCERTIFICATE-THUMBPRINT: {thumbprint hash}
2025/07/22 21:26:56Z: SSM: Amazon SSM Agent v3.3.2746.0
2025/07/22 21:26:57Z: User data format: no_user_data
2025/07/22 21:26:57Z: EC2LaunchTelemetry: IsTelemetryEnabled=true
2025/07/22 21:26:57Z: EC2LaunchTelemetry: AgentOsArch=windows_amd64
2025/07/22 21:26:57Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2025/07/22 21:26:57Z: EC2LaunchTelemetry: AgentCommandErrorCode=1
2025/07/22 21:26:57Z: EC2LaunchTelemetry: AdminPasswordTypeCode=0
2025/07/22 21:26:57Z: EC2LaunchTelemetry: AgentErrorLocation=execute_windows.go:410
2025/07/22 21:26:57Z: EC2LaunchTelemetry: IpConflictDetectionCode=0
2025/07/22 21:26:57Z: Message: Windows is Ready to use
```

```
{"type":"EC2AgentTelemetry","agentId":"WindowsLaunchAgentV2", ...}
{"type":"EC2AgentTelemetry","agentId":"WindowsLaunchAgentV2", ...}
```

EC2Launch v2-Konsolenprotokollmeldungen

Im Folgenden finden Sie eine Liste aller EC2Launch v2-Konsolenprotokollmeldungen.

```
Error EC2Launch service is stopping. {error message}
```

Einzelheiten zum Fehler beim Beenden des Services:

- `Error setting up EC2Launch agent folders`
- `See instance logs for detail`
- `Error stopping service`
- `Error initializing service`

```
Windows sysprep configuration complete
```

```
Invalid administrator username: {invalid username}
```

```
Invalid administrator password
Username: {username}
Password: <Password>{encrypted password}</Password>
```

Die folgende Nachricht ist ein Informationsblock, der AMI-Details enthält:

```
AMI Origin Version: {amiVersion}
AMI Origin Name: {amiName}
Microsoft Windows NT {currentVersion}.{currentBuildNumber}
OsVersion: {currentVersion}
OsProductName: {productName}
OsBuildLabEx: {buildLabEx}
OsCurrentBuild: {currentBuild}
OsReleaseId: {releaseId}
Language: {language}
TimeZone: {timeZone}
Offset: UTC {offset}
```

```
Launch agent: EC2Launch {BuildVersion}
AMI-ID: {amiId}
Instance-ID: {instanceId}
Instance Type: {instanceType}
HOSTNAME: {computer name}
RDPCERTIFICATE-SUBJECTNAME: {certificate subject name}
RDPCERTIFICATE-THUMBPRINT: {thumbprint hash}
SqlServerBilling: {sql billing}
SqlServerInstall: {sql patch leve, edition type}
Driver: AWS NVMe Driver {version}
Driver: Inbox NVMe Driver {version}
Driver: AWS PV Driver Package {version}
Microsoft-Hyper-V is installed.
Unable to get service status for vmms
Microsoft-Hyper-V is {status}
SSM: Amazon SSM Agent {version}
AWS VSS Version: {version}
```

```
Windows sysprep configuration complete.
Windows is being configured. 'SysprepState is {state}'
Windows is still being configured. 'SysprepState is {state}'
Windows is Ready to use
Waiting for access to metadata...
Meta-data is now available.
Metadata is not available for this instance.
Timed out waiting for access to metadata.
User data format: {format}
```

Telemetriemeldungen von EC2Launch v2 enthalten die Eigenschaftswerte der Starttelemetrie. Ab Version 2.2.63 werden die Telemetriedaten des EC2-Agenten als JSON-Objekt formatiert.

```
EC2LaunchTelemetry: {telemetry property}
```

```
{"type":"EC2AgentTelemetry","agentId":"WindowsLaunchAgentV2" ... }
```

EC2Versionsverläufe von Launch v2

Versionsverläufe

- EC2Versionsverlauf für Version 2 starten

EC2Versionsverlauf für Version 2 starten

Informationen dazu, wie Sie sicherstellen können, dass Sie den neuesten Startagenten installiert haben, finden Sie unter Installieren der neuesten Version von EC2Launch v2. Sie können Benachrichtigungen erhalten, wenn neue Versionen des EC2 Launch v2-Agents veröffentlicht werden. Weitere Informationen finden Sie unter Benachrichtigungen von EC2-Windows-Start-Agenten abonnieren.

In der folgenden Tabelle werden die veröffentlichten Versionen von EC2 Launch v2 beschrieben.

Version	Details	Datum der Veröffentlichung
2.3.56	• Es wurde ein Problem behoben, bei dem vorkonfigurierte persistente Netzwerkrouten von EC2 Launch v2 nicht richtig verarbeitet wurden.	4. November 2025
2.3.5	• Verbesserte Erkennung der primären Netzwerkschnittstelle mithilfe von IMDS beim Hinzufügen von Routen.	15. September 2025
2.2.63	• Der Startagent wurde aktualisiert, um Telemetrie zu verbessern.	29. Juli 2025
2.1.1	• Vollständige Unterstützung für hinzugefügt. IPv6	14. Mai 2025
2.0.2107	• Das Hinzufügen von Routen wurde verbessert, um Szenarien zu bewältigen, IPv4 in denen IPv6 Adressen auf der Schnittstelle nicht verfügbar sind.	27. März 2025
2.0.2081	• Es wurde ein Problem behoben, bei dem RDP-Zertifikatsinformationen nicht ordnungsgemäß abgerufen oder validiert wurden. Es wurde eine Funktion hinzugefügt, mit der die Remotedesktopservices bei Bedarf automatisch gestartet werden können.	4. Februar 2025

Version	Details	Datum der Veröffentlichung
	• Die Dienstberechtigungen für EC2 Launch v2 wurden angepasst, um ein Problem zu beheben, das bei der Abfrage des Dienststatus auftrat.	
2.0.2046	• Der Hintergrundpfad in der `agent-config.yml` -Datei wurde aktualisiert, sodass er den Standardpfad für das Hintergrundbild des Betriebssystems verwendet. • Es wurde Telemetrie hinzugefügt, um die Standorte zu überwachen, an denen Agentenfehler aufgetreten sind. • Agentenprotokollmeldungen wurde aktualisiert.	3. Oktober 2024
2.0.1981	• Aktualisierte `EC2Launch.exe` -CLI-Befehlsfehlermeldungen für Benutzer ohne Administratorrechte.	6. August 2024
2.0.1948	• Telemetrie wurde hinzugefügt, um die Verwendung der Administratorpasswortoptionen zu überwachen. • Geänderte EC2 Startberechtigungen.	1. Juli 2024
2.0.1924	• Die Benutzeroberfläche mit den EC2 Starteinstellungen wurde aktualisiert. • Der CLI-Befehl für das Hintergrundbild wurde aktualisiert. • Das EC2 Launch-Installationsprogramm wurde aktualisiert.	10. Juni 2024

Version	Details	Datum der Veröffentlichung
2.0.1914	• Fügen Sie Routen mit nicht spezifizierten Gateway-Adressen hinzu (`0.0.0.0`für IPv4 oder `::` fürIPv6). • Fügen Sie immer sowohl als auch IPv6 Routen IPv4 hinzu. • Es wurde ein Problem behoben, bei dem der `Administrator` -Benutzername zur `agent-config.yml` -Datei hinzugefügt wurde, obwohl er nicht angegeben wurde. • Geänderte EC2 Launch v2-Berechtigungen.	5. Juni 2024
2.0.1881	• Der Aufgabe `setAdminAccount` wurde eine Option für ein verschlüsseltes Passwort hinzugefügt. • CLI-Befehl zum Verschlüsseln des statischen Passworts in agent-config.yml hinzugefügt. • Es wurde ein Problem behoben, bei dem XML-Benutzerdaten keine PowerShell Argumente hinzufügen, wenn sie mit Administratorrechten ausgeführt wurden. Weitere Details finden Sie unter Wie Amazon EC2 mit Benutzerdaten für Windows-Instances umgeht. • Die PowerShell Argumente für die `executeScript` Aufgaben- und Benutzerdatenskripts wurden angepasst, wenn sie mit `LocalSystem` Berechtigungen ausgeführt wurden. Wenn die Argumente leer sind, verwendet der Agent den folgenden Standardwert: `-ExecutionPolicy Unrestricted` . • Das Drucken doppelter Treiberversionen in das Konsolenprotokoll wurde verhindert.	8. Mai 2024

Version	Details	Datum der Veröffentlichung
2.0.1815	• Die Fehlerbehandlung wurde so angepasst, dass sie bei kritischen Einrichtungsproblemen vor Sysprep fehlschlägt. • Es wurde ein Problem behoben, bei dem Hintergrundbild- und Host-Namenaufgaben in Instances, denen mehrere IP-Adressen der primären Netzwerkschnittstelle zugewiesen waren, eine falsche IP-Adresse verwenden konnten. • Die Aufgaben für Hintergrundbild und Host-Name wurden dahingehend geändert, dass sie zuerst private IP-Adressen von IMDS abrufen und dann wieder zu WMI zurückkehren, wenn IMDS deaktiviert ist. • Es wurde ein Problem mit der `initializeVolume` -Aufgabe behoben, bei dem `sc1`-Volumes aufgrund eines vorübergehenden Fehlers nicht initialisiert werden konnten.	6. März 2024
2.0.1739	• Es wurde ein Problem behoben, das verhinderte, dass Exit-Codes von `executeScript` -Aufgaben erfasst wurden, die als Windows-Administratorbenutzer ausgeführt wurden.	17. Januar 2024

Version	Details	Datum der Veröffentlichung
2.0.1702	• Eingeschränkte `Telemetry.log` Berechtigungen `read-execute` nur für Standardbenutzer. • Der EC2 Launch Windows-Dienst wurde so konfiguriert, dass er bei einem Startfehler neu gestartet wird. • `add-routes` Fehler wurden durch Protokollierung der Ausgabe umsetzbar gemacht. `route.exe stderr` • Es wurde ein Problem behoben, das auftritt, wenn Routenmetriken außerhalb des Bereichs [1, 9999] liegen. • Mehrere neue Instance-Typen unterstützen jetzt Bildschirmhintergründe. • Es wurde ein Problem behoben, das durch Skripte für Benutzerdaten verursacht wurde, die als Windows-Administrator ausgeführt werden und Ausgaben an `stderr`senden.	04. Januar 2024

Version	Details	Datum der Veröffentlichung
2.0.1643	• Das `ebsnvme-id.exe` -Tool wurde auf Version 1.1.0.7 aktualisiert. • Es wurde ein Problem mit den Einstellungen für die empfangsseitige Skalierung (RSS, Receive Side Scaling) und Receive Queue Depth bei Metal-Instance-Typen behoben, die mit 'metal-*' beginnen, wie z. B. metal-48x1. • Das Telemetrieereignis, das über XML-Benutzerdatenbefehle berichtet, die den Agenten blockieren, wurde entfernt. • Die `setDnsSuffix` -Aufgabe wurde aktualisiert, um die Übertragung von Domainnamen auf der Grundlage eines Registrierungseintrags einzuschränken: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Es wurden eine öffentliche Aufgabe und eine CLI hinzugefügt, die Netzwerkrouten hinzufügt. • Hinweis – Dies ist die letzte Version, die offiziell Windows Server 2012 unterstützt. • Hinweis – Dies ist die letzte Version, die offiziell 32-Bit-Betriebssysteme unterstützt.	04. Oktober 2023

Version	Details	Datum der Veröffentlichung
2.0.1580	• Die Art und Weise, wie der Launch-Agent Fehler behandelt, wenn Sie die Berechtigungen für Protokolldateien ändern, wurde geändert. • Es wurde ein Timeout für die Verbindung zur seriellen Schnittstelle hinzugefügt. Das Timeout ermöglicht es dem Launch-Agent, weiter zu laufen, wenn die serielle Schnittstelle verwendet wird.	5. September 2023

Version	Details	Datum der Veröffentlichung

2.0.1521	• Die –block-Markierung der EC2Launch.exe reset- und sysprep-Befehle ist veraltet.
	• EC2Launch.exe wurde aktualisiert, um die reset- und sysprep-Befehle zu erkennen und zu verarbeiten, die in Inline-executeScript -Aufgaben verwendet werden. Diese Befehle führen dazu, dass der Agent nicht mehr ausgeführt wird, nachdem die executeScript -Aufgabe diese ausgeführt hat.
	• Aktualisierte XML-Benutzerdatenskripte, sodass sie standardmäßig inline ausgeführt werden.
	• Ermöglichen Sie die getrennte Ausführung von XML-Benutzerdatenskripten mit dem neuen detach-Tag. Weitere Details finden Sie unter Benutzerdatenskripts.
	• Die folgenden Änderungen wurden am Agentenprotokoll vorgenommen.
	  • Aktualisierte Agentenprotokollmeldungen.
	  • executeScript -Inhalt und Ausgabe aus dem Agentenprotokoll entfernt.
	  • executeProgram -Argumente und Ausgabe aus dem Agentenprotokoll entfernt.
	• Die folgenden Änderungen wurden am Konsolenprotokoll vorgenommen.
	  • Der EnableSCSIPersistentReservations -Wert wurde dem Konsolenprotokoll hinzugefügt.
		03. Juli 2023

Version	Details	Datum der Veröffentlichung
2.0.1303	• Zusätzliche Fehlerbehandlung und Protokollzeilen beim Hinzufügen von Netzwerkrouten wurden hinzugefügt. • Erlaubt `executeScript` und `executeProgram` Aufgaben in der PreReady Phase. • Die Aufgabe `executeProgram` wurde aktualisiert, um Ausgabedateien zu generieren, die der Ausgabe der ExecuteScript-Aufgabe ähneln. Weitere Informationen finden Sie unter executeProgram. • Telemetrie wurde hinzugefügt, um die Verwendung von blockierenden Agentenbefehlen in XML-Benutzerdaten zu überwachen.	3. Mai 2023
2.0.1245	• Verbesserte Transparenz bei Abstürzen durch die Protokollierung von Crash-Call-Stacks im Klartext. • Der EventLog Service wurde als Startabhängigkeit hinzugefügt, um einen Absturz zu beheben, wenn der Amazon EC2 Launch-Service schneller startet als der EventLog Service. • XML-Benutzerdaten wurden vor der PostReady Phase aus der Agentenkonfigurationsdatei ausgeführt (wie EC2 Launch v1 und EC2 Config). • YAML-Benutzerdaten Version 1.1 wurden hinzugefügt, damit Benutzerdaten vor der PostReady Phase aus der Agentenkonfigurationsdatei ausgeführt werden (YAML-Benutzerdaten Version 1.0 werden nach der PostReady Phase aus der Agentenkonfigurationsdatei ausgeführt).	08. März 2023

Version	Details	Datum der Veröffentlichung
2.0.1173	• Fügt ein optionales Feature zur Anzeige von Instance-Tags auf dem Hintergrundbild hinzu. Weitere Informationen finden Sie unter setWallpaper . • Fügt eine Fehlerbehandlung hinzu, wenn die Sicherheitsgruppe für Elastic Graphics nicht richtig eingerichtet ist. • Behebt eine Zeitüberschreitung, wenn der Instance-Metadaten-Service nicht aktiviert ist.	06. Februar 2023
2.0.1121	• Behebt ein Problem, bei dem ein 404-Fehler auf dem Hintergrundbild angezeigt wird, wenn keine öffentliche IPv4 Adresse zugewiesen ist. • Behebt ein Problem, bei dem das Dateisystem des Volumes als `RAW` anstelle von `NTFS` formatiert wird, wenn der Laufwerksbuchstabe des Geräts auf `D` eingestellt ist. • Behebt ein Problem, bei dem NVMe SSD-Volumes fälschlicherweise als EBS-Volumes identifiziert wurden. • Behebt einen Fehler beim Aktivieren von Windows, wenn IMDS deaktiviert ist.	4. Januar 2023

Version	Details	Datum der Veröffentlichung
2.0.1082	• Behebt ein Problem, bei dem das `setWallpaper : privateIpAddress` -Feld leer ist, wenn IMDS deaktiviert ist. • Behebt ein Problem beim Setzen des Hostnamens auf die private IPv4 Adresse, wenn IMDS deaktiviert ist. • Behebt ein Problem mit der Initialisierung von Volumes auf Windows Server 2012. • Behebt ein Problem mit der Einstellung von Jumbo-Frames. • Behebt einen Fehler, wenn beim Start der Instance kein SSH-Schlüssel angegeben wurde. • Behebt einen Fehler auf Windows Server 2012, wenn Windows keinen Registrierungsschlüssel 'ReleaseId' hat.	7. Dezember 2022
2.0.1011	• Behebt die Logik für die Suche nach Netzwerkadaptern, wenn die PDevice Pn-ID leer ist.	11. November 2022
2.0.1009	• Verwendet PCI-Segmentinformationen, um den Konsolenport auszuwählen.	8. November 2022

Version	Details	Datum der Veröffentlichung
2.0.982	• Fügt eine Wiederholungslogik zum Abrufen von RDP-Informationen hinzu. • Behebt Fehler bei der Volume-Initialisierung auf `d2.8xlarge` -Instances. • Behebt ein Problem, bei dem nach einem Neustart ein falscher Netzwerkadapter ausgewählt werden kann. • Entfernt eine Fehlalarm-Fehlermeldung, wenn ACPI SPCR nicht verfügbar ist.	31. Oktober 2022
2.0.863	• Aktualisiert die IMDS-Wartelogik, sodass nur Anfragen gestellt werden. IMDSv2 • Fügt Logik hinzu, um Laufwerksbuchstaben Volumes zuzuweisen, die bereits initialisiert, aber nicht gemountet sind. • Druckt eine genauere Fehlermeldung, wenn der Schlüsselpaartyp nicht unterstützt wird. • Behebt einen 3010-Neustartcode-Fehler. • Fügt eine Überprüfung auf ungültige base64-verschlüsselte Benutzerdaten hinzu.	6. Juli 2022
2.0.698	• Rechtschreibfehler in der Protokollausgabe beim Ausführen von Skripten behoben.	30. Januar 2022

Version	Details	Datum der Veröffentlichung
2.0.674	• Telemetrie lädt die Datenschutzkontrolle hoch. enabled/disabled • Behebt den Fehler `index out of bounds`. • Entfernt Hintergrundverknüpfungen während `sysprep`.	15. November 2021
2.0.651	• Fügt eine Logik zur Deinstallation älterer Agenten während der EC2 Launch v2-Installation hinzu. • Behebt ein Problem mit dem CLI-Befehl `list-volume` , wenn das Root-Volume nicht als Volume 0 aufgeführt ist.	7. Oktober 2021
2.0.592	• Behebt Fehler, um den Status der Phase korrekt zu melden. • Entfernt Fehlalarmfehlermeldungen, wenn Protokolldateien geschlossen werden. • Fügt Telemetrie hinzu.	31. August 2021
2.0.548	• Fügt führende Nullen für Hex-IP-Hostnamen hinzu. • Behebt Dateiberechtigungen für `enableOpenSsh` -Aufgabe. • Behebt den Absturz des Sysprep-Befehls.	4. August 2021

Version	Details	Datum der Veröffentlichung
2.0.470	• Behebt einen Fehler in der Netzwerkphase, um zu warten, bis DHCP der Instance eine IP zuweist. • Behebt einen Fehler mit `setDnsSuffix` , wenn `SearchList` -Registrierungsschlüssel nicht vorhanden ist. • Behebt Fehler in DNS-Devolutionslogik in `setDnsSuffix` . • Fügt Netzwerkrouten nach Zwischenneustarts hinzu. • Erlaubt `initializeVolume` , um vorhandene Volumes neu zu schreiben. • Entfernt zusätzliche Informationen aus dem Unterbefehl Version.	20. Juli 2021
2.0.285	• Fügt die Option hinzu, Benutzerskripte in einem separaten Prozess auszuführen. • Legacy-Benutzerdaten (XML-Benutzerdaten) werden jetzt in einem losgelösten Prozess ausgeführt, der dem früheren Start-Agenten ähnlich ist. • Fügt `sysprep` und `reset`-Befehlen die CLI-Flag hinzu, die es ihnen ermöglichen, zu blockieren, bis der Dienst beendet ist. • Schränkt die Berechtigungen für den Konfigurationsordner ein.	8. März 2021

Version	Details	Datum der Veröffentlichung
2.0.207	• Fügt der `setHostName` -Aufgabe ein optionales `hostName`-Feld hinzu. • Behebt den Neustartfehler. Die Neustartaufgaben `executeScript` und `executeProgram` werden als „in Ausführung“ markiert. • Fügt dem Status-Befehl weitere Rückgabekodes hinzu. • Fügt einen Ladeprogramm-Dienst hinzu, um das Startup-Problem bei der Ausführung auf `t2.nano`-Instance-Typ zu beheben • Behebt den Bereinigungsinstallationsmodus, um Dateien zu entfernen, die vom Installationsprogramm nicht verfolgt werden	2. Februar 2021
2.0.160	• Behebt den `validate`-Befehl, um einen ungültigen Phasennamen zu erkennen. • Fügt den `w32tm resync`-Befehl in die `addroutes` -Aufgabe hinzu. • Behebt das Problem mit der Änderung der DNS-Suffixsuchreihenfolge. • Fügt Prüfbedingungen hinzu, um ungültige Benutzerdaten besser zu melden.	4. Dezember 2020
2.0.153	Fügt Sysprep-Funktionalität hinzu. UserData	3. November 2020

Version	Details	Datum der Veröffentlichung
2.0.146	• Behebt ein Problem mit einer anderen Sprache als RootExtend Englisch. AMIs • Erteilt Benutzergruppen Schreibberechtigung für Protokolldateien. • Erstellt MS-Reserved-Partition für GPT-Volumes. • Fügt den Befehl list-volumes und das Volume-Dropdown in den Amazon EC2 Launch-Einstellungen hinzu. • Fügt einen get-agent-config Befehl zum Drucken der Datei agent-config.yml im Yaml- oder JSON-Format hinzu. • Löscht das statische Passwort, wenn kein öffentlicher Schlüssel erkannt wurde.	6. Oktober 2020
2.0.124	• Fügt eine Option hinzu, um die OS-Version auf dem Bildschirmhintergrund anzuzeigen. • Initialisiert verschlüsselte EBS-Volumes. • Fügt Routen für VPCs ohne lokalen DNS-Namen hinzu.	10. September 2020
2.0.104	• Erstellt die DNS-Suffix-Suchliste, wenn keine vorhanden ist. • Überspringt den Ruhezustand, wenn nicht angefordert.	12. August 2020
2.0.0	Erstversion.	30. Juni 2020

Den EC2Launch-v1-Agenten verwenden, um Aufgaben während des Starts einer EC2-Windows-Instance auszuführen

Amazon-verwaltete AMIs für Windows Server 2016 und 2019 enthalten eine Reihe von Windows-Powershell-Skripts mit der Bezeichnung EC2Launch. EC2Launch führt während des ersten Starts der Instance einige Aktionen durch. Informationen zu den EC2Launch-Versionen, die in AWS-Windows-AMIs enthalten sind, finden Sie in der AMI–Referenz für AWS Windows.

> **Note**
>
> Der neueste Start-Agent für Windows Server 2016 und spätere Betriebssystem-Versionen ist EC2Launch v2, der sowohl EC2Config als auch EC2Launch ersetzt und auf AMIs von AWS Windows Server 2016 und 2019 mit Namen, die mit `EC2LaunchV2-Windows_Server-*` beginnen, vorinstalliert ist. Sie können den Agent auch manuell auf Windows Server 2016 und 2019 installieren und konfigurieren. Weitere Informationen finden Sie unter EC2Launch v2 installieren.
>
> Zur Verwendung von EC2Launch mit IMDSv2 muss die Version 1.3.2002730 oder höher vorhanden sein.

Sie können den folgenden Windows-PowerShell-Befehl verwenden, um die installierte Version von EC2Launch zu überprüfen.

```
Test-ModuleManifest -Path "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1" | Select Version
```

EC2Launch-Aufgaben

EC2Launch führt beim ersten Starten einer Instance standardmäßig die folgenden Aufgaben aus:

- Richtet einen neuen Bildschirmhintergrund ein, der Informationen über die Instance gibt.
- Setzt den Computernamen auf die private IPv4-Adresse der Instance.
- Sendet Instance-Informationen an die Amazon EC2-Konsole.
- Sendet den RDP-Zertifikat-Thumbprint an die EC2-Konsole.
- Richtet ein zufälliges Passwort für das Administratorkonto ein.
- Fügt DNS-Suffixe hinzu.

- Erweitert die Betriebssystempartition dynamisch mit nicht partitioniertem Speicherplatz.
- Führt Benutzerdaten aus (falls angegeben). Weitere Informationen zur Angabe von Benutzerdaten finden Sie unter Befehle ausführen, wenn Sie eine EC2 Instance mit Benutzerdateneingabe starten.
- Stellt persistente statische Routen so ein, dass sie den Metadaten-Service und AWS KMS-Server erreichen.

> **Important**
>
> Wenn aus dieser Instance ein benutzerdefiniertes AMI erstellt wird, werden diese Routen als Teil der OS-Konfiguration erfasst. Alle neuen Instances, die über dieses AMI gestartet werden, übernehmen ungeachtet der Subnetz-Platzierung dieselben Routen. Informationen zum Aktualisieren dieser Routen finden Sie unter Aktualisieren von Metadaten/KMS-Routen für Server 2016 und höher beim Starten eines benutzerdefinierten AMI.

Die folgenden Aufgaben tragen dazu bei, die Abwärtskompatibilität mit dem EC2Config-Service zu erhalten. Sie können EC2Launch auch zur Ausführung dieser Aufgaben beim Startup konfigurieren:

- Initialisieren von sekundären EBS-Volumes.
- Senden von Windows-Ereignisprotokollen an die EC2-Konsolenprotokolle.
- Senden der Windows ist einsatzbereit-Meldung an die EC2-Konsole.

EC2Launch-Verzeichnisstruktur

EC2Launch wird bei AMIs mit Windows Server 2016 und höher standardmäßig im Stammverzeichnis installier `C:\ProgramData\Amazon\EC2-Windows\Launch`.

> **Note**
>
> Windows blendet Dateien und Ordner unter standardmäßig au `C:\ProgramData`. Um die EC2Launch-Verzeichnisse und -Dateien anzuzeigen, müssen Sie entweder den Pfad im Windows Explorer eingeben oder die Ordnereigenschaften so ändern, dass ausgeblendete Dateien und Ordner angezeigt werden.

Das Verzeichnis `Launch` enthält die folgenden Unterverzeichnisse.

- `Scripts` — Enthält die PowerShell-Scripts, aus denen EC2Launch besteht.
- `Module` — Enthält das Modul zum Aufbau von Amazon EC2-Scripts.
- `Config` — Enthält Script-Konfigurationsdateien, die Sie anpassen können.
- `Sysprep` — Enthält Sysprep-Ressourcen.
- `Settings` — Enthält eine Anwendung für die grafische Benutzeroberfläche von Sysprep.
- `Library`: Enthält freigegebene Bibliotheken für EC2-Startagenten.
- `Log` – Enthält Unterverzeichnisse für Skripts und die Protokolldateien, die von den Skripten generiert werden.

Telemetrie

Telemetrie ist zusätzliche Information, die AWS hilft, Ihre Anforderungen besser zu verstehen, Probleme zu diagnostizieren und Features bereitzustellen, um Ihre Erfahrung mit AWS-Services zu verbessern.

EC2Launch-Version `1.3.2003498` und später erfassen Telemetriedaten wie Nutzungsmetriken und Fehler. Diese Daten werden von der Amazon-EC2-Instance erfasst, auf der EC2Launch ausgeführt wird. Dies umfasst alle Windows-AMIs, die gehören AWS.

EC2Launch erfasst folgende Telemetrie-Typen:

- Nutzungsinformationen – Agent-Befehle, Installationsmethode und geplante Ausführungsfrequenz.
- Fehler und Diagnoseinformationen – Agent-Installation und Ausführen von Fehlercodes.

Beispiele für die gesammelten Daten:

```
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsUserDataScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandCode=1
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandErrorCode=5
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallCode=2
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallErrorCode=0
```

Die Telemetrie ist standardmäßig aktiviert. Sie können die Telemetriesammlung jederzeit deaktivieren. Wenn Telemetrie aktiviert ist, sendet EC2Launch Telemetriedaten ohne zusätzliche Kundenbenachrichtigungen.

Ihre Entscheidung, Telemetrie zu aktivieren oder zu deaktivieren, wird erfasst.

Sie können die Telemetriesammlung aktivieren oder deaktivieren. Ihre Auswahl zur Aktivierung bzw. Deaktivierung von Telemetrie wird erfasst, um sicherzustellen, dass wir die festgelegte Option einhalten.

Telemetrie-Sichtbarkeit

Wenn Telemetrie aktiviert ist, wird sie in der Ausgabe der Amazon-EC2-Konsole wie folgt angezeigt:

```
2021/07/15 21:44:12Z: Telemetry: <Data>
```

Deaktivieren der Telemetrie auf einer Instance

Um Telemetrie durch Festlegen einer Systemumgebungsvariablen zu deaktivieren, führen Sie den folgenden Befehl als Administrator aus:

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Um die Telemetrie während der Installation zu deaktivieren, führen Sie `install.ps1` wie folgt aus:

```
. .\install.ps1 -EnableTelemetry:$false
```

Weitere Themen für EC2Launch

- Installieren der neuesten Version von EC2Launch
- Den EC2Launch-v1-Agent in Ihrer Windows-Instance konfigurieren
- EC2Launch-Versionsverlauf

Installieren der neuesten Version von EC2Launch

Mit dem folgenden Verfahren können Sie die neueste Version von EC2Launch herunterladen und auf Ihren Instances installieren.

So laden Sie die neueste Version von EC2Launch herunter und installieren sie

1. Wenn Sie EC2Launch bereits auf einer Instance installiert und konfiguriert haben, erstellen Sie ein Backup der EC2Launch-Konfigurationsdatei. Beim Installationsprozess werden Änderungen an dieser Datei nicht übernommen. Standardmäßig befindet sich die Datei im Verzeichnis `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

2. Laden Sie die Datei EC2-Windows-Launch.zip in ein Verzeichnis auf der Instance herunter.
3. Laden Sie die Datei install.ps1 in dasselbe Verzeichnis herunter, in das Sie `EC2-Windows-Launch.zip` heruntergeladen haben.
4. Führen Sie `install.ps1`
5. Wenn Sie ein Backup der EC2Launch-Konfigurationsdatei erstellt haben, kopieren Sie sie in das Verzeichnis `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Neueste Version von EC2Launch mit PowerShell herunterladen und installieren

Wenn Sie EC2Launch bereits auf einer Instance installiert und konfiguriert haben, erstellen Sie ein Backup der EC2Launch-Konfigurationsdatei. Beim Installationsprozess werden Änderungen an dieser Datei nicht übernommen. Standardmäßig befindet sich die Datei im Verzeichnis `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Um die neueste Version von EC2Launch über PowerShell zu installieren, führen Sie die folgenden Befehle in einem PowerShell-Fenster als Administrator aus:

```
mkdir $env:USERPROFILE\Desktop\EC2Launch
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/EC2-Windows-Launch.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/install.ps1"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
& $env:USERPROFILE\Desktop\EC2Launch\install.ps1
```

> **Note**
>
> Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 oder früher verwenden, muss möglicherweise TLS 1.2 für Ihr PowerShell-Terminal aktiviert werden. Sie können TLS 1.2 für die aktuelle PowerShell-Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
> ```

Überprüfen Sie die Installation, indem Sie den Start-Agent überprüfen. Führen Sie die folgenden Befehle in einem PowerShell-Fenster als Administrator aus:

```
Import-Module C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Ec2Launch.psm1
Import-LocalizedData -BaseDirectory C:\ProgramData\Amazon\EC2-Windows\Launch\Module\ -
FileName 'Ec2Launch.psd1' -BindingVariable moduleManifest
$moduleManifest.Get_Item('ModuleVersion')
```

Den EC2Launch-v1-Agent in Ihrer Windows-Instance konfigurieren

Wenn Ihre Instance zum ersten Mal initialisiert wurde, können Sie EC2Launch so konfigurieren, dass das Programm erneut ausgeführt wird und beim Startup verschiedene Aufgaben ausführt.

Aufgaben

- Konfigurieren von Initialisierungsaufgaben
- Planen von EC2Launch für die Ausführung bei jedem Start
- Initialisieren von Laufwerken und Zuordnen von Laufwerksbuchstaben
- Senden von Windows-Ereignisprotokollen an die EC2-Konsole
- Senden einer „Windows ist einsatzbereit“-Meldung nach erfolgreichem Start

Konfigurieren von Initialisierungsaufgaben

Geben Sie die Einstellungen in der Datei `LaunchConfig.json` an, um die folgenden Initialisierungsaufgaben zu aktivieren oder zu deaktivieren:

- Setzen Sie den Computernamen auf die private IPv4-Adresse der Instance.
- Stellen Sie den Monitor so ein, dass er immer eingeschaltet bleibt.
- Erstellen eines neuen Bildschirmhintergrunds.
- Hinzufügen einer DNS-Suffixliste.

> **Note**
>
> Dadurch wird eine DNS-Suffixsuche für die folgende Domain hinzugefügt und andere Standardsuffixe konfiguriert. Weitere Informationen zur Einrichtung von DNS-Suffixen durch Start-Agenten finden Sie unter Das DNS-Suffix für EC2-Windows-Start-Agenten konfigurieren.

```
region.ec2-utilities.amazonaws.com
```

- Erweitern der Größe des Boot-Volumes.
- Legen Sie das Administrator-Passwort fest.

So konfigurieren Sie die Initialisierungseinstellungen

1. Öffnen Sie in der Instance, die Sie konfigurieren möchten, die folgende Datei in einem Texteditor: `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\LaunchConfig.json`.
2. Aktualisieren Sie nach Bedarf die folgenden Einstellungen, und speichern Sie Ihre Änderungen. Geben Sie in `adminPassword` nur dann ein Passwort an, wenn `adminPasswordtype` `Specify` ist.

```
{
 "setComputerName": false,
 "setMonitorAlwaysOn": true,
 "setWallpaper": true,
 "addDnsSuffixList": true,
 "extendBootVolumeSize": true,
 "handleUserData": true,
 "adminPasswordType": "Random | Specify | DoNothing",
 "adminPassword": "password that adheres to your security policy (optional)"
}
```

Die Passworttypen sind wie folgt definiert:

`Random`

EC2Launch generiert ein Passwort und verschlüsselt es mit dem Schlüssel des Benutzers: Die Einstellung wird vom System nach dem Start der Instance deaktiviert, so dass das Passwort weiterhin gilt, wenn die Instance neu gestartet bzw. angehalten und gestartet wird.

`Specify`

EC2Launch verwendet das Passwort, das Sie unter angebe `adminPassword`. Wenn das Passwort nicht den Systemanforderungen entspricht, erstellt EC2Launch stattdessen ein zufälliges Passwort. Das Passwort wird in `LaunchConfig.json` im Klartext gespeichert und

gelöscht, wenn Sysprep das Administratorpasswort einstellt. EC2Launch verschlüsselt das Passwort mit dem Schlüssel des Benutzers.

`DoNothing`

EC2Launch verwendet das Passwort, das Sie in der Datei `unattend.xml`-Datei angeben. Wenn Sie in der Datei `unattend.xml` kein Passwort angeben, ist das Administratorkonto deaktiviert.

3. Führen Sie in Windows PowerShell den folgenden Befehl aus, sodass das Skript vom System als Windows-Task eingeplant wird. Das Script wird beim nächsten Starten einmal ausgeführt und deaktiviert dann die erneute Ausführung dieser Aufgaben.

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
```

Planen von EC2Launch für die Ausführung bei jedem Start

Sie können EC2Launch so planen, dass es bei jedem Start läuft und nicht nur beim ersten Start.

So aktivieren Sie die Ausführung von EC2Launch bei jedem Start

1. Öffnen Sie Windows PowerShell und führen Sie den folgenden Befehl aus:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
SchedulePerBoot
```

2. Alternativ können Sie die ausführbare Datei mit dem folgenden Befehl ausführen:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Settings\Ec2LaunchSettings.exe
```

Wählen Sie dann au `Run EC2Launch on every boot`. Sie können für Ihre EC2-Instance `Shutdown without Sysprep` oder `Shutdown with Sysprep` festlegen.

> **Note**
>
> Wenn Sie EC2Launch bei jedem Start aktivieren, passiert folgendes, wenn EC2Launch das nächste Mal ausgeführt wird:
>
> - Wenn `AdminPasswordType` immer noch auf `Random` gesetzt ist, generiert EC2Launch beim nächsten Booten ein neues Passwort. Nach diesem Bootvorgang

wird `AdminPasswordType` automatisch auf `DoNothing` gesetzt, um zu verhindern, dass EC2Launch bei nachfolgenden Bootvorgängen neue Kennwörter generiert. Um zu verhindern, dass EC2Launch beim ersten Booten ein neues Passwort generiert, setzen Sie `AdminPasswordType` vor dem Neustart manuell auf `DoNothing`.

- `HandleUserData` wird auf `false` zurückgesetzt, es sei denn, für die Benutzerdaten ist `persist` für die Einstellung `true` angegeben. Weitere Informationen finden Sie unter the section called “Benutzerdatenskripts”.

Initialisieren von Laufwerken und Zuordnen von Laufwerksbuchstaben

Geben Sie die Einstellungen in der Datei `DriveLetterMappingConfig.json` an, um den Volumes auf Ihrer EC2-Instance Laufwerksbuchstaben zuzuordnen. Das Skript initialisiert Laufwerke, die noch nicht initialisiert und partitioniert sind. Weitere Informationen zum Abrufen von Volume-Details in Windows finden Sie unter Get-Volume in der Microsoft-Dokumentation.

So ordnen Sie Volumes Laufwerkbuchstaben zu

1. Öffnen Sie die Datei `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` in einem Text-Editor.
2. Geben Sie die folgenden Volume-Einstellungen an, und speichern Sie Ihre Änderungen:

```
{
 "driveLetterMapping": [
  {
   "volumeName": "sample volume",
   "driveLetter": "H"
  }
 ]
}
```

3. Öffnen Sie Windows PowerShell und verwenden Sie den folgenden Befehl, um das EC2Launch-Skript auszuführen, das die Datenträger initialisiert:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

Fügen Sie die Flag `-Schedule` wie folgt hinzu, um die Datenträger bei jedem Start der Instance zu initialisieren:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -Schedule
```

Senden von Windows-Ereignisprotokollen an die EC2-Konsole

Geben Sie die Einstellungen in der Datei `EventLogConfig.json` an, damit Windows-Ereignisprotokolle an EC2-Konsolenprotokolle gesendet werden.

So konfigurieren Sie die Einstellungen zum Senden von Windows-Ereignisprotokollen

1. Öffnen Sie in der Instance die Datei `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\EventLogConfig.json` in einem Text-Editor.
2. Konfigurieren Sie die folgenden Protokoll-Einstellungen an, und speichern Sie Ihre Änderungen:

   ```
   {
    "events": [
     {
      "logName": "System",
      "source": "An event source (optional)",
      "level": "Error | Warning | Information",
      "numEntries": 3
     }
    ]
   }
   ```
3. Führen Sie in Windows PowerShell den folgenden Befehl aus, so dass das Script vom System jedes Mal, wenn die Instance startet, als geplante Windows-Task ausgeführt wird.

   ```
   C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendEventLogs.ps1 -Schedule
   ```

   Es kann drei Minuten oder länger dauern, bis die Protokolle in den EC2-Konsolenprotokollen angezeigt werden.

Senden einer „Windows ist einsatzbereit“-Meldung nach erfolgreichem Start

Der EC2Config-Service sendete nach jedem Starten die Meldung „Windows ist einsatzbereit“ an die EC2-Konsole. EC2Launch sendet diese Meldung nur nach dem ersten Starten. Um die Abwärtskompatibilität mit dem EC2Config-Service zu gewährleisten, können Sie EC2Launch so konfigurieren, dass diese Meldung nach jedem Startvorgang gesendet wird. Öffnen Sie Windows

PowerShell in der Instance, und führen Sie den folgenden Befehl aus. Das System führt das Skript als geplante Windows-Task aus.

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendWindowsIsReady.ps1 -Schedule
```

EC2Launch-Versionsverlauf

> **Important**
>
> Ab dem 1. Januar 2025 werden nur die letzten beiden Versionen unterstützt. Wenn eine neue Version veröffentlicht wird, wird die älteste zuvor unterstützte Version automatisch als privat markiert und steht nicht mehr zum Download zur Verfügung.

Informationen zum Herunterladen der neuesten Version von EC2Launch finden Sie unter Installieren der neuesten Version von EC2Launch.

Sie können benachrichtigt werden, wenn neue Versionen des EC2Launch-Agenten veröffentlicht werden. Weitere Informationen finden Sie unter Benachrichtigungen von EC2-Windows-Start-Agenten abonnieren.

Die folgenden EC2Launch-Agent-Versionen werden unterstützt und stehen zum Download zur Verfügung.

Version	Details	Datum der Veröffentlichung
1.4.6	• Agentenprotokollmeldungen wurde aktualisiert.	13. Oktober 2025

Die folgenden früheren Versionen von EC2Launch stehen nicht mehr zum Download zur Verfügung.

Version	Details	Datum der Veröffentlichung
1.3.2005119	• Es wurde ein Problem behoben, bei dem `Invoke-Userdata` fehlschlägt, wenn es ohne Parameter aufgerufen wird.	11. Februar 2025
1.3.2005065	• Es wurde ein Problem behoben, bei dem RDP-Zertifikatsinformationen nicht ordnungsgemäß abgerufen oder validiert wurden. Es wurde eine Funktion hinzugefügt, mit der die Remotedesktopservices bei Bedarf automatisch gestartet werden können.	22. Oktober 2024
1.3.2005008	• `Set-Wallpaper` wurde aktualisiert, sodass auf einen einfarbigen Hintergrund zurückgegriffen wird, falls das Standard-Hintergrundbild nicht gefunden wird.	6. August 2024
1.3.2004959	• Die Installationslogik wurde aktualisiert, um eine nicht unterstützte Installation unter Windows Server 2025 oder höher zu verhindern.	2. Juli 2024
1.3.2004891	• Es wurde ein Problem behoben, bei dem `HandleUserData` nicht wie erwartet auf `false` eingestellt war. • Es wurde eine `Encrypted` -Passwortoption zu `LaunchConfig.json` hinzugefügt. • Das `Settings UI`-Verhalten wurde geändert, damit das vom Benutzer angegebene Passwort standardmäßig verschlüsselt wird. • Es wurde `SetAdminPasswordConfig.ps1` hinzugefügt, um die `Specify`-Kennwortoption in die `Encrypted`	31. Mai 2024

Version	Details	Datum der Veröffentlichung
	-Kennwortoption in der Agenten-Konfigurationsdatei zu konvertieren.	
1.3.2004617	• Ein Fehler beim Einstellen des Hintergrundbilds wurde behoben.	15. Januar 2024
1.3.2004592	• Die von install.ps1 festgelegten Zugriffsrechte für wurden aktualisiert `%ProgramData%\Amazon\EC2-Windows\Launch` . • Eingeschränkter EC2Launch-Ordner-/Dateizugriff auf Lese- und Ausführungsrechte nur für Standardbenutzerkonten. • Der Agent wartet nun nicht mehr auf die Initialisierung des Instance Metadata Service (IMDS), wenn IMDS für die Instance nicht aktiviert ist. • Beim Warten auf die Initialisierung des IMDS wurde ein Zeitlimit von fünf Minuten hinzugefügt. • Der Agent schreibt nun die Telemetriedaten vor der `Windows is Ready`-Meldung in das Konsolenprotokoll der Instance, anstatt danach. • Mehrere neue Instance-Typen unterstützen jetzt Bildschir mhintergründe. Weitere Informationen zu Zugriffsberechtigungen und Benutzerkontenberechtigungen für EC2Launch-Verzeichnisse finden Sie unter. the section called “EC2Launch-Verzeichnisstruktur”.	2. Januar 2024

Version	Details	Datum der Veröffentlichung
1.3.2004491	• Telemetrie wurde hinzugefügt, um die Verwendung der Option Administratorpasswort angeben zu überwachen.	9. November 2023
1.3.2004462	• Es wurde ein Leerungsvorgang nach jedem Schreibvorgang in die serielle Konsole hinzugefügt.	18. Oktober 2023
1.3.2004438	• Einschränkung der Übertragung von Domainnamen auf der Grundlage eines Registrierungseintrags: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • `UserdataExecution.log` -Berechtigungen nur auf `Administrators` beschränkt. • Dem Windows-Ereignisprotokoll wurden Fehlermeldungen hinzugefügt, wenn die Protokollinitialisierung fehlschlägt.	04. Oktober 2023
1.3.2004256	• `EnableSCSIPersistentReservations` -Wert dem Konsolenprotokoll hinzugefügt. • Wiederholungsfunktion für Get-ConsolePort hinzugefügt.	07. Juli 2023

Version	Details	Datum der Veröffentlichung
1.3.2004052	• Fehler behoben, wenn beim Start der Instance kein SSH-Schlüssel angegeben wurde. • Aktualisiert, um den Start des AmazonSSMAgent Windows-Dienstes bei Fehlern zu wiederholen. • Aktualisiert, damit SysprepInstance.ps1 fehlschlägt, wenn BeforeSysprep.cmd mit einem Exit-Code ungleich Null fehlschlägt.	08. März 2023
1.3.2003975	• Problem behoben, das sich auf Packer-AMI-Builds auswirkte, bei dem `SysprepInstance.ps1` einen `$LastErrorCode` von 1 zurückgegeben hat.	24. Dezember 2022
1.3.2003961	• Problem behoben, bei dem explizit angegebene Administratorkennwörter auf schnell gestarteten Instances mit einem zufälligen Passwort überschrieben wurden. • Problem behoben, bei dem der SSM-Agent auf kleineren Instance-Typen nicht gestartet werden konnte. • Problem behoben, bei dem das Instance-Konsolenprotokoll `RDPCERTIFICATE-THUMBPRINT: 0000000 0000000000000000` anstelle eines gültigen RDP-Zertifikats einen Fingerabdruckwert enthielt.	6. Dezember 2022
1.3.2003923	• Korrigiert die Logik für die Suche nach einem Netzwerkadapter, wenn PnPDeviceID leer ist.	9. November 2022

Version	Details	Datum der Veröffentlichung
1.3.2003919	• Get-ConsolePort wurde aktualisiert, um PCI-Segmentinformationen zu verwenden. • Problem behoben, bei dem nach einem Neustart ein falscher Netzwerkadapter ausgewählt werden konnte. • Die Timeout-Logik für den Start-SSM-Agent wurde korrigiert. • Die Abwärtskompatibilität für den Funktionsalias Send-AdminCredentials wurde behoben.	8. November 2022
1.3.2003857	• Priorisiert Adapter mit einem Standard-Gateway, wenn der primäre Netzwerkadapter ausgewählt ist. • Speicherinterne Passwortverschlüsselung erweitert.	3. Oktober 2022
1.3.2003824	• Fehler bei `setComputerName` behoben. • Logik hinzugefügt, um die Windows-Aktivierung bei Erkennung eines BYOL-Abrechnungscodes zu überspringen. • Speicherinterne Passwortverschlüsselung hinzugefügt. • Fehler bei der Volume-Initialisierung auf `m6id.4xlarge` behoben.	30. August 2022
1.3.2003691	• Die IMDS-Wartelogik wurde aktualisiert, um nur IMDSv2-Anforderungen zu stellen. • Fehler behoben, der die eGPU-Installation beeinträchtigte.	21. Juni 2022

Version	Details	Datum der Veröffentlichung
1.3.2003639	• Die Wartelogik des Netzwerkadapters wurde hinzugefügt, um die Verwendung vor der Initialisierung zu verhindern. • Kleinere Probleme wurden behoben.	10. Mai 2022
1.3.2003498	• Telemetrie hinzugefügt. • Verknüpfung zur Einstellungen-Benutzeroberfläche hinzugefügt. • PowerShell-Skripte formatiert. • Es wurde ein Problem mit dem Herunterfahren behoben, das auftrat, bevor BeforeSysprep.cmd abgeschlossen war.	31. Januar 2022
1.3.2003411	Logik zur Passworterstellung geändert, um Passwörter mit geringer Komplexität auszuschließen.	04. August 2021
1.3.2003364	Install-EgpuManager mit IMDSv2-Unterstützung aktualisiert.	7. Juni 2021
1.3.2003312	• Protokollzeilen vor und nach `setMonitorAlwaysOn` -Einstellung hinzugefügt. • AWS-Nitro-Enclaves-Paketversion zu Konsolenprotokoll hinzugefügt.	04. Mai 2021
1.3.2003284	Das Berechtigungsmodell wurde verbessert, indem der Speicherort von Benutzerdaten zu aktualisiert wurd `LocalAppData` .	23. März 2021

Version	Details	Datum der Veröffentlichung
1.3.2003236	• Aktualisierte Methode zum Festlegen des Benutzerpassworts in `Set-AdminAccount` und `Randomize-LocalAdminPassword` . • Behoben`InitializeDisks` , um zu überprüfen, ob die Festplatte nur auf Lesen eingestellt ist, bevor sie auf beschreibbar gesetzt wird.	11. Februar 2021
1.3.2003210	Lokalisierungsupdate für `install.ps1` .	7. Januar 2021
1.3.2003205	Sicherheitsupdate für `install.ps1` zum Aktualisieren von Berechtigungen für das `%ProgramData%AmazonEC2-WindowsLaunchModuleScripts` -Verzeichnis.	28. Dezember 2020
1.3.2003189	`w32tm resync` hinzugefügt, nachdem Routen hinzugefügt wurden.	4. Dezember 2020
1.3.2003155	Informationen zum Instance-Typ wurden aktualisiert.	25. August 2020
1.3.2003150	`OsCurrentBuild` und `OsReleaseId` zur Konsolenausgabe hinzugefügt.	22. April 2020
1.3.2003040	IMDS Version 1 Fallback-Logik wurde korrigiert.	7. April 2020
1.3.2002730	Unterstützung für IMDS V2 hinzugefügt.	3. März 2020
1.3.2002240	Kleinere Probleme wurden behoben.	31. Oktober 2019
1.3.2001660	Automatisches Anmeldeproblem für Benutzer ohne Passwort nach der ersten Ausführung von Sysprep behoben.	2. Juli 2019
1.3.2001360	Kleinere Probleme wurden behoben.	27. März 2019

Version	Details	Datum der Veröffentlichung
1.3.2001220	Alle PowerShell-Skripts signiert.	28. Februar 2019
1.3.2001200	Es wurde ein Problem mit InitializeDisks.ps1 behoben, bei dem das Ausführen des Skripts auf einem Knoten in einem Windows Server Failover Cluster zur Formatierung von Laufwerken auf entfernten Knoten führte, deren Laufwerksbuchstabe mit dem lokalen Laufwerksbuchstaben übereinstimmte.	27. Februar 2019
1.3.2001160	Das fehlende Hintergrundbild in Windows 2019 wurde hinzugefügt.	22. Februar 2019
1.3.2001040	• Es wurde ein Plug-In hinzugefügt, mit dem sich einstellen lässt, dass der Monitor nie ausgeschaltet wird, um ACPI-Probleme zu beheben. • SQL Server-Edition und -Version werden in die Konsole geschrieben.	21. Januar 2019
1.3.2000930	Ein Fehler beim Hinzufügen von Routen zu Metadaten auf ENIs mit IPv6-Unterstützung wurde behoben.	2. Januar 2019
1.3.2000760	• Standardkonfiguration für RSS- und Empfangswarteschlangen-Einstellungen für ENA-Geräte hinzugefügt. • Ruhezustand während Sysprep deaktiviert.	5. Dezember 2018

Version	Details	Datum der Veröffentlichung
1.3.2000630	• Route 169.254.169.253/32 für DNS-Server hinzugefügt. • Filter der Einstellung des Admin-Benutzers hinzugefügt. • Verbesserungen beim Instance-Ruhezustand. • Option hinzugefügt, um EC2Launch so zu planen, dass es bei jedem Start ausgeführt wird.	9. November 2018
1.3.2000430.0	• Route 169.254.169.123/32 zum AMZN-Zeitservice hinzugefügt. • Route 169.254.169.249/32 zum GRID-Lizenzdienst hinzugefügt. • Beim Versuch, Systems Manager zu starten, wurde ein Timeout von 25 Sekunden hinzugefügt.	19. September 2018
1.3.200039.0	• Fehlerhafte Laufwerksbeschriftung für EBS NVME-Volumes behoben. • Zusätzliche Protokollierung für NVME-Treiberversionen hinzugefügt.	15. August 2018
1.3.2000080	Kleinere Probleme wurden behoben.	
1.3.610	Behebung eines Fehlers mit der Umleitung von Ausgabe und Fehlern von Benutzerdaten zu Dateien.	

Version	Details	Datum der Veröffentlichung
1.3.590	• Hinzufügung fehlender Instance-Types im Hintergrundbild. • Behebung eines Fehlers mit Laufwerkbuchstabenzuordnung und Festplatteninstallation.	
1.3.580	• Behebung von `Get-Metadata` zur Verwendung der Standard-Systemproxyeinstellungen für Webanfragen. • Hinzufügung eines besonderen Falls für NVMe bei der Festplatteninitialisierung. • Kleinere Probleme wurden behoben.	
1.3.550	Hinzufügung einer `-NoShutdown` -Option zur Aktivierung von Sysprep ohne Herunterfahren.	
1.3.540	Kleinere Probleme wurden behoben.	
1.3.530	Kleinere Probleme wurden behoben.	
1.3.521	Kleinere Probleme wurden behoben.	
1.3.0	• Ein Problem mit einer hexadezimalen Länge für eine Computer-Namen-Änderung wurde behoben. • Ein Problem mit einer möglichen Neustartschleife für eine Computer-Namen-Änderung wurde behoben. • Ein Problem mit der Einrichtung eines Bildschirmhintergrunds wurde behoben.	

Version	Details	Datum der Veröffentlichung
1.2.0	• Aktualisierung zum Anzeigen von Informationen über das installierte Betriebssystem (OS) im EC2-Systemprotokoll. • Aktualisierung zum Anzeigen der Version von EC2Launch und SSM Agent im EC2-Systemprotokoll. • Kleinere Probleme wurden behoben.	
1.1.2	• Aktualisierung zum Anzeigen von ENA-Treiberinformationen im EC2-Systemprotokoll. • Aktualisierung zum Ausschließen von Hyper-V von primärer NIC-Filterlogik. • AWS KMS-Server und -Port wurden im Registrierungsschlüssel zur KMS-Aktivierung hinzugefügt. • Die Einrichtung des Bildschirmhintergrunds wurde für mehrere Benutzer verbessert. • Aktualisierung zum Löschen von Routen aus dem persistenten Speicher. • Aktualisierung zum Entfernen des z von Availability Zone in der DNS-Suffixliste. • Aktualisierung zur Behebung eines Problems mit dem Tag (Markierung) <runAsLocalSystem> in den Benutzerdaten.	
1.1.1	Erstversion.	

Den EC2Config-Service verwenden, um Aufgaben während des Starts der EC2-Legacy-Windows-Betriebssysteminstance auszuführen

> **Note**
>
> EC2Config-Service hat das Ende der Unterstützung erreicht. Die Betriebssystemversionen, auf denen es ausgeführt wird, werden von Microsoft nicht mehr unterstützt. Wir empfehlen dringend, ein Aktualisierung auf den neuesten Start-Agenten durchzuführen.
> Der neueste Start-Agent für Windows Server 2022 und spätere Betriebssystem-Versionen ist EC2Launch v2, der sowohl EC2Config als auch EC2Launch ersetzt und auf AWS-Windows-Server-2022- und 2025-AMIs vorinstalliert ist. Sie können den Agent auch manuell auf Windows Server 2016 und 2019 installieren und konfigurieren. Weitere Informationen finden Sie unter EC2Launch v2 installieren.

Windows-AMIs vor Windows Server 2016 schließen den optionalen EC2Config-Service (`EC2Config.exe`) ein. EC2Config startet, wenn die Instance hochgefahren wird. Darüber hinaus führt der Service beim ersten Startup sowie bei jedem Stoppen und Starten der Instance Aufgaben aus. Zudem kann EC2Config nach Bedarf Aufgaben ausführen. Einige dieser Aufgaben sind automatisch aktiviert, während andere manuell aktiviert werden müssen. Obwohl dieser Service optional ist, liefert er Zugriff auf erweiterte Features, die anderweitig nicht verfügbar sind. Dieser Service wird im LocalSystem-Konto ausgeführt.

Der EC2Config-Service führt Sysprep aus, ein Microsoft-Tool, mit dem Sie ein benutzerdefiniertes Windows-AMI erstellen können, das wiederverwendet werden kann. Wenn EC2Config Sysprep aufruft, verwendet es die Dateien in `%ProgramFiles%\Amazon\EC2ConfigService\Settings`, um zu bestimmen, welche Operationen ausgeführt werden sollen. Sie können diese Dateien indirekt über das Dialogfeld EC2-Serviceeigenschaften oder direkt in einem XML-Editor oder einem Texteditor bearbeiten. Es gibt jedoch einige erweiterte Einstellungen, die nicht im Dialogfeld EC2-Serviceeigenschaften verfügbar sind. Diese Einträge müssen Sie direkt bearbeiten.

Wenn Sie ein AMI aus einer Instance erstellen, nachdem Sie deren Einstellungen aktualisiert haben, werden die neuen Einstellungen auf alle Instances angewandt, die von diesem AMI gestartet werden. Weitere Informationen über die Erstellung eines AMI finden Sie unter Ein Amazon-EBS-gestütztes AMI erstellen.

EC2Config verwendet Einstellungsdateien, um den eigenen Betrieb zu kontrollieren. Sie können diese Einstellungsdateien aktualisieren, indem Sie entweder ein grafisches Tool verwenden oder die

XML-Dateien direkt bearbeiten. Die Binärdateien des Service sowie zusätzliche Dateien befinden sich im Verzeichnis `%ProgramFiles%\Amazon\EC2ConfigService`.

Inhalt

- EC2Config und AWS Systems Manager
- EC2Config-Aufgaben
- EC2Config-Einstellungsdateien
- Installieren der neuesten Version von EC2Config
- .NET-Proxy-Einstellungen für den EC2Config-Service konfigurieren
- Legen Sie die Eigenschaften des EC2Config-Services im Systemdialog auf Ihrer EC2-Windows-Instance fest
- Fehlerbehebung beim EC2Config-Start-Agent
- EC2Config-Versionshistorie

EC2Config und AWS Systems Manager

Der EC2Config-Service verarbeitet Systems Manager-Anfragen auf Instances, die aus AMIs für Windows Server-Versionen vor Windows Server 2016 erstellt und vor November 2016 veröffentlicht wurden.

Instances, die aus AMIs für Windows Server-Versionen vor Windows Server 2016 erstellt und nach November 2016 veröffentlicht wurden, enthalten den EC2Config-Service und SSM Agent. EC2Config führt alle zuvor beschriebenen Aufgaben aus und SSM Agent verarbeitet Anfragen für Systems Manager-Funktionen wie Run Command und State Manager.

Sie können über den Run Command Ihre vorhandenen Instances upgraden, damit diese die aktuelle Version des EC2Config-Service und von SSM Agent verwenden. Weitere Informationen finden Sie unter Aktualisieren des SSM Agent mit Run Command im Benutzerhandbuch für AWS Systems Manager.

EC2Config-Aufgaben

EC2Config führt die Startaufgaben beim ersten Startup der Instance aus und deaktiviert sie anschließend. Um diese Aufgaben erneut ausführen zu können, müssen Sie sie vor dem Herunterfahren der Instance ausdrücklich aktivieren oder Sysprep manuell ausführen. Es handelt sich dabei um die folgenden Aufgaben:

- Einrichtung eines zufälligen, verschlüsselten Passworts für das Administratorkonto.
- Generation und Installation des Hostzertifikats zur Verwendung für die Remote Desktop Connection.
- Erweiterung der Betriebssystempartition, um den gesamten nicht partitionierten Speicherplatz mit einzuschließen.
- Ausführung der angegebenen Benutzerdaten (sowie von Cloud-Init, sofern installiert). Weitere Informationen zur Angabe von Benutzerdaten finden Sie unter Befehle ausführen, wenn Sie eine EC2 Instance mit Benutzerdateneingabe starten.

EC2Config führt beim ersten Start einer Instance die folgenden Aufgaben aus:

- Änderung des Hostnamens, sodass er mit der privaten IP-Adresse in Hexa-Schreibweise übereinstimmt. (Diese Aufgabe ist standardmäßig deaktiviert und muss zunächst aktiviert werden, um beim Start der Instance ausgeführt werden zu können.)
- Konfiguration des Schlüsselverwaltungsservers (Key Management Server, AWS KMS), Überprüfung des Aktivierungsstatus von Windows und gegebenenfalls die Aktivierung von Windows.
- Mounten aller Amazon EBS-Volumes und Instance-Speicher-Volumes sowie Zuweisung der Volumenamen zu den Laufwerkbuchstaben.
- Schreiben der Ereignisprotokolleinträge in die Konsole, um die Fehlerbehebung zu unterstützen. (Diese Aufgabe ist standardmäßig deaktiviert und muss zunächst aktiviert werden, um beim Start der Instance ausgeführt werden zu können.)
- Mitteilung an die Konsole schreiben, dass Windows einsatzbereit ist.
- Hinzufügung einer benutzerdefinierten Route zum primären Netzwerkadapter, um die folgenden IP-Adressen zu aktivieren, wenn eine einzelne NIC oder mehrere NICs zugeordnet sind: `169.254.169.250`, `169.254.169.251` und `169.254.169.254`. Diese Adressen werden von der Windows-Aktivierung und beim Zugriff auf Instance-Metadaten verwendet.

> **Note**
>
> Wenn das Windows-Betriebssystem für die Verwendung von IPv4 konfiguriert ist, können diese Link-local-IPv4-Adressen verwendet werden. Wenn das Windows-Betriebssystem den IPv4-Netzwerkprotokollstack deaktiviert hat und stattdessen IPv6 verwendet, fügen Sie `[fd00:ec2::250]` anstelle von `169.254.169.250` und `169.254.169.251` hinzu. Dann fügen Sie `[fd00:ec2::254]` anstelle von `169.254.169.254` hinzu.

EC2Config führt bei jedem Anmelden eines Benutzers die folgenden Aufgaben aus:

- Anzeigen der Informationen zum Bildschirmhintergrund auf dem Desktop-Hintergrund.

Während die Instance ausgeführt wird, können Sie beantragen, dass EC2Config die folgenden Aufgaben nach Bedarf ausführt:

- Ausführung von Sysprep und Herunterfahren der Instance, damit Sie daraus ein AMI erstellen können. Weitere Informationen finden Sie unter Ein Amazon-EC2-AMI mit Windows Sysprep erstellen.

EC2Config-Einstellungsdateien

Die Einstellungsdateien steuern den Betrieb des EC2Config-Services. Diese Dateien befinden sich im Verzeichnis `C:\Program Files\Amazon\Ec2ConfigService\Settings`:

- `ActivationSettings.xml`—Steuert die Produktaktivierung mithilfe eines Schlüsselverwaltungsservers (AWS KMS).
- `AWS.EC2.Windows.CloudWatch.json` — Steuert, welche Leistungsindikatoren an CloudWatch und welche Protokolle an CloudWatch Logs gesendet werden.
- `BundleConfig.xml` — Steuert, wie EC2Config eine Instance, die von einem Instance-Speicher gestützt wird, auf die AMI-Erstellung vorbereitet.
- `Config.xml` — Steuert die primären Einstellungen.
- `DriveLetterConfig.xml` — Steuert die Zuweisung der Laufwerkbuchstaben.
- `EventLogConfig.xml` — Steuert die Ereignisprotokollinformationen, die während des Starts der Instance auf der Konsole angezeigt werden.
- `WallpaperSettings.xml` — Steuert die Informationen, die auf dem Desktop-Hintergrund angezeigt werden.

ActivationSettings.xml

Diese Datei enthält Einstellungen, die die Produktaktivierung steuern. Beim Start von Windows, überprüft der EC2Config-Service, ob Windows bereits aktiviert ist. Wenn Windows nicht bereits aktiviert ist, versucht der Service, Windows durch die Suche nach dem angegebenen AWS KMS zu aktivieren.

- `SetAutodiscover`: Gibt an, ob ein AWS KMS automatisch erkannt werden soll.
- `TargetKMSServer`—Speichert die private IP-Adresse eines AWS KMS. Das AWS KMS muss sich in derselben Region wie Ihre Instance befinden.
- `DiscoverFromZone`: Ermittelt den AWS KMS-Server in der angegebenen DNS-Zone.
- `ReadFromUserData`: Ruft den AWS KMS-Server aus UserData ab.
- `LegacySearchZones`: Ermittelt den AWS KMS-Server in der angegebenen DNS-Zone.
- `DoActivate` — Versucht die Aktivierung anhand der angegebenen Einstellungen im Abschnitt einzuleiten. Dabei kann es sich um den Wert `true` oder `false` handeln.
- `LogResultToConsole` — Zeigt die Ergebnisse auf der Konsole an.

BundleConfig.xml

Diese Datei enthält Einstellungen, die die Vorbereitung einer Instance auf die Erstellung eines AMI durch EC2Config steuern.

- `AutoSysprep` — Gibt an, ob Sysprep automatisch verwendet werden soll. Ändern Sie den Wert auf `Yes`, um Sysprep zu verwenden.
- `SetRDPCertificate` — Legt ein selbstsigniertes Zertifikat für den Remote Desktop-Server fest. Auf diese Weise kann die Übermittlung an die Instances mithilfe von RDP sicher erfolgen. Ändern Sie den Wert zu `Yes`, wenn die neuen Instances über das Zertifikat verfügen sollen.

  Diese Einstellung wird nicht für Instances mit Betriebssystemversionen vor Windows Server 2016 verwendet, da diese ihre eigenen Zertifikate generieren können.
- `SetPasswordAfterSysprep` — Legt ein zufälliges Passwort für eine neu gestartete Instance fest, verschlüsselt sie mit dem Benutzer-Startschlüssel und gibt das verschlüsselte Passwort an die Konsole aus. Ändern Sie den Wert dieser Einstellung zu `No`, wenn für die neuen Instances nicht ein zufällig verschlüsseltes Passwort festgelegt werden soll.

Config.xml

Plug-ins

- `Ec2SetPassword` — Generiert bei jedem Start einer Instance ein zufälliges, verschlüsseltes Passwort. Dieses Feature wird standardmäßig nach dem ersten Start deaktiviert, sodass das vom Benutzer festgelegte Passwort auch durch Neustarts dieser Instance nicht geändert wird. Ändern

Sie diese Einstellung auf `Enabled`, um weiterhin bei jedem Start einer Instance Passwörter zu generieren.

Diese Einstellung ist wichtig, wenn Sie planen, aus Ihrer Instance ein AMI zu erstellen.

- `Ec2SetComputerName` — Gibt den Hostnamen einer Instance basierend auf der IP-Adresse der Instance als eindeutigen Namen an und startet die Instance neu. Deaktivieren Sie diese Einstellung, um Ihren eigenen Hostnamen anzugeben oder den bestehenden Namen vor einer Änderung zu schützen.
- `Ec2InitializeDrives` — Initialisiert und formatiert alle Volumes während des Startups. Dieses Feature ist standardmäßig aktiviert.
- `Ec2EventLog` — Zeigt Protokolleinträge in der Konsole an. Standardmäßig werden die drei neuesten Fehlereinträge vom Systemereignisprotokoll angezeigt. Um festzulegen, welche Ereignisprotokolleinträge angezeigt werden, bearbeiten Sie die Datei `EventLogConfig.xml` im Verzeichnis `EC2ConfigService\Settings`. Weitere Informationen über die Einstellungen in dieser Datei finden Sie unter Eventlog Key.
- `Ec2ConfigureRDP` — Richtet eine selbstsignierte Zertifikat auf der Instance ein, sodass Benutzer mithilfe von Remote Desktop sicher auf die Instance zugreifen können. Diese Einstellung wird nicht für Instances mit Betriebssystemversionen vor Windows Server 2016 verwendet, da diese ihre eigenen Zertifikate generieren können.
- `Ec2OutputRDPCert` — Zeigt die Informationen zum Remote Desktop-Zertifikat auf der Konsole an, damit der Benutzer die Informationen mit dem Thumbprint vergleichen kann.
- `Ec2SetDriveLetter` — Legt die Laufwerkbuchstaben der bereitgestellten Volumes aufgrund der benutzerdefinierten Einstellungen fest. Wenn ein Amazon EBS-Volume einer Instance angefügt ist, kann es unter Verwendung des Laufwerkbuchstaben auf der Instance angezeigt werden. Um die Zuweisung der Laufwerkbuchstaben festzulegen, bearbeiten Sie die Datei `DriveLetterConfig.xml` im Verzeichnis `EC2ConfigService\Settings`.
- `Ec2WindowsActivate` — Das Plug-in führt die Windows-Aktivierung aus. Es überprüft, ob Windows aktiviert ist. Ist dies nicht der Fall, aktualisiert das Plug-in die Einstellungen des AWS KMS-Clients und aktiviert anschließend Windows.

  Um die AWS KMS-Einstellungen zu ändern, bearbeiten Sie die Datei `ActivationSettings.xml` im `EC2ConfigService\Settings`-Verzeichnis.
- `Ec2DynamicBootVolumeSize` — Erweitert Festplatte 0/Volume 0, sodass der gesamte nicht partitionierte Speicherplatz eingeschlossen ist.

- `Ec2HandleUserData` — Erstellt vom Benutzer angefertigte Skripte und führt diese beim ersten Starten einer Instance aus, nachdem Sysprep ausgeführt wurde. Befehle, die in Skript-Tags verpackt sind, werden in einer Batch-Datei gespeichert, und Befehle, die in PowerShell-Tags verpackt sind, werden in einer PS1-Datei gespeichert (entspricht dem Kontrollkästchen Benutzerdaten im Systemdialogfeld Ec2-Serviceeigenschaften).
- `Ec2ElasticGpuSetup` — Installiert das Elastic GPU-Softwarepaket, wenn die Instance mit einer elastischen GPU verknüpft ist.
- `Ec2FeatureLogging` — Sendet die Installation der Windows-Features und den zugehörigen Service-Status an die Konsole. Wird nur für das Microsoft Hyper-V-Feature und den zugehörigen VMMS-Service unterstützt.

Globale Einstellungen

- `ManageShutdown` – Stellt sicher, dass Instances, die von Amazon-S3-gestützten AMIs gestartet werden, während der Ausführung von Sysprep nicht beendet werden.
- `SetDnsSuffixList` — Legt das DNS-Suffix des Netzwerkadapters für Amazon EC2 fest. Hierdurch ist die DNS-Auflösung der Server, die in Amazon EC2 ausgeführt werden, ohne Bereitstellung des vollständig qualifizierten Domain-Namens möglich.

> **Note**
>
> Dadurch wird eine DNS-Suffixsuche für die folgende Domain hinzugefügt und andere Standardsuffixe konfiguriert. Weitere Informationen zur Einrichtung von DNS-Suffixen durch Start-Agenten finden Sie unter Das DNS-Suffix für EC2-Windows-Start-Agenten konfigurieren.
>
> ```
> region.ec2-utilities.amazonaws.com
> ```

- `WaitForMetaDataAvailable` — Stellt sicher, dass der EC2Config-Service darauf wartet, dass die Metadaten zugänglich sind und das Netzwerk verfügbar ist, bevor der Start fortgesetzt wird. Durch diese Überprüfung wird sichergestellt, dass EC2Config Informationen aus den Metadaten abrufen kann, die für die Aktivierung und andere Plug-ins hilfreich sind.
- `ShouldAddRoutes` — Hinzufügung einer benutzerdefinierten Route zum primären Netzwerkadapter, um die folgenden IP-Adressen zu aktivieren, wenn mehrere NICs zugeordnet sind: 169.254.169.250, 169.254.169.251 und 169.254.169.254. Diese Adressen werden von der Windows-Aktivierung und beim Zugriff auf Instance-Metadaten verwendet.

- `RemoveCredentialsfromSyspreponStartup` — Entfernt das Administratorpasswort aus `Sysprep.xml`, sobald der Server das nächste Mal gestartet wird. Bearbeiten Sie diese Einstellung, um sicherzustellen, dass das Passwort erhalten bleibt.

DriveLetterConfig.xml

Diese Datei enthält Einstellungen, die die Zuweisung der Laufwerkbuchstaben steuern. Standardmäßig kann ein Volume jedem beliebigen Laufwerkbuchstaben zugeordnet werden. Sie können ein Volume einem bestimmten Laufwerkbuchstaben folgendermaßen bereitstellen.

```
<?xml version="1.0" standalone="yes"?>
<DriveLetterMapping>
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
  . . .
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
</DriveLetterMapping>
```

- `VolumeName` — Die Bezeichnung des Volumes. Beispiel, *`My Volume`*. Um die Zuweisung für ein Instance-Speicher-Volume festzulegen, verwenden Sie die Bezeichnung `Temporary Storage X`, wobei `X` eine Zahl zwischen 0 bis 25 ist.
- `DriveLetter` — Der Laufwerkbuchstabe. Beispiel, *`M:`*. Wird der Laufwerkbuchstabe bereits verwendet, schlägt die Zuweisung fehl.

EventLogConfig.xml

Diese Datei enthält Einstellungen, die die Ereignisprotokollinformationen steuern, die beim Start der Instance auf der Konsole angezeigt werden. Standardmäßig werden die drei neuesten Fehlereinträge aus dem Systemereignisprotokoll angezeigt.

- `Category` — Der zu überwachende Ereignisprotokollschlüssel.
- `ErrorType`—Der Ereignistyp (beispielsweise, `Error`, `Warning`, `Information`.)
- `NumEntries` — Die Anzahl der gespeicherten Ereignisse in dieser Kategorie.

- `LastMessageTime` — Um zu verhindern, dass die gleiche Nachricht wiederholt mithilfe von Push übertragen wird, aktualisiert der Service diesen Wert jedes Mal, wenn eine Nachricht übertragen wird.
- `AppName` — Die Ereignisquelle oder die Anwendung, die das Ereignis protokolliert hat.

WallpaperSettings.xml

Diese Datei enthält Einstellungen, die die auf dem Desktop-Hintergrund angezeigten Informationen steuern. Standardmäßig werden die folgenden Informationen angezeigt.

- `Hostname` — Zeigt den Computer-Namen an.
- `Instance ID` — Zeigt die Instance-ID an.
- `Public IP Address` — Zeigt die öffentliche IP-Adresse der Instance an.
- `Private IP Address` — Zeigt die private IP-Adresse der Instance an.
- `Availability Zone` — Zeigt die Availability Zone an, in der die Instance ausgeführt wird.
- `Instance Size` — Zeigt den Instance-Typ an.
- `Architecture` — Zeigt die Einstellungen der Umgebungsvariablen `PROCESSOR_ARCHITECTURE` an.

Sie können alle standardmäßig angezeigten Informationen entfernen, indem Sie deren Eintrag löschen. Um zusätzliche Instance-Metadaten anzuzeigen, gehen Sie folgendermaßen vor.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>metadata</source>
  <identifier>meta-data/path</identifier>
</WallpaperInformation>
```

Um zusätzliche Systemumgebungsvariablen anzuzeigen, gehen Sie folgendermaßen vor.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>EnvironmentVariable</source>
  <identifier>variable-name</identifier>
</WallpaperInformation>
```

InitializeDrivesSettings.xml

Diese Datei enthält Einstellungen, die die Initialisierung von Laufwerken durch EC2Config steuern.

EC2Config initialisiert standardmäßig Laufwerke, die nicht mit dem Betriebssystem online geschaltet wurden. Sie können das Plug-in folgendermaßen anpassen.

```
<InitializeDrivesSettings>
    <SettingsGroup>setting</SettingsGroup>
</InitializeDrivesSettings>
```

Verwenden Sie eine Einstellungsgruppe, um festzulegen, wie die Laufwerke initialisiert werden sollen:

FormatWithTRIM

Aktiviert den TRIM-Befehl für die Formatierung der Laufwerke. Nachdem das Laufwerk formatiert und initialisiert wurde, stellt das System die TRIM-Konfiguration wieder her.

Ab EC2Config Version 3.18 ist der TRIM-Befehl standardmäßig während der Formatierungsoperation der Festplatte deaktiviert. Dadurch wird die Formatierungszeit verbessert. Verwenden Sie diese Einstellung, um TRIM während der Festplattenformatierung für EC2Config Version 3.18 und höher zu aktivieren.

FormatWithoutTRIM

Deaktiviert den TRIM-Befehl während der Formatierung der Laufwerke und verbessert die Formatierungszeiten in Windows. Nachdem das Laufwerk formatiert und initialisiert wurde, stellt das System die TRIM-Konfiguration wieder her.

DisableInitializeDrives

Deaktiviert die Formatierung neuer Laufwerke. Verwenden Sie diese Einstellung, um Laufwerke manuell zu initialisieren.

Installieren der neuesten Version von EC2Config

> **Note**
>
> Der neueste Start-Agent für Windows Server 2022 und spätere Betriebssystem-Versionen ist EC2Launch v2, der sowohl EC2Config als auch EC2Launch ersetzt. EC2Launch v2 ist auf AMIs von AWS Windows Server 2022 und 2025 vorinstalliert. Sie können den Agent auch manuell auf Windows Server 2016 und 2019 installieren und konfigurieren. Weitere Informationen finden Sie unter EC2Launch v2 installieren.

Weitere Informationen darüber, wie Sie Benachrichtigungen über EC2Config-Updates erhalten, finden Sie unter Benachrichtigungen von EC2-Windows-Start-Agenten abonnieren. Informationen über Änderungen in den einzelnen Versionen finden Sie unter EC2Config-Versionshistorie.

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie über das .NET-Framework 3.5 SP1 oder höher verfügen.
- Standardmäßig ersetzt Setup Ihre Einstellungsdateien während der Installation mit Standardeinstellungsdateien und startet den EC2Config-Service nach Abschluss der Installation neu. Wenn Sie die EC2Config-Serviceeinstellungen geändert haben, kopieren Sie die Datei `config.xml` aus dem Verzeichnis `%Program Files%\Amazon\Ec2ConfigService\Settings`. Nachdem Sie den EC2Config-Service aktualisiert haben, können Sie die Datei wiederherstellen, um Ihre Konfigurationsänderungen zu erhalten.

Überprüfen der EC2Config-Version

Gehen Sie wie folgt vor, um zu überprüfen, welche Version von EC2Config in Ihren Instances installiert ist.

So überprüfen Sie die installierte EC2Config-Version

1. Starten Sie eine Instance von Ihrem AMI und stellen Sie eine Verbindung damit her.
2. Wählen Sie in der Systemsteuerung Programs and Features aus.
3. Suchen Sie in der Liste mit den installierten Programmen nach `Ec2ConfigService`. Die Versionsnummer wird in der Spalte Version angegeben.

Aktualisieren von EC2Config

Gehen Sie wie folgt vor, um die neueste Version von EC2Config herunterzuladen und in Ihren Instances zu installieren.

So laden Sie die neueste Version von EC2Config herunter und installieren sie

1. Laden Sie das EC2Config-Installationsprogramm herunter und entzippen Sie es.
2. Führen Sie `EC2Install.exe`. Eine vollständige Liste der verfügbaren Optionen erhalten Sie, wenn Sie `EC2Install` mit der Option `/?` ausführen. Standardmäßig werden Eingabeaufforderungen angezeigt. Um den Befehl ohne Eingabeaufforderungen auszuführen, verwenden Sie die Option `/quiet`.

> **Important**
>
> Um die benutzerdefinierten Einstellungen aus der von Ihnen gespeicherten Datei `config.xml` beizubehalten, führen Sie `EC2Install` mit der Option `/norestart` aus, stellen Sie Ihre Einstellungen wieder her und starten Sie den EC2Config-Service manuell neu.

3. Wenn Sie EC2Config Version 4.0 oder höher ausführen, müssen Sie SSM Agent vom Microsoft Service Snap-in aus auf der Instance neu starten.

> **Note**
>
> Die aktualisierten Informationen zur EC2Config-Version werden im Instance-Systemprotokoll oder in der Trusted Advisor-Überprüfung nicht angezeigt, bis Sie Ihre Instance neu starten bzw. beenden und starten.

Neueste Version von EC2Config mit PowerShell herunterladen und installieren

Um die neueste Version von EC2Config über PowerShell zu installieren, führen Sie die folgenden Befehle in einem PowerShell-Fenster aus:

```
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Config/EC2Install.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\" + $(Split-Path -Path $Url -Leaf)
$ExtractPath = "$env:USERPROFILE\Desktop\"
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$ExtractShell = New-Object -ComObject Shell.Application
$ExtractFiles = $ExtractShell.Namespace($DownloadZipFile).Items()
$ExtractShell.NameSpace($ExtractPath).CopyHere($ExtractFiles)
Start-Process $ExtractPath
Start-Process `
    -FilePath $env:USERPROFILE\Desktop\EC2Install.exe `
    -ArgumentList "/S"
```

> **Note**
>
> Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 oder früher verwenden, muss TLS 1.2 möglicherweise für Ihr PowerShell-

Terminal aktiviert werden. Sie können TLS 1.2 für die aktuelle PowerShell-Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

Prüfen Sie zur Verifizierung der Installation, ob unter `C:\Program Files\Amazon\` das Verzeichnis `Ec2ConfigService` angelegt wurde.

.NET-Proxy-Einstellungen für den EC2Config-Service konfigurieren

Mithilfe der folgenden Methoden können Sie den EC2Config-Service so konfigurieren, dass er durch einen Proxy kommuniziert: das AWS SDK for .NET, das Element `system.net` oder die Microsoft Gruppenrichtlinie und Internet Explorer. Die Verwendung des AWS-SDK für .NET ist die bevorzugte Methode, da Sie hierbei Anmeldeinformationen angeben können.

Methoden

- Konfiguration der Proxy-Einstellungen mithilfe von AWS SDK für .NET (bevorzugt)
- Konfigurieren der Proxy-Einstellungen mithilfe des system.net-Elements
- Konfigurieren der Proxy-Einstellungen mithilfe der Microsoft-Gruppenrichtlinien und Microsoft Internet Explorer

Konfiguration der Proxy-Einstellungen mithilfe von AWS SDK für .NET (bevorzugt)

Sie können die Proxy-Einstellungen für den EC2Config-Service anhand des Elements `proxy` in der Datei `Ec2Config.exe.config` konfigurieren. Weitere Informationen finden Sie unter Konfigurationsdateireferenz für AWS SDK for .NET.

So legen Sie das Proxy-Element in Ec2Config.exe.config fest

1. Bearbeiten Sie die Datei `Ec2Config.exe.config` auf allen Instances, auf denen der EC2Config-Service über einen Proxy kommunizieren soll. Standardmäßig befindet sich die Datei im folgenden Verzeichnis: `%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Fügen Sie das folgende Element `aws` den `configSections` hinzu. Fügen Sie dies keiner vorhandenen hinz `sectionGroups`.

   Für EC2Config Versionen 3.17 und niedriger

```
<configSections>
   <section name="aws" type="Amazon.AWSSection, AWSSDK"/>
</configSections>
```

Für EC2Config Versionen 3.18 und höher

```
<configSections>
     <section name="aws" type="Amazon.AWSSection, AWSSDK.Core"/>
</configSections>
```

3. Fügen Sie das folgende `aws`-Element der Datei `Ec2Config.exe.config` hinzu.

```
<aws>
   <proxy
     host="string value"
     port="string value"
     username="string value"
     password="string value" />
</aws>
```

4. Speichern Sie Ihre Änderungen.

Konfigurieren der Proxy-Einstellungen mithilfe des system.net-Elements

Sie können die Proxy-Einstellungen im `system.net`-Element in der Datei `Ec2Config.exe.config` festlegen. Weitere Informationen finden Sie unter defaultProxy-Element (Netzwerkeinstellungen).

So legen Sie das system.net-Element in Ec2Config.exe.config fest

1. Bearbeiten Sie die Datei `Ec2Config.exe.config` auf allen Instances, auf denen der EC2Config-Service über einen Proxy kommunizieren soll. Standardmäßig befindet sich die Datei im folgenden Verzeichnis: `%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Fügen Sie einen `defaultProxy`-Eintrag `system.net` hinzu. Weitere Informationen finden Sie unter defaultProxy-Element (Netzwerkeinstellungen).

   In der folgenden Konfiguration verwendet der gesamte Datenverkehr beispielsweise den derzeit für Internet Explorer konfigurierten Proxy. Dabei stellen die Metadaten und der lizensierte Datenverkehr eine Ausnahme dar, da sie den Proxy umgehen.

```
<defaultProxy>
    <proxy usesystemdefault="true" />
    <bypasslist>
        <add address="169.254.169.250" />
        <add address="169.254.169.251" />
        <add address="169.254.169.254" />
        <add address="[fd00:ec2::250]" />
        <add address="[fd00:ec2::254]" />
    </bypasslist>
</defaultProxy>
```

3. Speichern Sie Ihre Änderungen.

Konfigurieren der Proxy-Einstellungen mithilfe der Microsoft-Gruppenrichtlinien und Microsoft Internet Explorer

Der EC2Config-Service wird unter dem lokalen Systembenutzerkonto ausgeführt. Nachdem Sie die Gruppenrichtlinieneinstellungen auf der Instance geändert haben, können Sie für dieses Konto instanceweite Proxy-Einstellungen festlegen.

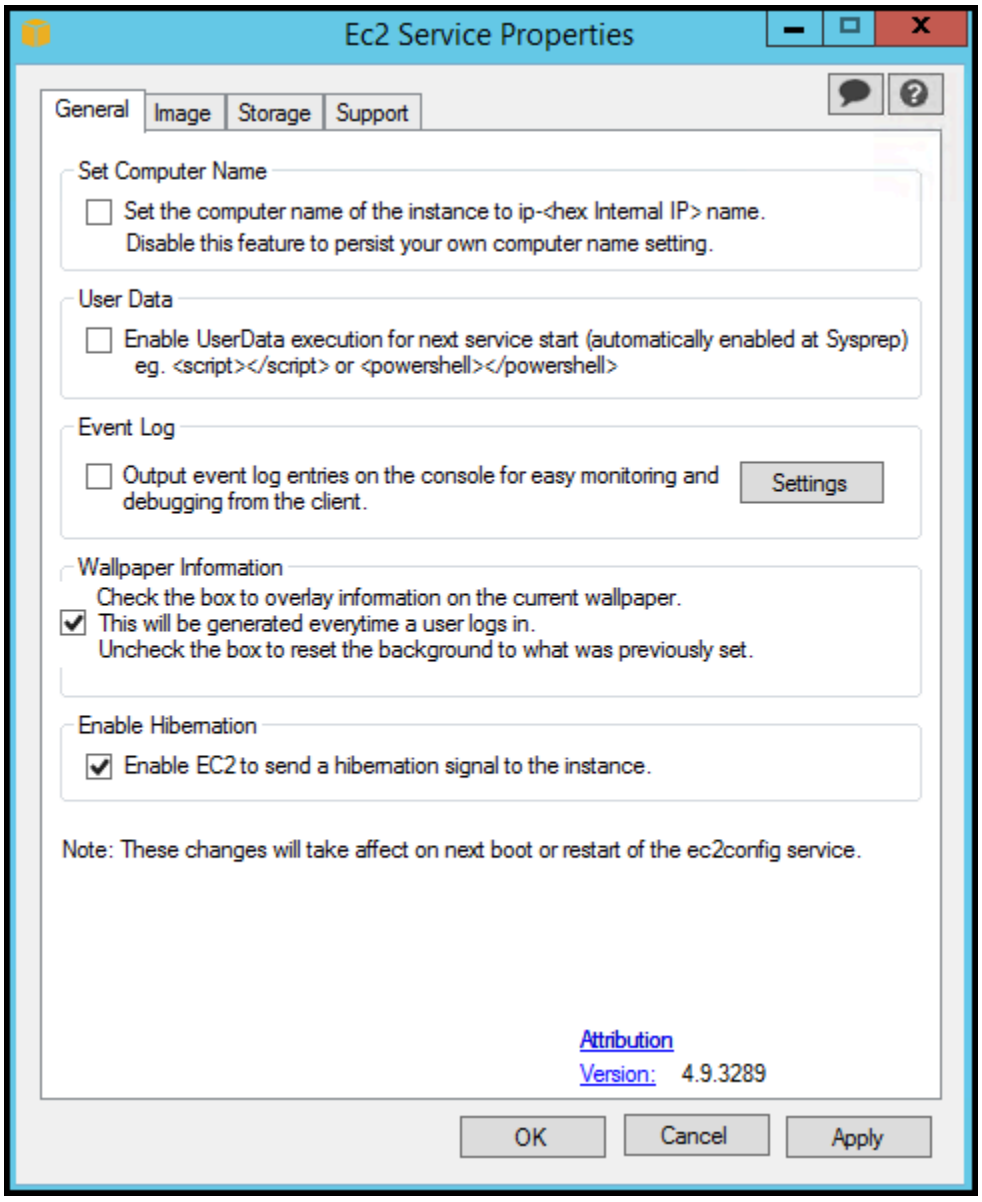
So konfigurieren Sie Proxy-Einstellungen mithilfe der Gruppenrichtlinie und Internet Explorer

1. Öffnen Sie auf einer Instance, auf der der EC2Config-Service über einen Proxy kommunizieren soll, die Eingabeaufforderung als Administrator, geben Sie **`gpedit.msc`** ein und drücken Sie auf die Eingabetaste.
2. Wählen Sie im lokalen Gruppenrichtlinien-Editor unter Local Computer Policy die Optionen Computer Configuration, Administrative Templates, Windows Components, Internet Explorer aus.
3. Wählen Sie im rechten Bereich Make proxy settings per-machine (rather than per-user) und anschließend Edit policy setting aus.
4. Wählen Sie Enabled und anschließend Apply aus.
5. Öffnen Sie Internet Explorer und wählen Sie die Schaltfläche Tools aus.
6. Wählen Sie Internet Option und anschließend die Registerkarte Connections aus.
7. Wählen Sie LAN settings aus.
8. Wählen Sie unter Proxy server die Option Use a proxy server for your LAN aus.
9. Geben Sie die Adresse und die Port-Informationen ein und wählen Sie anschließend OK aus.

Legen Sie die Eigenschaften des EC2Config-Services im Systemdialog auf Ihrer EC2-Windows-Instance fest

Der folgende Vorgang beschreibt, wie die Einstellungen anhand des Dialogfelds EC2-Service-Eigenschaften aktiviert bzw. deaktiviert werden.

1. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
2. Klicken Sie im Startmenü auf Alle Programme und anschließend auf EC2ConfigService Settings.



3. Aktivieren bzw. deaktivieren Sie auf der Registerkarte Allgemein im Dialogfeld EC2-Service-Eigenschaften die folgenden Einstellungen.

Set PC Name

Wenn diese Einstellung aktiviert ist (standardmäßig ist sie deaktiviert), wird der Hostname bei jedem Start mit der aktuellen internen IP-Adresse verglichen. Stimmen der Hostname und die interne IP-Adresse nicht überein, wird der Hostname zurückgesetzt, sodass er die interne IP-Adresse enthält und das System wird anschließend neu gestartet, um den neuen Hostnamen zu übernehmen. Aktivieren Sie diese Einstellung nicht, wenn Sie Ihren eigenen Hostnamen einrichten oder verhindern möchten, dass Ihr vorhandener Hostname geändert wird.

User Data

Die Ausführung der Benutzerdaten ermöglicht es Ihnen, in den Instance-Metadaten Skripts anzugeben. Standardmäßig werden diese Skripts beim ersten Start ausgeführt. Sie können sie auch so konfigurieren, dass sie beim nächsten Neustart oder Start der Instance oder bei jedem Neustart oder Start der Instance ausgeführt werden.

Wenn Sie ein großes Skript verwenden, empfehlen wir Ihnen, das Skript mithilfe der Benutzerdaten herunterzuladen und es anschließend auszuführen.

Weitere Informationen finden Sie unter Ausführung von Benutzerdaten.

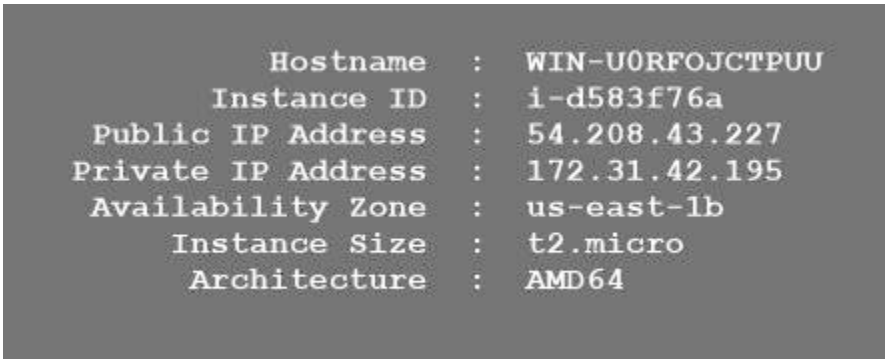
Ereignisprotokoll

Verwenden Sie diese Einstellung, um Ereignisprotokolleinträge während des Starts auf der Konsole anzuzeigen. Dadurch wird die Überwachung und das Debugging vereinfacht.

Klicken Sie auf Settings, um die Filter für die Protokolleinträge festzulegen, die an die Konsole gesendet werden sollen. Der Standardfilter sendet die drei neuesten Fehlereinträge vom Systemereignisprotokoll an die Konsole.

Wallpaper Information

Verwenden Sie diese Einstellung, um die Systeminformationen auf dem Desktop-Hintergrund anzuzeigen. Das folgende Beispiel zeigt die Informationen, die auf dem Desktop-Hintergrund angezeigt werden.

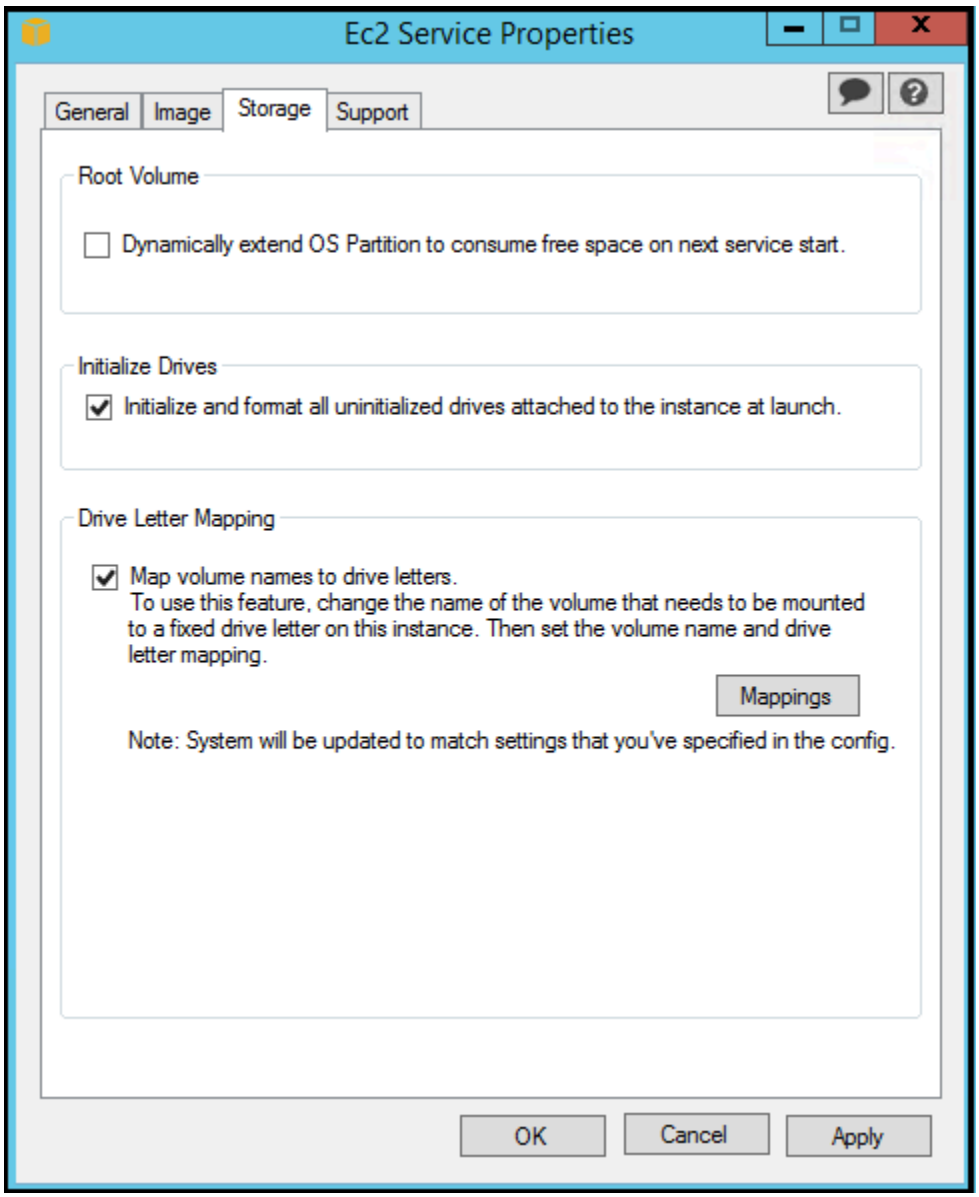


Die auf dem Desktop-Hintergrund angezeigten Informationen werden von der Einstellungsdatei gesteuer `EC2ConfigService\Settings\WallpaperSettings.xml`.

Enable Hibernation (Ruhezustand aktivieren

Verwenden Sie diese Einstellung, um zuzulassen, dass EC2 dem Betriebssystem signalisiert, die Instance in den Ruhezustand zu versetzen.

4. Klicken Sie auf die Registerkarte Storage. Sie können die folgenden Einstellungen aktivieren oder deaktivieren.



Root Volume

Diese Einstellung erweitert Festplatte 0/Volume 0 dynamisch, sodass der gesamte nicht partitionierte Speicherplatz eingeschlossen ist. Dies ist nützlich, wenn die Instance von einem Root-Volume gestartet wird, das eine benutzerdefinierte Größe hat.

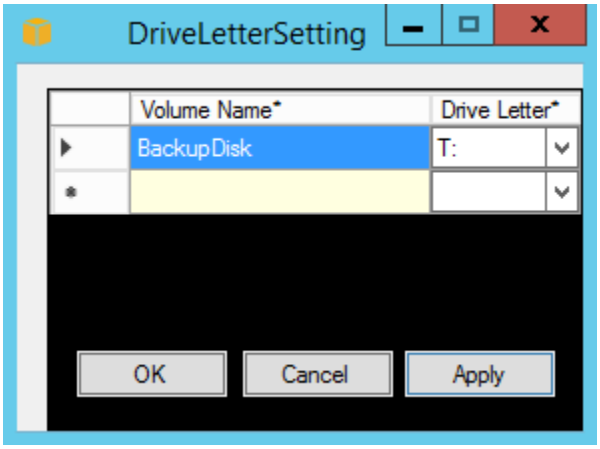
Initialize Drives

Diese Einstellung formatiert und installiert alle Volumes, die der Instance beim Start angefügt sind.

Drive Letter Mapping

Das System ordnet die Volumes, die einer Instance angefügt sind, einem Laufwerkbuchstaben zu. Standardmäßig werden die Amazon EBS-Volumes den Laufwerkbuchstaben von D: nach Z: zugeordnet. Die Standardeinstellung für Instance-Speicher-Volumes hängt vom Treiber ab. AWS PV-Treiber und Citrix-PV-Treiber ordnen die Instance-Speicher-Volumes den Laufwerkbuchstaben von Z: nach A: zu. Red Hat-Treiber ordnen die Instance-Speicher-Volumes den Laufwerkbuchstaben von D: nach Z: zu.

Klicken Sie auf Mappings, um die Laufwerkbuchstaben für die Volumes auszuwählen. Geben Sie im Dialogfeld DriveLetterSetting (Einstellung des Laufwerkbuchstaben) die Werte Volume Name (Volume-Name) und Drive Letter (Laufwerkbuchstabe) für die einzelnen Volumes an und klicken Sie auf Apply (Übernehmen) und OK. Wir empfehlen Ihnen, Laufwerkbuchstaben zu verwenden, die keine Konflikte mit bereits verwendeten Laufwerkbuchstaben hervorrufen, beispielsweise Laufwerkbuchstaben aus der Mitte des Alphabets.



Nachdem Sie eine Laufwerkzuweisung festgelegt und ein Volume mit der gleichen Kennung wie einer der angegebenen Volumenamen angefügt haben, weist EC2Config den angegebenen Laufwerksbuchstaben automatisch diesem Volume zu. Wird der Laufwerkbuchstabe jedoch bereits verwendet, schlägt die Zuweisung des Laufwerkbuchstaben fehl. Beachten Sie, dass EC2Config die Laufwerkbuchstaben der Volumes, die vor der Zuweisung des Laufwerkbuchstabens bereits gemountet waren, nicht ändert.

5. Um die Einstellungen zu speichern und mit der Arbeit daran an einem späteren Zeitpunkt fortzufahren, klicken Sie auf OK, um das Dialogfeld EC2-Serviceeigenschaften zu schließen. Wenn die Anpassung der Instance abgeschlossen ist und Sie ein AMI aus der Instance erstellen

möchten, finden Sie weitere Information unter Ein Amazon-EC2-AMI mit Windows Sysprep erstellen.

Fehlerbehebung beim EC2Config-Start-Agent

Die folgenden Informationen können Ihnen helfen, Probleme mit Ihrem EC2Config-Service zu beheben.

Aktualisieren von EC2Config auf einer unerreichbaren Instance

Verwenden Sie das folgende Verfahren, um den EC2Config-Service auf einer unerreichbaren Windows Server-Instance mithilfe des Remote Desktop zu aktualisieren.

So aktualisieren Sie EC2Config auf einer von Amazon EBS gestützten Windows-Instance, zu der Sie keine Verbindung herstellen können

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Starten Sie die betroffene Instance. Wählen Sie die Instance und wählen Sie Instance state (Instance-Status) und dann Stop instance (Instance anhalten).

   > **Warning**
   >
   > Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

4. Wählen Sie Launch Instance (Instance starten) aus und erstellen Sie eine temporäre `t2.micro`-Instance in derselben Availability Zone wie die betroffene Instance. Verwenden Sie ein anderes AMI als das, mit dem die betroffene Instance gestartet wurde.

   > **Important**
   >
   > Wenn Sie die Instance nicht in der gleichen Availability Zone wie die betroffene Instance erstellen, können Sie das Stamm-Volume der betroffenen Instance nicht der neuen Instance anfügen.

5. Wählen Sie in der EC2-Konsole Volumes aus.

6. Lokalisieren Sie das Stamm-Volume der betroffenen Instance. Trennen Sie das Volume und fügen Sie das Volume anschließend der temporären Instance an, die Sie zuvor erstellt haben. Fügen Sie es dem standardmäßigen Gerätenamen (xvdf) an.
7. Stellen Sie über Remote Desktop eine Verbindung mit der temporären Instance her und verwenden Sie anschließend das Dienstprogramm für die Datenträgerverwaltung, um das Volume verfügbar zu machen und es zu verwenden.
8. Laden Sie die aktuelle Version des EC2Config-Service herunter. Extrahieren Sie die Dateien aus der `.zip`-Datei in das `Temp`-Verzeichnis auf dem von Ihnen angefügten Laufwerk.
9. Öffnen Sie in der temporären Instance das Dialogfeld "Ausführen", geben Sie **`regedit`** ein und drücken Sie die Eingabetaste.
10. Wählen Sie `HKEY_LOCAL_MACHINE`. Wählen Sie im Menü File die Option Load Hive aus. Wählen Sie das Laufwerk aus und navigieren Sie zur folgenden Datei und öffnen Sie sie: `Windows\System32\config\SOFTWARE`. Geben Sie nach Aufforderung einen Schlüsselnamen ein.
11. Wählen Sie den gerade geladenen Schlüssel aus und navigieren Sie zu `Microsoft\Windows\CurrentVersion`. Wählen Sie den `RunOnce`-Schlüssel aus. Wenn dieser Schlüssel nicht vorhanden ist, wählen Sie im Kontextmenü (rechte Maustaste) `CurrentVersion`, New und anschließend Key aus. Benennen Sie den Schlüssel `RunOnce`.
12. Wählen Sie im Kontextmenü (rechte Maustaste) den `RunOnce`-Schlüssel, New und anschließend String Value aus. Geben Sie `Ec2Install` als den Namen und `C:\Temp\Ec2Install.exe /quiet` als die Daten ein.
13. Wählen Sie den `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon`-Schlüssel aus. Wählen Sie im Kontextmenü (rechte Maustaste) die Option New und anschließend String Value aus. Geben Sie **`AutoAdminLogon`** als den Namen und **`1`** als die Daten ein.
14. Wählen Sie den `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon`>-Schlüssel aus. Wählen Sie im Kontextmenü (rechte Maustaste) die Option New und anschließend String Value aus. Geben Sie **`DefaultUserName`** als den Namen und **`Administrator`** als die Daten ein.
15. Wählen Sie den `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon`-Schlüssel aus. Wählen Sie im Kontextmenü (rechte Maustaste) die Option New und anschließend String Value aus. Geben Sie **`DefaultPassword`** als Namen an und geben Sie ein Passwort in den Wertedaten ein.

16. Wählen Sie im Navigationsbereich „Registry Editor“ den temporären Schlüssel aus, den Sie beim ersten Öffnen des Registrierungs-Editors erstellt haben.
17. Wählen Sie im Menü File die Option Unload Hive aus.
18. Wählen Sie im Dienstprogramm für die Datenträgerverwaltung das Laufwerk aus, das Sie zugewiesen haben, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie die Option Offline aus.
19. Trennen Sie in der Amazon EC2-Konsole das betroffene Volume von der temporären Instance und ordnen Sie es wieder der ursprünglichen Instance mit dem Gerätenamen z `/dev/sda1`. Sie müssen diesen Gerätenamen angeben, um das Volume als Stamm-Volume hinzufügen zu können.
20. Stoppen und starten Sie EC2 Amazon-InstancesFühren Sie das der Instance aus.
21. Überprüfen Sie nach dem Start der Instance das Systemprotokoll und vergewissern Sie sich, dass die Meldung Windows ist einsatzbereit angezeigt wird.
22. Öffnen Sie den Registrierungs-Editor und wählen Sie au `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`. Löschen Sie die zuvor von Ihnen erstellten Schlüssel für den Zeichenfolgenwert: AutoAdminLogon, DefaultUserName und DefaultPassword.
23. Löschen Sie die in diesem Vorgang erstellte temporäre Instance bzw. beenden Sie sie.

EC2Config-Versionshistorie

Die folgende Tabelle beschreibt die veröffentlichten Versionen von EC2Config. Weitere Informationen zu den Aktualisierungen von SSM Agent finden Sie in den Versionshinweisen für Systems Manager-SSM-Agent.

> **Important**
>
> EC2Config-Service hat das Ende der Unterstützung erreicht. Nur die aktuelle Version des EC2Config-Agenten steht zum Herunterladen zur Verfügung. Frühere Versionen sind als privat gekennzeichnet.

Version	Details	Datum der Veröffentlichung
4.9.5777	• Es wurde ein Problem behoben, bei dem die RSS-Konfiguration für einige Instance-Typen falsch eingestellt war. • Neue Version von SSM Agent `3.3.484.0` .	17. Juni 2024
4.9.5554	• Einschränkung der Übertragung von Domainnamen auf der Grundlage eines Registrierungseintrags: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Neue Version von SSM Agent `3.2.1630.0` .	04. Oktober 2023
4.9.5467	• Wiederholungsfunktion zum Erkennen des Konsolenports hinzugefügt. • Neue Version von SSM Agent `3.1.2282.0` .	01. August 2023
4.9.5288	• AWS Core SDK wurde auf Version `3.7.103.23` aktualisiert. • Es wurde ein Problem behoben, bei dem das `AWS-UpdateEC2Config` -SSM-Dokument `EC2Config` auf Instances, die nur mit IMDSv2 aktiviert sind, nicht aktualisiert. • Neue Version von SSM Agent `3.1.2144.0` .	08. März 2023
4.9.5231	• Neue Version des SSM-Agenten 3.1.1927.0.	14. Februar 2023
4.9.5103	• Problem behoben, bei dem ephemere Volumes in den Instance-Familien R5D und i4i falsch identifiziert wurden. •	5. Dezember 2022

Version	Details	Datum der Veröffentlichung
	Neue Version von SSM Agent 3.1.1856.0.	
4.9.5064	• Aktualisiert, um PCI-Segmentinformationen zur Auswahl des Konsolenports zu verwenden. • Signierte PowerShell-Skripts und zusätzliche Copyright-Header. • Die Auswahllogik für den primären Netzwerkadapter wurde korrigiert. • Neue Version von SSM Agent 3.1.1732.0.	16. November 2022
4.9.4588	• Die IMDS-Wartelogik wurde aktualisiert, um nur IMDSv2-Anforderungen zu stellen. • Die Shared Library libec2launch.dll launch-agent wurde hinzugefügt. • Neue Version von SSM Agent 3.1.1188.0.	31. Mai 2022
4.9.4556	• Wartelogik wurde hinzugefügt, um vollständige Initialisierung des NIC vor der Verwendung sicherzustellen. • Neue Version von Log4Net 2.0.14.0 nimmt Sicherheitspatch auf. • Neue Version von SSM Agent 3.1.1045.0 nimmt Sicherheitspatch auf.	1. März 2022
4.9.4536	• Es wurde ein Problem behoben, bei dem userdata abstürzt, wenn der Temp-Ordner fehlt. • Neue Version von SSM Agent 3.1.804.0.	31. Januar 2022

Version	Details	Datum der Veröffentlichung
4.9.4508	• Es wurde ein Problem mit der Berechnung des DiskPart-Skriptpfads behoben. • Neue Version von SSM Agent 3.1.338.0.	6. Oktober 2021
4.9.4500	• Aktualisiert `Install-EgpuManagerConfig` mit IMDS-v2-Unterstützung. • Weblinks wurden aktualisiert, um https zu verwenden. • Neue Version von SSM Agent 3.1.282.0	7. September 2021
4.9.4419	• IMDS Version 1 Fallback-Logik wurde korrigiert • Aktualisiert die gesamte Verwendung des temporären Windows Verzeichnisses in das temporäre Verzeichnis EC2Config • Neue Version von SSM Agent 3.0.1124.0	2. Juni 2021
4.9.4381	• Unterstützung für SSM-Dokumentschema-Version 2.2 in EC2ConfigUpdater hinzugefügt • AWS-Nitro-Enclaves-Paketversion zu Konsolenprotokoll hinzugefügt • Neue Version von SSM Agent 3.0.529.0	04. Mai 2021
4.9.4326	• Alle Links in der Einstellungen Benutzeroberfläche entfernt • Dies ist die letzte EC2Config-Version, die Windows Server 2008 unterstützt.	3. März 2021

Version	Details	Datum der Veröffentlichung
4.9.4279	• Sicherheitsproblem im Zusammenhang mit der geplanten Aufgabe `Ec2ConfigMonitor` behoben • Problem mit der Zuordnung von Laufwerksbuchstaben und falscher Anzahl flüchtiger Datenträger behoben • `OsCurrentBuild` und `OsReleaseId` zur Konsolenausgabe hinzugefügt • Neue Version von SSM Agent 2.3.871.0	11. Dezember 2020
4.9.4222	• IMDS Version 1 Fallback-Logik wurde korrigiert • Neue Version von SSM Agent (2.3.842.0)	7. April 2020
4.9.4122	• Unterstützung für IMDS v2 hinzugefügt • Neue Version von SSM Agent (2.3.814.0)	4. März 2020
4.9.3865	• Problem mit dem Erkennen des COM-Anschlusses für Windows Server 2008 R2 auf Metal-Instances behoben • Neue Version von SSM Agent (2.3.722.0)	31. Oktober 2019
4.9.3519	• Neue Version von SSM Agent (2.3.634.0)	18. Juni 2019
4.9.3429	• Neue Version von SSM Agent (2.3.542.0)	25. April 2019
4.9.3289	• Neue Version von SSM Agent 2.3.444.0	11. Februar 2019
4.9.3270	• Plug-In hinzugefügt, mit dem sich einstellen lässt, dass der Monitor nie ausgeschaltet wird, um ACPI-Probleme zu beheben • SQL Server-Edition und -Version in die Konsole geschrieben • Neue Version von SSM Agent 2.3.415.0	22. Januar 2019

Version	Details	Datum der Veröffentlichung
4.9.3230	• Zuweisung des Laufwerkbuchstabens für eine bessere Abstimmung mit der Funktionalität aktualisiert • Neue Version von SSM Agent 2.3.372.0	10. Januar 2019
4.9.3160	• Erhöhte Wartezeit für die primäre NIC • Standardkonfiguration für RSS- und Empfangswarteschlangen-Einstellungen für ENA-Geräte hinzugefügt • Ruhezustand während Sysprep deaktiviert • Neue Version von SSM Agent 2.3.344.0 • AWS SDK auf 3.3.29.13 upgegradet	15. Dezember 2018
4.9.3067	• Verbesserungen beim Instance-Ruhezustand • Neue Version von SSM Agent 2.3.235.0	8. November 2018
4.9.3034	• Route 169.254.169.253/32 für DNS-Server hinzugefügt • Neue Version von SSM Agent 2.3.193.0	24. Oktober 2018
4.9.2986	• Signatur für alle EC2Config-bezogenen Binärdateien hinzugefügt • Neue Version von SSM Agent 2.3.136.0	11. Oktober 2018
4.9.2953	Neue Version von SSM Agent (2.3.117.0)	2. Oktober 2018
4.9.2926	Neue Version von SSM Agent (2.3.68.0)	18. September 2018

Version	Details	Datum der Veröffentlichung
4.9.2905	• Neue Version von SSM Agent (2.3.50.0) • Route 169.254.169.123/32 zum AMZN-Zeitservice hinzugefügt • Route 169.254.169.249/32 zum GRID-Lizenzdienst hinzugefügt • Behebung eines Fehlers, der dazu geführt hat, dass EBS-NVMe-Volumes flüchtig ausgeführt werden.	17. September 2018
4.9.2854	Neue Version von SSM Agent (2.3.13.0)	17. August 2018
4.9.2831	Neue Version von SSM Agent (2.2.916.0)	7. August 2018
4.9.2818	Neue Version von SSM Agent (2.2.902.0)	31. Juli 2018
4.9.2756	Neue Version von SSM Agent (2.2.800.0)	27. Juni 2018
4.9.2688	Neue Version von SSM Agent (2.2.607.0)	25. Mai 2018
4.9.2660	Neue Version von SSM Agent (2.2.546.0)	11. Mai 2018
4.9.2644	Neue Version von SSM Agent (2.2.493.0)	26. April 2018
4.9.2586	Neue Version von SSM Agent (2.2.392.0)	28. März 2018
4.9.2565	• Neue Version von SSM Agent (2.2.355.0) • Behebung eines Problems auf M5- und C5-Instances (PV-Treiber konnten nicht gefunden werden) • Hinzufügen der Konsolenprotokollierung für den Instance-Typ, neueste PV-Treiber und NVMe-Treiber	13. März 2018
4.9.2549	Neue Version von SSM Agent (2.2.325.0)	8. März 2018

Version	Details	Datum der Veröffentlichung
4.9.2461	Neue Version von SSM Agent (2.2.257.0)	15. Februar 2018
4.9.2439	Neue Version von SSM Agent (2.2.191.0)	6. Februar 2018
4.9.2400	Neue Version von SSM Agent (2.2.160.0)	16. Januar 2018
4.9.2327	• Neue Version von SSM Agent (2.2.120.0) • COM-Port-Discovery auf Amazon EC2-Bare-Metal-Instances hinzugefügt • Hyper-V-Statusprotokollierung auf Amazon EC2-Bare-Metal-Instances hinzugefügt	2. Januar 2018
4.9.2294	Neue Version von SSM Agent (2.2.103.0)	4. Dezember 2017
4.9.2262	Neue Version von SSM Agent (2.2.93.0)	15. November 2017
4.9.2246	Neue Version von SSM Agent (2.2.82.0)	11. November 2017
4.9.2218	Neue Version von SSM Agent (2.2.64.0)	29. Oktober 2017
4.9.2212	Neue Version von SSM Agent (2.2.58.0)	23. Oktober 2017
4.9.2203	Neue Version von SSM Agent (2.2.45.0)	19. Oktober 2017

Version	Details	Datum der Veröffentlichung
4.9.2188	Neue Version von SSM Agent (2.2.30.0)	10. Oktober 2017
4.9.2180	• Neue Version von SSM Agent (2.2.24.0) • Das Elastic GPU-Plug-in für GPU-Instances hinzugefügt.	5. Oktober 2017
4.9.2143	Neue Version von SSM Agent (2.2.16.0)	1. Oktober 2017
4.9.2140	Neue Version von SSM Agent (2.1.10.0)	
4.9.2130	Neue Version von SSM Agent (2.1.4.0)	
4.9.2106	Neue Version von SSM Agent (2.0.952.0)	
4.9.2061	Neue Version von SSM Agent (2.0.922.0)	
4.9.2047	Neue Version von SSM Agent (2.0.913.0)	
4.9.2031	Neue Version von SSM Agent (2.0.902.0)	
4.9.2016	• Neue Version von SSM Agent (2.0.879.0) • Den CloudWatch Logs-Verzeichnispfad für Windows Server 2003 korrigiert.	
4.9.1981	• Neue Version von SSM Agent (2.0.847.0) • Problem mit der Generierung von `important.txt` in den EBS-Volumes behoben.	
4.9.1964	Neue Version von SSM Agent (2.0.842.0)	

Version	Details	Datum der Veröffentlichung
4.9.1951	• Neue Version von SSM Agent (2.0.834.0) • Problem bei der Zuweisung des Laufwerkbuchstaben für flüchtige Laufwerke von Z: aus behoben.	
4.9.1925	• Neue Version von SSM Agent (2.0.822.0) • [Fehler] Diese Version ist kein gültiges Aktualisierungsziel von SSM Agent v4.9.1775.	
4.9.1900	Neue Version von SSM Agent (2.0.805.0)	
4.9.1876	• Neue Version von SSM Agent (2.0.796.0) • Problem mit der Ausgabe-/Fehlerweiterleitung bei der Ausführung der Administrator-Benutzerdaten behoben.	
4.9.1863	• Neue Version von SSM Agent (2.0.790.0) • Probleme beim Anfügen mehrerer EBS-Volumes an eine Amazon EC2-Instance behoben. • Verbesserung von CloudWatch bei der Ausführung des Konfigurationspfads bei gleichzeitiger Beibehaltung der Abwärtskompatibilität.	
4.9.1791	Neue Version von SSM Agent (2.0.767.0)	
4.9.1775	Neue Version von SSM Agent (2.0.761.0)	
4.9.1752	Neue Version von SSM Agent (2.0.755.0)	
4.9.1711	Neue Version von SSM Agent (2.0.730.0)	

Version	Details	Datum der Veröffentlichung
4.8.1676	Neue Version von SSM Agent (2.0.716.0)	
4.7.1631	Neue Version von SSM Agent (2.0.682.0)	
4.6.1579	• Neue Version von SSM Agent (2.0.672.0) • Problem bei der Agenten-Aktualisierung in v4.3, v4.4 und v4.5 behoben.	
4.5.1534	Neue Version von SSM Agent (2.0.645.1)	
4.4.1503	Neue Version von SSM Agent (2.0.633.0)	
4.3.1472	Neue Version von SSM Agent (2.0.617.1)	
4.2.1442	Neue Version von SSM Agent (2.0.599.0)	
4.1.1378	Neue Version von SSM Agent (2.0.558.0)	

Version	Details	Datum der Veröffentlichung
4.0.1343	• Run Command, State Manager, der CloudWatch-Agent und der Support für die Domain-Verbindung wurden in einen anderen Agenten mit dem Namen SSM Agent verschoben. SSM Agent wird als Teil des EC2Config-Upgrades installiert. Weitere Informationen finden Sie unter EC2Config und AWS Systems Manager. • Wenn Sie in EC2Config einen Proxy eingerichtet haben, müssen Sie Ihre Proxy-Einstellungen für SSM Agent aktualisieren, bevor Sie den Upgrade vornehmen können. Wenn Sie die Proxy-Einstellungen nicht aktualisieren, können Sie den Run Command nicht für die Verwaltung Ihrer Instances verwenden. Um dies zu vermeiden, beachten Sie die folgenden Informationen, bevor Sie das Update auf die neuere Version ausführen: Installation und Konfiguration von SSM Agent auf Windows-Instances im AWS Systems Manager-Benutzerhandbuch. • Wenn Sie zuvor die CloudWatch-Integration durch eine lokale Konfigurationsdatei (`AWS.EC2.Windows.CloudWatch.json`) auf Ihren Instances aktiviert haben, müssen Sie die Datei für die Zusammenarbeit mit SSM Agent konfigurieren.	
3.19.1153	• Erneut aktivierter Aktivierungs-Plug-in für Instances mit alter AWS KMS-Konfiguration. Überspringen Sie die Aktivierung für BYOL-Benutzer. • Änderung des TRIM-Standardverhaltens, sodass es während der Festplattenformatierung deaktiviert ist, und Hinzufügung von FormatWithTRIM, um das InitializeDisks-Plug-in mit Benutzerdaten zu überschreiten.	

Version	Details	Datum der Veröffentlichung
3.18.1118	• Korrektur, um dem primären Netzwerkadapter jetzt zuverlässig Routen hinzufügen zu können. • Updates, um den Support der AWS-Services zu verbessern.	
3.17.1032	• Korrektur der duplizierten Systemprotokolle, wenn die Filter auf die gleiche Kategorie gesetzt sind. • Korrektur des "Hängenbleibens" während der Festplatteninitialisierung.	
3.16.930	Zusätzlicher Support beim Start für die Protokollierung des Ereignisses "Windows ist einsatzbereit" im Windows-Ereignisprotokoll.	
3.15.880	Korrektur, um das Hochladen der Systems Manager Run Command-Ausgabe in S3-Bucket-Namen mit dem Zeichen ‘.’ zu erlauben.	
3.14.786	Zusätzlicher Support, um die Einstellungen des InitializeDisks-Plug-ins zu überschreiben. Beispiel: Um die Initialisierung der SSD-Festplatte zu beschleunigen, können Sie TRIM vorübergehend deaktivieren, indem Sie dies in den Benutzerdaten festlegen: <InitializeDrivesSettings><SettingsGroup>FormatWithoutTRIM</SettingsGroup></InitializeDrivesSettings	
3.13.727	Systems Manager Run Command – Korrektur, um Befehle nach dem Windows-Neustart zuverlässig zu verarbeiten.	

Version	Details	Datum der Veröffentlichung
3.12.649	• Korrektur, um den Neustart bei der Ausführung von Befehlen/Skripten zuverlässig auszuführen. • Korrektur, um Ausführungsbefehle zuverlässig abzubrechen. • Unterstützung für das (optionale) Hochladen der MSI-Protokolle nach S3 hinzugefügt, wenn Anwendungen über Systems Manager Run Command installiert werden.	
3.11.521	• Korrektur der Generierung von RDP-Thumbprints für Windows Server 2003 • Korrektur, durch die die Zeitzonen und der UTC-Offset in die EC2Config-Protokollzeilen eingeschlossen werden. • Systems Manager-Unterstützung, um Run Command-Befehle im Parallelmodus auszuführen. • Zurücksetzen der vorangegangenen Änderung, um partitionierte Festplatten online zu stellen.	
3.10.442	• Behebden der Systems Manager-Konfigurationsfehler bei der Installation von MSI-Anwendungen. • Korrektur, um die Speicherlaufwerke zuverlässig online zu stellen. • Updates, um den Support der AWS-Services zu verbessern.	

Version	Details	Datum der Veröffentlichung
3.9.359	• Korrektur der Bereitstellung des Sysprep-Skripts, um die Konfiguration des Windows-Updates im Standardstatus zu belassen. • Korrektur des Plug-ins für die Passwortgenerierung, um die Einhaltung der Einstellungen für die GPO-Passwortrichtlinien zu verbessern. • Beschränkung der EC2Config-/SSM-Protokollordnerberechtigungen auf die lokale Administratorgruppe. • Updates, um den Support der AWS-Services zu verbessern.	
3.8.294	• Korrektur eines Problems mit CloudWatch, durch das die Protokolle nicht hochgeladen werden konnten, wenn Sie sich nicht auf dem primären Laufwerk befanden. • Verbesserung der Festplatteninitialisierung durch das Hinzufügen von Logik für Wiederholversuche. • Verbesserung der Fehlerbehandlung, wenn das SetPassword-Plug-in bei der AMI-Erstellung gelegentlich fehlschlug. • Updates, um den Support der AWS-Services zu verbessern.	

Version	Details	Datum der Veröffentlichung
3.7.308	• Verbesserungen am Dienstprogramm "ec2config-cli" beim "config"-Testen und bei der Fehlerbehebung innerhalb der Instance. • Vermeiden Sie das Hinzufügen statischer Routen auf einem OpenVPN-Adapter für den AWS KMS- und Metadaten-Service. • Korrektur eines Problems, bei dem bei der Ausführung der Benutzerdaten das "persist"-Tags (Markierungen) nicht berücksichtigt wurde. • Verbesserung der Fehlerbehandlung, wenn die Anmeldung bei der EC2-Konsole nicht möglich war. • Updates, um den Support der AWS-Services zu verbessern.	
3.6.269	• Korrektur der Aktivierungszuverlässigkeit von Windows durch die Verwendung der lokalen Adresse 169.254.0.250/251 für die Aktivierung von Windows über AWS KMS • Verbesserte Proxy-Handhabung in Systems Manager-, Windows-Aktivierungs- und Domain-Verbindungsszenarien • Korrektur eines Problems, bei dem der Sysprep-Antwortdatei duplizierte Benutzerkontenzeilen hinzugefügt wurden.	

Version	Details	Datum der Veröffentlichung
3.5.228	• Korrektur eines Szenarios, bei dem das CloudWatch-Plug-in möglicherweise exzessive CPU- und Windows Ereignisprotokolle verbraucht. • Ein Link zur Konfigurationsdokumentation von CloudWatch wurde der Benutzeroberfläche für die EC2Config-Einstellungen hinzugefügt.	
3.4.212	• Korrektur von EC2Config bei der Verwendung mit VM Import. • Korrektur eines Problems bei der Namensgebung im WiX-Installer.	

Version	Details	Datum der Veröffentlichung
3.3.174	• Verbesserung bei der Ausnahmebehandlung von Fehlschlägen in Systems Manager und bei der Verbindung von Domains. • Änderung zur Unterstützung des Systems Manager-Schema-Versioning. • Fehlerbehebung bei der Formatierung flüchtiger Festplatten unter Win2K3. • Änderung, um die Konfiguration von Festplattengrößen über 2 TB zu unterschützen. • Geringerer Verbrauch des virtuellen Speichers durch die Einrichtung des GC-Modus als Standard. • Unterstützung für Herunterladen von Artefakten aus dem UNC-Pfad im `aws:psModule` - und `aws:application` - Plug-in. • Verbesserung der Protokollierung für das Windows Aktivierungs-Plug-in.	

Version	Details	Datum der Veröffentlichung
3.2.97	• Leistungsverbesserungen durch verzögertes Laden der Systems Manager-SSM-Komponenten. • Verbesserte Ausnahmebehandlung für falsch formatierte sysprep2008.xml. • Befehlszeilenunterstützung für die Systems Manager „Apply“-Konfiguration. • Änderung, um die Verbindung von Domains zu unterstützen, wenn eine Umbenennung des Computers ansteht. • Unterstützung optionaler Parameter im `aws:applications` -Plug-in. • Unterstützung des Befehls-Arrays im `aws:psModule` -Plug-in.	
3.0.54	• Unterstützung für Systems Manager aktiviert. • Automatische Domain-Verbindung von EC2-Windows-Instances mit einem AWS-Verzeichnis über Systems Manager. • Konfiguration und Upload der CloudWatch Logs/-Metriken über Systems Manager. • Installation der PowerShell-Module über Systems Manager. • Installation der MSI-Anwendungen über Systems Manager.	

Version	Details	Datum der Veröffentlichung
2.4.233	• Hinzufügen einer geplanten Aufgabe, um EC2Config nach fehlerhaften Service-Startups wiederherzustellen. • Verbesserungen an den Benachrichtigungen über die Protokollfehler für die Konsole. • Updates, um den Support der AWS-Services zu verbessern.	
2.3.313	• Korrektur des hohen Speicherverbrauchs, der zeitweise auftrat, wenn das Feature "CloudWatch Logs" aktiviert ist. • Upgradefehler behoben, sodass EC2Config-Versionen niedriger als 2.1.19 auf die neueste Version aktualisiert werden können. • Ausnahmebehandlung für die COM-Port-Öffnung aktualisiert, sodass sie benutzerfreundlicher und zweckdienlicher ist. • Größenanpassung der Ec2configServiceSettings-Benutzeroberfläche deaktiviert und Probleme bei der Platzierung der Attribut- und Versionenanzeige in der Benutzeroberfläche behoben.	
2.2.12	• Behandlung der NullPointerException, die bei einer Abfrage des Registrierungsschlüssels zur Bestimmung des Windows Sysprep-Status gelegentlich "Null" zurückgab. • Freisetzung unverwalteter Ressourcen im finally-Block.	
2.2.11	Problem bei der Handhabung leerer Protokollzeilen im CloudWatch-Plug-in behoben.	

Version	Details	Datum der Veröffentlichung
2.2.10	• Konfiguration der CloudWatch-Log-Einstellungen mithilfe der Benutzeroberfläche entfernt. • Ermöglichen Sie Benutzern das Definieren von CloudWatch-Logs-Einstellungen in der `%ProgramFiles%\Amazon\Ec2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json` -Datei, um zukünftige Verbesserungen zu ermöglichen.	
2.2.9	Problem mit unbehandelten Ausnahmen behoben sowie Protokollierung hinzugefügt.	
2.2.8	• Problem bei der Überprüfung der Windows-Betriebssystemversion im EC2Config-Installer behoben, um Windows Server 2003 SP1 und höher zu unterstützen. • Problem bei der Behandlung des Nullwerts beim Lesen der Registrierungsschlüssel behoben, die für die Aktualisierung der Sysprep-Config-Dateien benötigt werden.	
2.2.7	• Support für EC2Config hinzugefügt, um bei der Ausführung von Sysprep für Windows 2008 und höher ausgeführt zu werden. • Verbesserung der Ausnahmebehandlung und Protokollierung zur Optimierung der Diagnosen.	

Version	Details	Datum der Veröffentlichung
2.2.6	• Reduzierung der Last für die Instance und die CloudWatch-Protokolle, wenn Protokollereignisse hochgeladen werden. • Problem beim Upgrade behoben, bei dem das Plug-in für die CloudWatch Logs nicht immer aktiv blieb.	
2.2.5	• Support beim Hochladen der Protokolle zum CloudWatch-Log-Service hinzugefügt. • Problem mit der Bedingung im EC2OutputRDPCert-Plug-in behoben. • Änderung der Wiederherstellungsoption für den EC2Config -Service, sodass der Neustart von TakeNoAction erfolgen kann. • Weitere Ausnahmeinformationen hinzugefügt, für den Fall, das EC2Config fehlschlägt.	
2.2.4	• Rechtschreibfehler in PostSysprep.cmd korrigiert. • Problem beim Anpinnen von EC2Config im Startmenü von OS2012+ behoben.	

Version	Details	Datum der Veröffentlichung
2.2.3	• Option hinzugefügt, sodass EC2Config sofort nach dem Installieren startet, auch ohne Service. Führen Sie dazu "Ec2Install.exe start=false'" von der Befehlszeile aus. • Parameter im Bildschirmhintergrund-Plug-in hinzugefügt, über den das Hinzufügen/Entfernen des Bildschirmhintergrunds gesteuert werden kann. Führen Sie dazu "Ec2WallpaperInfo.exe set" oder "Ec2WallpaperInfo.exe revert" von der Befehlszeile aus. • Überprüfung des RealTimeIsUniversal-Schlüssels sowie Ausgabe der falschen Einstellungen des RealTimeIsUniveral-Registrierungsschlüssels an die Konsole hinzugefügt. • EC2Config-Abhängigkeit vom Windows Temp-Ordner entfernt. • Abhängigkeit von der UserData-Ausführung auf .Net 3.5 entfernt.	
2.2.2	• Zusätzliche Überprüfung des Verhaltens bei der Servicebeendigung, damit sichergestellt wird, dass Ressourcen freigegeben werden. • Problem mit langen Ausführungszeiten bei der Verbindung zur Domain behoben	

Version	Details	Datum der Veröffentlichung
2.2.1	• Installer aktualisiert, damit Upgrades von älteren Versionen möglich sind. • Ec2WallpaperInfo-Fehler nur in der .Net4.5-Umgebung behoben. • Fehler bei der zeitweiligen Treiberermittlung behoben. • Option zur Installation im Hintergrund hinzugefügt. Führen Sie Ec2Install.exe mit der "q"-Option aus, z. B. "Ec2Install.exe -q"	
2.2.0	• Support für .Net4- und .Net4.5-Umgebungen hinzugefügt. • Installer aktualisiert	
2.1.19	• Unterstützung für die Kennzeichnung flüchtiger Datenspeicher bei Verwendung des Intel-Netzwerktreibers (z. B. C3-Instance-Typ) hinzugefügt. Weitere Informationen finden Sie unter Erweitertes Netzwerk in Amazon-EC2-Instances. • Support für AMI Origin Version und AMI Origin Name zur Konsolenausgabe hinzugefügt. • Änderungen an der Konsolenausgabe vorgenommen, um konsistente Formatierung/Analyse zu gewährleisten • Hilfedatei aktualisiert	

Version	Details	Datum der Veröffentlichung
2.1.18	• EC2Config-WMI-Objekt zur Abschlussbenachrichtigung hinzugefügt (-Namespace root\Amazon -Class EC2_ConfigService) • Performance der Startup-WMI-Abfrage mit großen Ereignisprotokollen verbessert, kann möglicherweise während der ersten Ausführung zu einer hohen CPU führen	
2.1.17	• Problem mit dem Füllen des Puffers für die Standardausgabe- und den Standardfehler bei der UserData-Ausführung behoben. • Anzeige eines falschen RDP-Thumbprints in der Konsolenausgabe für >= w2k8 OS behoben. • Die Konsolenausgabe umfasst jetzt "RDPCERTIFICATE-SubjectName:" für Windows 2008+, wobei der Wert für den Computer-Namen eingeschlossen ist. • Dem Dropdownmenü für die Zuweisung des Laufwerkbuchstaben wurde "D:\" hinzugefügt. • Schaltfläche "Hilfe" wurde nach oben rechts verschoben sowie das Erscheinungsbild verändert • Link zur Feedback-Umfrage hinzugefügt	

Version	Details	Datum der Veröffentlichung
2.1.16	• Registerkarte "General" umfasst einen Link zur EC2Config-Download-Seite für neue Versionen • Überlagerung des Desktop-Hintergrunds wird jetzt im Ordner "Users Local Appdata" und nicht mehr unter "My Documents" gespeichert, um die MyDoc-Weiterleitung zu unterstützen. • MSSQL-Servername wurde mit dem System im Post-Sysprep-Skript (2008+) synchronisiert. • Der Anwendungsordner wurde neu organisiert (Dateien wurden in das Plug-in-Verzeichnis verschoben und doppelte Dateien entfernt). • Ausgabe des Systemprotokolls wurde geändert (Konsole): • * Wechsel zu einem Datums-, Namens-, Wertformat zur Vereinfachung der Analyse. (Beginnen Sie, die Abhängigk eiten in das neue Format zu migrieren.) • * Plug-in-Status "Ec2SetPassword" hinzugefügt • * Sysprep wurden Start- und Endzeiten hinzugefügt • Problem bei der Kennzeichnung der flüchtigen Festplatten als "Temporary Storage" für Betriebssysteme behoben, die nicht in Englisch ausgeführt werden • Problem beim Deinstallieren von EC2Config nach der Ausführung von Sysprep behoben	

Version	Details	Datum der Veröffentlichung
2.1.15	• Anfragen an den Metadaten-Service optimiert • Metadaten umgehen jetzt die Proxy-Einstellungen • Flüchtige Festplatten werden als "Temporary Storage" gekennzeichnet und Impotant.txt wird, falls gefunden, auf das Volume platziert (nur Citrix PV-Treiber). Weitere Informationen finden Sie unter Upgrade von PV-Treibern auf EC2-Windows-Instances. • Flüchtigen Festplatten werden Laufwerkbuchstaben von Z nach A zugeordnet (nur Citrix PV-Treiber) – die Zuweisung kann mithilfe des Plug-ins für die Zuweisung des Laufwerkbuchstaben durch die Volume-Kennzeichnung "Temporary Storage X" überschrieben werden, wobei es sich bei "X" um eine Zahl zwischen 0 und 25 handelt • UserData wird direkt nach "Windows is Ready" ausgeführt	
2.1.14	Korrekturen für den Desktop-Hintergrund	
2.1.13	• Desktop-Hintergrund zeigt den Hostnamen standardmäßig an • Abhängigkeit vom Windows-Zeitdienst wurde entfernt • In Fällen, bei denen einer einzelnen Schnittstelle mehrere IPs zugeordnet wurden, wurde eine Route hinzugefügt	

Version	Details	Datum der Veröffentlichung
2.1.11	• Änderungen am Ec2Activation-Plug-in vorgenommen • - Aktivierungsstatus wird alle 30 Tagse überprüft • - Verbleiben bei der Übergangsfrist 90 Tage (von 180), wird die Aktivierung erneut versucht	
2.1.10	• Überlagerung des Desktop-Hintergrunds bleibt mit Sysprep oder beim Herunterfahren ohne Sysprep nicht länger erhalten • Benutzerdatenoption wird bei jedem Service-Start mit <persist>true</persist> ausgeführt • Speicherort und Name von /DisableWinUpdate.cmd auf /Scripts/PostSysprep.cmd geändert • Administratorpasswort in /Scripts/PostSysprep.cmd läuft jetzt standardmäßig nicht ab • Bei der Deinstallation wird das EC2Config-PostSysprep-Skript aus c:\windows\setup\script\CommandComplete.cmd entfernt • "Add Route" unterstützt benutzerdefinierte Schnittstellenmetriken	
2.1.9	UserData-Ausführung nicht länger auf 3851 Zeichen beschränkt	

Version	Details	Datum der Veröffentlichung
2.1.7	• Betriebssystemversion und Sprachen-ID werden in die Konsole geschrieben • EC2Config-Version wird in die Konsole geschrieben • PV-Treiber-Version wird in die Konsole geschrieben • Erkennung der Fehlerprüfung und Ausgabe werden beim nächsten Start an die Konsole übermittelt • config.xml wurde eine Option hinzugefügt, um Sysprep-Anmeldeinformationen zu erhalten • Logik zur Routenwiederholung hinzugefügt, falls ENI beim Start nicht verfügbar ist • PID für die Benutzerdaten-Ausführung in die Konsole geschrieben • Mindestlänge für das generierte Passwort vom GPO abgerufen • Legen Sie den Service-Start auf 3 Versuche fest. • S3_DownloadFile.ps1- und S3_Upload file.ps1-Beispiele dem /Scripts-Ordner hinzugefügt	

Version	Details	Datum der Veröffentlichung
2.1.6	• Versionsinformationen zur Registerkarte "General" hinzugefügt • Registerkarte "Bundle" zu "Image" umbenannt • Festlegung der Passwörter vereinfacht und passwortbezogene Benutzeroberflächenelemente von der Registerkarte "General" auf die Registerkarte "Image" verschoben • Registerkarte "Disk Settings" zu "Storage" umbenannt • Registerkarte "Support" mit häufig verwendeten Tools zur Fehlerbehebung hinzugefügt • Die Datei `sysprep.ini` unter Windows Server 2003 so eingestellt, dass die Betriebssystempartition standardmäßig erweitert wird. • Private IP-Adresse dem Bildschirmhintergrund hinzugefügt • Private IP-Adresse wird auf dem Bildschirmhintergrund angezeigt • Logik für Wiederholversuche der Konsolenausgabe hinzugefügt • Problem bei der Com-Port-Ausnahme für die Verfügbarkeit der Metadaten behoben – bewirkte, dass EC2Config vor dem Anzeigen der Konsolenausgabe beendet wurde • Überprüfung des Aktivierungsstatus bei jedem Start – Aktivierung nach Bedarf •	

Version	Details	Datum der Veröffentlichung
	Problem bei den relativen Pfaden behoben – hervorgerufen durch die manuelle Ausführung einer Bildschirmhintergrund-Verknüpfung aus dem Startup-Ordner heraus; auf "Administrator/logs" verweisend • Problem mit der Hintergrundfarbe für Benutzer von Windows Server 2003 behoben (abgesehen vom Administrator).	

Version	Details	Datum der Veröffentlichung
2.1.2	• Konsolenzeitstempel auf UTC (Zulu) gesetzt • Anzeige eines Hyperlinks auf der Registerkarte Sysprep entfernt • Feature-Ergänzung zur dynamischen Erweiterung des Stamm-Volumes beim ersten Start von Windows 2008+ • Wenn "Set-Password" aktiviert ist, kann EC2Config automatisch das Passwort festlegen • EC2Config überprüft den Aktivierungsstatus vor dem Ausführen von Sysprep (zeigt Warnung an, falls nicht aktiviert) • Die Datei `Sysprep.xml` für Windows Server 2003 ist jetzt standardmäßig auf die Zeitzone UTC und nicht mehr auf Pacific eingestellt. • Zufällige Aktivierungsserver • Registerkarte "Drive Mapping" zu "Disk Settings" umbenannt • Benutzeroberflächenelemente "Initialize Drives" von der Registerkarte "General" auf die Registerkarte "Disk Settings" verschoben • Schaltfläche "Hilfe" verweist jetzt auf die HTML-Hilfedatei • HTML-Hilfedatei wurde mit den Änderungen aktualisiert • Hinweistext für die Zuweisungen von Laufwerkbuchstaben aktualisiert •	

Version	Details	Datum der Veröffentlichung
	InstallUpdates.ps1 zum /Scripts-Ordner hinzugefügt, um Patches zu automatisieren und eine Bereinigung vor dem Ausführen von Sysprep vorzunehmen	
2.1.0	• Desktop-Hintergrund zeigt beim ersten Anmelden (nicht beim Trennen/Wiederherstellen der Verbindung) standardmäßig Instance-Informationen an • PowerShell kann von den Benutzerdaten aus ausgeführt werden, wenn der Code mit <powershell></powershell> umschlossen wird	

Verwenden Sie EC2-Schnellstart für Ihre Windows-Instances

Wenn Sie ein Windows-Server-AMI für EC2-Schnellstart konfigurieren, erstellt Amazon EC2 wie folgt eine Reihe von vorab bereitgestellten Snapshots, die für einen schnelleren Start verwendet werden.

1. Amazon EC2 startet entsprechend Ihren Einstellungen eine Reihe temporärer t3-Instances.
2. Sobald die einzelnen temporären Instances die standardmäßigen Startschritte abschließen, erstellt Amazon EC2 jeweils einen vorab bereitgestellten Snapshot der Instance. Der Snapshot wird in Ihrem Amazon-S3-Bucket gespeichert.
3. Wenn der Snapshot fertig ist, beendet Amazon EC2 die zugehörige t3-Instance, um die Ressourcenkosten so gering wie möglich zu halten.
4. Wenn Amazon EC2 das nächste Mal eine Instance über das AMI mit aktiviertem EC2-Schnellstart startet, verwendet es einen der Snapshots, um die Startzeit erheblich zu verkürzen.

Amazon EC2 füllt die vorhandenen Snapshots automatisch auf, da es damit Instances über das AMI mit aktivierten EC2-Schnellstart startet.

Sämtliche Konten, die Zugang zu einem AMI mit aktiviertem EC2-Schnellstart haben, können von kürzeren Startzeiten profitieren. Wenn der AMI-Besitzer Ihnen Zugriff zum Starten von Instances gewährt, stammen die vorab bereitgestellten Snapshots aus dem Konto des AMI-Besitzers.

Wenn für Sie ein AMI mit EC2-Schnellstart-Unterstützung freigegeben wird, können Sie den Schnellstart für das freigegebene AMI selbst aktivieren oder deaktivieren. Wenn Sie den EC2-Schnellstart für ein freigegebenes AMI aktivieren, erstellt Amazon EC2 die vorab bereitgestellten Snapshots direkt in Ihrem Konto. Wenn die in Ihrem Konto verfügbaren Snapshots aufgebraucht sind, können Sie weiterhin Snapshots aus dem Konto des AMI-Besitzers verwenden.

> **Note**
>
> EC2-Schnellstart löscht vorab bereitgestellte Snapshots, sobald sie bei einem Start genutzt werden, um die Speicherkosten zu minimieren und eine Wiederverwendung zu verhindern. Wenn die gelöschten Snapshots jedoch einer Aufbewahrungsregel entsprechen, werden sie automatisch im Papierkorb aufbewahrt. Wir empfehlen Ihnen, den Geltungsbereich Ihrer Aufbewahrungsregeln für den Papierkorb zu überprüfen, damit dies nicht passiert. Weitere Informationen finden Sie unter Bereinigen des Papierkorbs im Amazon-EBS-Benutzerhandbuch.
> Dieses Feature ist nicht identisch mit der schnellen EBS-Snapshot-Wiederherstellung. Die schnelle EBS-Snapshot-Wiederherstellung müssen Sie explizit für jeden einzelnen Snapshot aktivieren, was mit entsprechenden Kosten verbunden ist.

Das folgende Video zeigt, wie Sie Ihr Windows-AMI für einen schnelleren Start konfigurieren. Außerdem bietet es einen kurzen Überblick über die zugehörigen Schlüsselbegriffe und deren Definitionen: EC2-Windows-Instances in AWS bis zu 65 % schneller starten.

Kosten für die Ressourcen

Es fallen keine Servicegebühren an, um Windows AMIs für EC2-Schnellstart zu konfigurieren. Die Standardpreise gelten jedoch für alle zugrundeliegenden AWS-Ressourcen, die Amazon EC2 verwendet. Weitere Informationen zu den damit verbundenen Ressourcenkosten und deren Verwaltung finden Sie unter Verwalten Sie die Kosten für die zugrunde liegenden EC2-Schnellstart-Ressourcen.

Inhalt

- Wichtige Begriffe

- Voraussetzungen für das Einrichten von EC2-Schnellstart für Windows
- Konfiguration der EC2-Schnellstart-Einstellungen für Ihr Amazon EC2 Windows Server AMI
- Windows-AMIs mit aktiviertem EC2-Schnellstart anzeigen
- Verwalten Sie die Kosten für die zugrunde liegenden EC2-Schnellstart-Ressourcen
- EC2-Schnellstart überwachen
- Serviceverknüpfte Rolle für EC2-Schnellstart
- Problembehebung für Windows EC2 Fast Launch

Wichtige Begriffe

Im Zusammenhang mit dem Feature EC2-Schnellstart werden die folgenden Schlüsselbegriffe verwendet:

Vorab bereitgestellter Snapshot

Ein Snapshot einer Instance, die über ein Windows-AMI mit aktiviertem EC2-Schnellstart gestartet wurde, die folgenden Windows-Startschritte abgeschlossen hat und je nach Bedarf neu gestartet wurde.

- Sysprep spezialisieren
- Windows Out of Box Experience (OOBE)

Wenn diese Schritte abgeschlossen sind, stoppt EC2-Schnellstart die Instance und erstellt entsprechend Ihrer Konfiguration einen Snapshot, der später für ein schnelleres Starten über das AMI verwendet wird.

Starthäufigkeit

Legt die Anzahl der vorab bereitgestellten Snapshots fest, die Amazon EC2 innerhalb des angegebenen Zeitrahmens starten kann. Wenn Sie EC2-Schnellstart für Ihr AMI aktivieren, erstellt Amazon EC2 im Hintergrund den ersten Satz von vorab bereitgestellten Snapshots. Wenn die Starthäufigkeit beispielsweise auf den Standardwert von fünf Starts pro Stunde festgelegt ist, erstellt EC2-Schnellstart eine erste Gruppe von fünf vorab bereitgestellten Snapshots.

Wenn Amazon EC2 eine Instance von einem AMI mit aktiviertem EC2-Schnellstart startet, verwendet es einen der vorab bereitgestellten Snapshots, um die Startzeit zu verkürzen. Wenn Snapshots verwendet werden, werden sie automatisch auf die mit der Startfrequenz angegebenen Anzahl aufgefüllt.

Wenn Sie eine Zunahme der Instances erwarten, die über Ihr AMI gestartet werden – zum Beispiel während eines besonderen Ereignisses – können Sie die Starthäufigkeit im Voraus erhöhen, um die zusätzlich benötigten Instances abzudecken. Wenn Ihr Startvolumen wieder normal ist, können Sie die Häufigkeit wieder nach unten anpassen.

Wenn die Zahl der Starts höher ist als erwartet, verbrauchen Sie unter Umständen alle verfügbaren vorab bereitgestellten Snapshots. Das führt nicht dazu, dass Starts fehlschlagen. Es kann jedoch dazu führen, dass einige Instances den Standardstartprozess durchlaufen, bis Snapshots wieder aufgefüllt werden können.

Anzahl der Zielressourcen

Die Anzahl der vorab bereitgestellten Snapshots, die für ein Windows-Server-AMI von Amazon EC2 mit aktiviertem EC2-Schnellstart zur Verfügung stehen sollen.

Max. Anzahl paralleler Starts

Legt fest, wie viele Instances Amazon EC2 gleichzeitig starten kann, um die vorab bereitgestellten Snapshots für EC2-Schnellstart zu erstellen. Wenn die Anzahl der Zielressourcen höher ist als die konfigurierte maximale Anzahl an parallelen Starts, startet Amazon EC2 zunächst die Anzahl an Instances, die durch die Einstellung Max. Anzahl paralleler Starts für die Erstellung der Snapshots festgelegt wurde. Wenn diese Instances den Vorgang abgeschlossen haben, erstellt Amazon EC2 den Snapshot und stoppt die Instance. Anschließend werden weitere Instances gestartet, bis die Gesamtzahl der verfügbaren Snapshots die Anzahl der Zielressourcen erreicht hat. Der Wert für Max. Anzahl paralleler Starts muss 6 oder höher sein.

Voraussetzungen für das Einrichten von EC2-Schnellstart für Windows

Stellen Sie vor Einrichtung von EC2-Schnellstart sicher, dass die folgenden Voraussetzungen für die Erstellung von Snapshots für die AMIs in Ihrem AWS-Konto erfüllt sind:

- Wenn Sie bei der Konfiguration von EC2 Fast Launch eine benutzerdefinierte Startvorlage angeben, verwendet der Service die VPC und andere Konfigurationseinstellungen, die Sie in der Startvorlage definiert haben. Weitere Informationen finden Sie unter Startvorlage beim Einrichten von EC2-Schnellstart verwenden.
- Wenn Sie keine benutzerdefinierte Startvorlage verwenden, um Ihre Einstellungen zu konfigurieren, müssen Sie die EC2FastLaunchFullAccess-Richtlinie an Ihre aktuelle IAM-Rolle anhängen, bevor Sie EC2 Fast Launch aktivieren. Der Service erstellt dann automatisch einen CloudFormation-Stack mit den folgenden Ressourcen in Ihrem AWS-Konto.

  - Eine Virtual Private Cloud (VPC)
  - Private Subnetze über mehrere Availability Zones hinweg
  - Eine Startvorlage, konfiguriert mit Instance Metadata Service Version 2 (IMDSv2)
  - Eine Sicherheitsgruppe mit keinen Regeln für ein- oder ausgehenden Datenverkehr
- Private EC2-Schnellstart-AMIs müssen die Ausführung von Benutzerdatenskripts unterstützen.
- Um EC2-Schnellstart für ein AMI zu konfigurieren, müssen Sie das AMI mit Sysprep mit der Option „Shutdown“ erstellen. Das Feature EC2-Schnellstart unterstützt derzeit keine AMIs, die über eine laufende Instance erstellt wurden.

  Informationen zum Erstllen eines AMI mit Sysprep finden Sie unter Ein Amazon-EC2-AMI mit Windows Sysprep erstellen.
- Um EC2 Fast Launch für ein verschlüsseltes AMI zu aktivieren, das einen kundenverwalteten Schlüssel für die Verschlüsselung verwendet, müssen Sie der serviceverknüpften Rolle für EC2 Fast Launch die Berechtigung zur Verwendung des CMK erteilen. Weitere Informationen finden Sie unter the section called “Zugriff auf kundenverwaltete Schlüssel”.
- Das Standardkontingent für Max. Anzahl paralleler Starts für alle AMIs in einem AWS-Konto beträgt 40 pro Region. Auf folgende Weise können Sie eine Erhöhung der Service Quotas für Ihr Konto anfordern.

  1. Öffnen Sie die Service-Quotas-Konsole unter https://console.aws.amazon.com/servicequotas/.
  2. Wählen Sie im Navigationsbereich aus AWS-Services.
  3. Geben Sie in der Suchleiste **`EC2 Fast Launch`** ein und wählen Sie das Ergebnis aus.
  4. Wählen Sie den Link Parallele Instance-Starts, um die Service-Quotas-Detailseite zu öffnen.
  5. Wählen Sie Erhöhung auf Kontoebene beantragen aus.

  Weitere Informationen finden Sie unter Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Konfiguration der EC2-Schnellstart-Einstellungen für Ihr Amazon EC2 Windows Server AMI

Sie können EC2-Schnellstart für Windows-AMIs konfigurieren, die Sie besitzen, oder für AMIs, die Sie über die AWS-Managementkonsole, API, SDKs, CloudFormation oder AWS Command Line Interface (AWS CLI) freigegeben haben. Vergewissern Sie sich vor dem Konfigurieren von EC2-Schnellstart,

dass Ihr AMI alle erforderlichen Voraussetzungen für die Erstellung der vorab bereitgestellten Snapshots erfüllt. Weitere Informationen finden Sie unter Voraussetzungen für das Einrichten von EC2-Schnellstart für Windows.

Wenn Sie den schnelleren Start für Windows-Instances aktivieren, überprüft Amazon EC2, ob Sie über die erforderlichen Berechtigungen zum Starten von Instances aus dem angegebenen AMI und der Startvorlage (falls vorhanden) verfügen, einschließlich der Berechtigungen für verschlüsselte AMIs. Um Fehler beim Instance-Start zu vermeiden, validiert der Service Ihre Berechtigungen, bevor EC2-Schnellstart aktiviert wird. Wenn Sie nicht über die erforderlichen Berechtigungen verfügen, gibt der Service einen Fehler zurück und aktiviert EC2-Schnellstart nicht.

EC2-Schnellstart ist in EC2 Image Builder integriert, sodass Sie benutzerdefinierte Images erstellen können, bei denen EC2-Schnellstart aktiviert ist. Weitere Informationen finden Sie unter Erstellen von Verteilungseinstellungen für ein Windows-AMI mit aktiviertem EC2-Schnellstart (AWS CLI) im Benutzerhandbuch von EC2 Image Builder.

EC2-Schnellstart aktivieren

Um diese Einstellungen zu ändern, stellen Sie sicher, dass Ihr AMI und die Region, in der Sie ausführen, alle erfüllen Voraussetzungen für das Einrichten von EC2-Schnellstart für Windows.

Console

So aktivieren Sie EC2 Fast Launch

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Images die Option AMIs aus.
3. Wählen Sie das zu aktualisierende AMI aus, indem Sie das Kontrollkästchen neben dem Namen aktivieren.
4. Wählen Sie im Menü Aktionen über der Liste der AMIs den Befehl Schnellstart konfigurieren. Dadurch wird die Seite Schnellstart konfigurieren geöffnet, auf der Sie die Einstellungen für EC2-Schnellstart konfigurieren.
5. Um mit vorab bereitgestellten Snapshots Instances schneller über Ihr Windows-AMI zu starten, aktivieren Sie das Kontrollkästchen Windows-Schnellstart aktivieren.
6. Wählen Sie in der Dropdownliste Set anticipated launch frequency (Voraussichtliche Starthäufigkeit festlegen) einen Wert aus, um die Anzahl der Snapshots festzulegen, die erstellt und beibehalten werden, um das erwartete Startvolumen Ihrer Instance abzudecken.

7. Wenn Sie die gewünschten Änderungen vorgenommen haben, wählen Sie Save changes (Änderungen speichern).

> **Note**
>
> Wenn Sie eine Startvorlage verwenden müssen, um eine VPC anzugeben oder um Metadateneinstellungen für IMDSv2 zu konfigurieren, siehe Startvorlage beim Einrichten von EC2-Schnellstart verwenden.

AWS CLI

So aktivieren Sie EC2 Fast Launch

Verwenden Sie den Befehl enable-fast-launch, um EC2 Fast Launch für das angegebene AMI zu aktivieren und sechs parallele Instances für die Vorabbereitstellung zu starten.

```
aws ec2 enable-fast-launch \
    --image-id ami-0abcdef1234567890  \
    --max-parallel-launches 6 \
    --resource-type snapshot
```

Es folgt eine Beispielausgabe.

```
{
 "ImageId": "ami-0abcdef1234567890",
 "ResourceType": "snapshot",
 "SnapshotConfiguration": {
     "TargetResourceCount": 10
 },
 "LaunchTemplate": {},
 "MaxParallelLaunches": 6,
 "OwnerId": "0123456789123",
 "State": "enabling",
 "StateTransitionReason": "Client.UserInitiated",
 "StateTransitionTime": "2022-01-27T22:16:03.199000+00:00"
}
```

PowerShell

So aktivieren Sie EC2 Fast Launch

Verwenden Sie das cmdlet Enable-EC2FastLaunch, um EC2 Fast Launch für das angegebene AMI zu aktivieren und sechs parallele Instances für die Vorabbereitstellung zu starten.

```
Enable-EC2FastLaunch `
 -ImageId ami-0abcdef1234567890 `
 -MaxParallelLaunch 6 `
 -Region us-west-2 `
 -ResourceType snapshot
```

Es folgt eine Beispielausgabe.

```
ImageId               : ami-0abcdef1234567890
 LaunchTemplate        :
 MaxParallelLaunches   : 6
 OwnerId               : 0123456789123
 ResourceType          : snapshot
 SnapshotConfiguration : Amazon.EC2.Model.FastLaunchSnapshotConfigurationResponse
 State                 : enabling
 StateTransitionReason : Client.UserInitiated
 StateTransitionTime   : 2/25/2022 12:24:11 PM
```

EC2-Schnellstart deaktivieren

Um diese Einstellungen zu ändern, stellen Sie sicher, dass Ihr AMI und die Region, in der Sie ausführen, alle erfüllen Voraussetzungen für das Einrichten von EC2-Schnellstart für Windows.

Console

So deaktivieren Sie EC2 Fast Launch

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Images die Option AMIs aus.
3. Wählen Sie das zu aktualisierende AMI aus, indem Sie das Kontrollkästchen neben dem Namen aktivieren.
4. Wählen Sie im Menü Aktionen über der Liste der AMIs den Befehl Schnellstart konfigurieren. Dadurch wird die Seite Schnellstart konfigurieren geöffnet, auf der Sie die Einstellungen für EC2-Schnellstart konfigurieren.

5. Deaktivieren Sie das Kontrollkästchen Schnellstart für Windows aktivieren, um den EC2-Schnellstart zu deaktivieren und vorab bereitgestellte Snapshots zu entfernen. Dies führt dazu, dass das AMI in Zukunft den Standardstartprozess für jede Instance verwendet.

   > **Note**
   >
   > Wenn Sie die Windows-Image-Optimierung deaktivieren, werden alle vorhandenen vorab bereitgestellten Snapshots automatisch gelöscht. Dieser Schritt muss abgeschlossen sein, bevor Sie das Feature erneut verwenden können.

6. Wenn Sie die gewünschten Änderungen vorgenommen haben, wählen Sie Save changes (Änderungen speichern).

AWS CLI

So deaktivieren Sie EC2 Fast Launch

Verwenden Sie den Befehl disable-fast-launch, um EC2 Fast Launch für das angegebene AMI zu deaktivieren und vorhandene vorab bereitgestellte Snapshots zu bereinigen.

```
aws ec2 disable-fast-launch --image-id ami-01234567890abcedf
```

Es folgt eine Beispielausgabe.

```
{
    "ImageId": "ami-01234567890abcedf",
    "ResourceType": "snapshot",
    "SnapshotConfiguration": {},
    "LaunchTemplate": {
        "LaunchTemplateId": "lt-01234567890abcedf",
        "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
        "Version": "1"
    },
    "MaxParallelLaunches": 6,
    "OwnerId": "0123456789123",
    "State": "disabling",
    "StateTransitionReason": "Client.UserInitiated",
    "StateTransitionTime": "2022-01-27T22:47:29.265000+00:00"
}
```

PowerShell

So deaktivieren Sie EC2 Fast Launch

Verwenden Sie das cmdlet Disable-EC2FastLaunch, um EC2 Fast Launch für das angegebene AMI zu deaktivieren und vorhandene vorab bereitgestellte Snapshots zu bereinigen.

```
Disable-EC2FastLaunch -ImageId ami-0abcdef1234567890
```

Es folgt eine Beispielausgabe.

```
ImageId               : ami-0abcdef1234567890
 LaunchTemplate        :
 Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
 MaxParallelLaunches   : 6
 OwnerId               : 0123456789123
 ResourceType          : snapshot
 SnapshotConfiguration :
 State                 : disabling
 StateTransitionReason : Client.UserInitiated
 StateTransitionTime   : 2/25/2022 1:10:08 PM
```

Startvorlage beim Einrichten von EC2-Schnellstart verwenden

Mit einer Startvorlage können Sie eine Reihe von Startparametern konfigurieren, die Amazon EC2 bei jedem Start einer Instance aus dieser Vorlage verwendet. Sie können Dinge wie ein AMI angeben, das für Ihr Basis-Image, Instance-Typen, Speicher, Netzwerkeinstellungen und mehr verwendet werden soll.

Startvorlagen sind optional, mit Ausnahme der folgenden Sonderfälle, in denen Sie eine Startvorlage für Ihr Windows-AMI verwenden müssen, wenn Sie einen schnelleren Start konfigurieren:

- Sie müssen eine Startvorlage verwenden, um eine vorhandene VPC für Ihr Windows-AMI anzugeben. Dies gilt nicht, wenn Sie die Standard-VPC für Ihr AWS-Konto verwenden.
- Wenn Ihr Konto eine Richtlinie enthält, die IMDSv2 für Amazon-EC2-Instances erzwingt, müssen Sie eine Startvorlage erstellen, in der die Metadatenkonfiguration zur Erzwingung von IMDSv2 angegeben ist.

Verwenden Sie die Startvorlage, die Ihre Metadatenkonfiguration enthält, von der EC2-Konsole aus oder wenn Sie den Befehl enable-fast-launch in der Datei AWS CLI ausführen oder die API-Aktion EnableFastLaunch aufrufen.

Amazon-EC2-Schnellstart unterstützt die folgende Konfiguration nicht, wenn Sie eine Startvorlage verwenden. Wenn Sie eine Startvorlage für EC2-Schnellstart verwenden, dürfen Sie Folgendes nicht angeben:

- Benutzerdatenskripts
- Termination protection
- Deaktivierte Metadaten
- Spot-Option
- Verhalten beim Herunterfahren, das die Instance beendet
- Ressourcen-Tags für Netzwerkschnittstellen-, Elastic Graphic- oder Spot-Instance-Anfragen

Eine VPC angeben

Schritt 1: Eine Startvorlage erstellen

Erstellen Sie eine Startvorlage, die die folgenden Details für Ihre Windows-Instances angibt:

- Das VPC-Subnetz.
- Einen Instance-Typ von `t3.xlarge`.

Weitere Informationen finden Sie unter Erstellen Sie eine EC2 Amazon-Startvorlage.

Schritt 2: Angeben der Startvorlage für Ihr EC2-Schnellstart-AMI

Console

So geben Sie die Startvorlage für EC2 Fast Launch an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Images die Option AMIs aus.
3. Wählen Sie das zu aktualisierende AMI aus, indem Sie das Kontrollkästchen neben dem Namen aktivieren.

4. Wählen Sie im Menü Aktionen über der Liste der AMIs den Befehl Schnellstart konfigurieren. Dadurch wird die Seite Schnellstart konfigurieren geöffnet, auf der Sie die Einstellungen für EC2-Schnellstart konfigurieren.
5. Die Launch template (Startvorlage) führt eine gefilterte Suche durch, bei der Startvorlagen in Ihrem Konto in der aktuellen Region gefunden werden, die mit dem von Ihnen eingegebenen Text übereinstimmen. Geben Sie den Namen oder die ID der Startvorlage ganz oder teilweise in das Feld ein, um eine Liste mit übereinstimmenden Startvorlagen anzuzeigen. Wenn Sie beispielsweise `fast` in der Box eingeben, findet Amazon EC2 alle Startvorlagen in Ihrem Konto in der aktuellen Region, die „schnell“ im Namen haben.

   Um eine neue Startvorlage zu erstellen, können Sie Create launch template (Startvorlage erstellen) wählen.
6. Wenn Sie eine Startvorlage auswählen, zeigt Amazon EC2 die Standardversion für diese Vorlage im Feld Source template version (Quellvorlagenversion) an. Um eine andere Version anzugeben, markieren Sie die Standardversion, um sie zu ersetzen, und geben Sie die gewünschte Versionsnummer in das Feld ein.
7. Wenn Sie die gewünschten Änderungen vorgenommen haben, wählen Sie Save changes (Änderungen speichern).

AWS CLI

So geben Sie die Startvorlage für EC2 Fast Launch an

Verwenden Sie den Befehl enable-fast-launch mit der Option `--launch-template` und geben Sie entweder den Namen oder die ID der Startvorlage an.

```
--launch-template LaunchTemplateName=my-launch-template
```

PowerShell

So geben Sie die Startvorlage für EC2 Fast Launch an

Verwenden Sie das cmdlet Enable-EC2FastLaunch mit dem Parameter `-LaunchTemplate_LaunchTemplateId` oder `-LaunchTemplate_LaunchTemplateName`.

```
-LaunchTemplate_LaunchTemplateName my-launch-template
```

Weitere Informationen über EC2-Startvorlagen finden Sie unter Instance-Startparameter in EC2 Amazon-Startvorlagen speichern.

Windows-AMIs mit aktiviertem EC2-Schnellstart anzeigen

Mit dem Befehl describe-fast-launch-images in der AWS CLI oder dem Cmdlet Get-EC2FastLaunchImage von Tools für PowerShell können Sie Details zu Windows-AMIs abrufen, bei denen der EC2-Schnellstart aktiviert ist.

Amazon EC2 bietet die folgenden Details für jedes Windows-AMI in den Ergebnissen:

- Die Image-ID für ein AMI mit aktiviertem EC2-Schnellstart.
- Der Ressourcentyp, der für die Vorabbereitstellung des zugeordneten Windows-AMI verwendet wird. Unterstützter Wert: `snapshot`.
- Die Snapshot-Konfiguration, also eine Gruppe von Parametern, die die Vorabbereitstellung für das zugehörige Windows-AMI mit Snapshots konfigurieren.
- Startvorlageninformationen, einschließlich der ID, des Namens und der Version der Startvorlage, die das zugeordnete AMI verwendet, wenn es Window-Instances aus vorab bereitgestellten Snapshots startet.
- Die maximale Anzahl an Instances, die, zum Erstellen von Ressourcen, gleichzeitig gestartet werden können.
- Das ist die Besitzer-ID für das zugeordnete AMI. Für AMIs, die für Sie freigegeben wurden, wurde dieses Feld nicht ausgefüllt.
- Der aktuelle Status von EC2-Schnellstart für das zugehörige AMI. Zu den unterstützten Werten gehören: `enabling | enabling-failed | enabled | enabled-failed | disabling | disabling-failed`.

  > **Note**
  >
  > Sie können den aktuellen Status auch auf der Seite Manage image optimization (Image-Optimierung verwalten) in der EC2-Konsole als Image optimization state (Image-Optimierungsstatus) anzeigen.

- Der Grund dafür, dass EC2-Schnellstart für das zugehörige AMI in den aktuellen Zustand geändert wurde.
- Der Zeitpunkt, zu dem EC2-Schnellstart für das zugehörige AMI in den aktuellen Zustand übergegangen ist.

AWS CLI

So suchen Sie AMIs, die für EC2 Fast Launch konfiguriert sind

Verwenden Sie den Befehl describe-fast-launch-images, um die Details für jedes der AMIs im Konto zu beschreiben, die für EC2 Fast Launch konfiguriert sind. In diesem Beispiel ist nur ein AMI im Konto für EC2-Schnellstart konfiguriert.

```
aws ec2 describe-fast-launch-images
```

Es folgt eine Beispielausgabe.

```
{
    "FastLaunchImages": [
        {
            "ImageId": "ami-01234567890abcedf",
            "ResourceType": "snapshot",
            "SnapshotConfiguration": {},
            "LaunchTemplate": {
                "LaunchTemplateId": "lt-01234567890abcedf",
                "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
                "Version": "1"
            },
            "MaxParallelLaunches": 6,
            "OwnerId": "0123456789123",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated",
            "StateTransitionTime": "2022-01-27T22:20:06.552000+00:00"
        }
    ]
}
```

PowerShell

So suchen Sie AMIs, die für EC2 Fast Launch konfiguriert sind

Verwenden Sie das cmdlet Get-EC2FastLaunchImage, um die Details für alle AMIs im Konto zu beschreiben, die für EC2 Fast Launch konfiguriert sind. In diesem Beispiel ist nur ein AMI im Konto für EC2-Schnellstart konfiguriert.

```
Get-EC2FastLaunchImage -ImageId ami-0abcdef1234567890
```

Es folgt eine Beispielausgabe.

```
ImageId               : ami-0abcdef1234567890
LaunchTemplate        :
 Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
MaxParallelLaunches   : 6
OwnerId               : 012345678912
ResourceType          : snapshot
SnapshotConfiguration :
State                 : enabled
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 12:54:43 PM
```

Verwalten Sie die Kosten für die zugrunde liegenden EC2-Schnellstart-Ressourcen

Es fallen keine Servicegebühren an, um Windows AMIs für EC2-Schnellstart zu konfigurieren. Wenn Sie jedoch EC2-Schnellstart für ein Windows-AMI von Amazon EC2 aktivieren, gelten die Standardpreise für die zugrundeliegenden AWS-Ressourcen, mit deren Hilfe Amazon EC2 die vorab bereitgestellten Snapshots vorbereitet und speichert. Sie können Kostenzuweisungs-Tags konfigurieren, um die Kosten im Zusammenhang mit EC2-Schnellstart-Ressourcen zu verfolgen und zu verwalten. Weitere Informationen zum Konfigurieren von Kostenzuweisungs-Tags finden Sie unter Kosten für EC2-Schnellstart auf Ihrer Rechnung verfolgen.

Das folgende Beispiel zeigt, wie die Kosten für EC2-Schnellstart-Snapshots zugeteilt werden könnten.

Beispielszenario: Das AtoZ-Beispielunternehmen hat ein Windows-AMI mit einem 50-GiB-EBS-Root-Volume. Es wird EC2-Schnellstart für ein AMI aktiviert und die Anzahl der Zielressourcen wird auf fünf gesetzt. Im Lauf eines Monats kostet die Nutzung von EC2-Schnellstart für das AMI rund 5,00 USD. Die Kostenaufschlüsselung ist wie folgt:

1. Wenn Atoz Example EC2-Schnellstart aktiviert, startet Amazon EC2 fünf kleine Instances. Jede Instance läuft durch die Startschritte von Sysprep und OOBE Windows und wird bei Bedarf neu gestartet. Dies dauert für jede Instance mehrere Minuten (die Zeit kann variieren, je nachdem, wie ausgelastet diese Region oder Availability Zone (AZ) ist, und wie groß das AMI ist).

   Kosten

   - Instance-Laufzeitkosten (oder ggf. minimale Laufzeit): fünf Instances
   - Volumenkosten: fünf EBS Root-Volumes

2. Wenn der Vorab-Bereitstellungsprozess abgeschlossen ist, erstellt Amazon EC2 einen Snapshot der Instance und speichert diesen in Amazon S3. Snapshots werden in der Regel 4-8 Stunden lang gespeichert, bevor sie bei einem Start verbraucht werden. In diesem Fall betragen die Kosten etwa 0,02 bis 0,05 USD pro Snapshot.

   Kosten

   - Snapshot-Speicher (Amazon S3): Fünf Snapshots

3. Nachdem Amazon EC2 den Snapshot erstellt hat, stoppt es die Instance. Zu diesem Zeitpunkt fallen für die Instance keine Kosten mehr an. Die EBS-Volumenkosten fallen jedoch weiterhin an.

   Kosten

   - EBS-Volumes: Die Kosten für die zugehörigen EBS Root-Volumes laufen weiter.

> **Note**
>
> Die hier angegebenen Kosten dienen nur zu Demonstrationszwecken. Ihre Kosten variieren je nach AMI-Konfiguration und Preisplan.

Kosten für EC2-Schnellstart auf Ihrer Rechnung verfolgen

Kostenverteilungs-Tags können Ihnen bei der Organisation Ihrer AWS-Fakturierung helfen, um die Kosten für EC2-Schnellstart zu berücksichtigen. Sie können das folgende Tag verwenden, das Amazon EC2 den Ressourcen hinzufügt, die es erstellt, wenn es vorab bereitgestellte Snapshots für EC2-Schnellstart vorbereitet und speichert:

Tag-Schlüssel: `CreatedBy`, Wert: `EC2 Fast Launch`

Nachdem Sie das Tag in der Konsole für Fakturierung und Kostenmanagement aktiviert und Ihren detaillierten Rechnungsbericht eingerichtet haben, erscheint die Spalte `user:CreatedBy` im Bericht. Die Spalte enthält Werte aus allen Services. Wenn Sie jedoch die CSV-Datei herunterladen, können Sie die Daten in eine Tabellenkalkulation importieren und nach `EC2 Fast Launch` im Wert filtern. Diese Informationen werden auch in den AWS Cost and Usage Report angezeigt, wenn das Tag aktiviert ist.

Schritt 1: Benutzerdefinierte Kostenzuordnungs-Tags aktivieren

Um Ressourcen-Tags in Ihre Kostenberichte aufzunehmen, müssen Sie sie zuerst in der Konsole für Fakturierung und Kostenmanagement aktivieren. Weitere Informationen finden Sie unter Benutzerdefinierte Kostenzuordnungs-Tags aktivieren im AWS Fakturierung und Kostenmanagement-Benutzerhandbuch.

> **Note**
>
> Die Aktivierung kann bis zu 24 Stunden dauern.

Schritt 2: Kostenbericht einrichten

Wenn Sie bereits einen Kostenbericht eingerichtet haben, wird bei der nächsten Ausführung des Berichts nach Abschluss der Aktivierung eine Spalte für Ihr Tag angezeigt. Um Kostenberichte zum ersten Mal zu erstellen, wählen Sie eine der folgenden Optionen aus.

- Weitere Informationen finden Sie unter Einrichten Ihres monatlichen Kostenzuordnungsberichts im AWS Fakturierung und Kostenmanagement-Benutzerhandbuch.
- Weitere Informationen finden Sie im Benutzerhandbuch zu AWS Cost and Usage Reporten unter Erstellen von Kosten- und Nutzungsberichten.

> **Note**
>
> Es kann bis zu 24 Stunden dauern, bis AWS Berichte an Ihren S3-Bucket sendet.

Sie können EC2-Schnellstart für Windows-AMIs, die Ihnen gehören, oder für AMIs, die für Sie freigegeben wurden, über die Amazon-EC2-Konsole, per API, mithilfe von SDKs, per CloudFormation oder mithilfe von ec2-Befehlen über die AWS CLI konfigurieren. In den folgenden Abschnitten werden Konfigurationsschritte für die Amazon-EC2-Konsole und behandelt AWS CLI.

Außerdem können Sie Windows-AMIs, die für EC2-Schnellstart konfiguriert sind, mit EC2 Image Builder erstellen. Weitere Informationen finden Sie unter Erstellen von Verteilungseinstellungen für ein Windows-AMI mit aktiviertem EC2-Schnellstart (AWS CLI).

EC2-Schnellstart überwachen

In diesem Abschnitt wird beschrieben, wie Sie die Windows-Server-AMIs von Amazon EC2 in Ihrem Konto überwachen, für die EC2-Schnellstart aktiviert ist.

Statusänderungen von EC2-Schnellstart mit EventBridge überwachen

Wenn sich der Status eines AMI mit aktiviertem EC2-Schnellstart ändert, generiert Amazon EC2 ein `EC2 Fast Launch State-change Notification`-Ereignis. Dann sendet Amazon EC2 das Zustandsänderungsereignis an Amazon EventBridge (früher bekannt als Amazon CloudWatch Events).

Sie können EventBridge-Regeln erstellen, die als Reaktion auf das Zustandsänderungsereignis eine oder mehrere Aktionen auslösen. Sie können zum Beispiel eine EventBridge-Regel erstellen, die erkennt, wenn EC2-Schnellstart aktiviert ist, und die folgenden Aktionen durchführt:

- Sendet eine Nachricht an ein Amazon-SNS-Thema, um die Abonnenten zu benachrichtigen.
- Ruft eine Lambda-Funktion auf, die eine Aktion ausführt.
- Sendet die Zustandsänderungsdaten zur Analytik an Amazon Kinesis Data Firehose.

Weitere Informationen finden Sie unter Erstellen von Erstellen von Amazon-EventBridge-Regeln, die auf Ereignisse reagieren im Amazon-EventBridge-Benutzerhandbuch.

Statusänderungsereignisse

Das Feature EC2-Schnellstart sendet JSON-formatierte Statusänderungsereignisse auf einer Bester-Aufwand-Basis. Amazon EC2 sendet die Ereignisse nahezu in Echtzeit an EventBridge. In diesem Abschnitt werden die Ereignisfelder beschrieben und ein Beispiel für das Ereignisformat gezeigt.

`EC2 Fast Launch State-change Notification`

imageId

Identifiziert das AMI mit der Statusänderung von EC2-Schnellstart.

resourceType

Der Ressourcentyp, der für die Vorabbereitstellung verwendet werden soll. Unterstützter Wert: `snapshot`. Der Standardwert ist `snapshot`.

state

Der aktuelle Status des Features EC2-Schnellstart für das angegebene AMI. Gültige Werte sind unter anderem:

- Aktivieren – Sie haben das Feature EC2-Schnellstart für das AMI aktiviert, und Amazon EC2 hat damit begonnen, Snapshots für den Vorabbereitstellungsprozess zu erstellen.

- Aktivieren fehlgeschlagen – Es ist ein Fehler aufgetreten, der dazu geführt hat, dass der Vorabbereitstellungsprozess fehlschlug, als Sie das Feature EC2-Schnellstart für ein AMI zum ersten Mal aktivierten. Dies kann jederzeit während des Vorabbereitstellungsprozesses passieren.
- Aktiviert – Das Feature EC2-Schnellstart ist aktiviert. Der Status wechselt zu `enabled`, sobald Amazon EC2 den ersten vorab bereitgestellten Snapshot für ein neu aktiviertes EC2-Schnellstart-AMI erstellt. Wenn das AMI bereits aktiviert war und erneut die Vorabbereitstellung durchläuft, erfolgt die Statusänderung sofort.
- enabled-failed – Dieser Status gilt nur, wenn dies nicht das erste Mal ist, dass Ihr EC2-Schnellstart-AMI den Vorabbereitstellungsprozess durchläuft. Dies kann passieren, wenn das Feature EC2-Schnellstart deaktiviert und später wieder aktiviert wird, oder wenn eine Konfigurationsänderung oder ein anderer Fehler auftritt, nachdem die Vorabbereitstellung zum ersten Mal abgeschlossen wurde.
- deaktivieren – Der AMI-Besitzer hat das Feature EC2-Schnellstart des AMI deaktiviert und Amazon EC2 hat den Bereinigungsprozess gestartet.
- deaktiviert – Das Feature EC2-Schnellstart ist deaktiviert. Der Status wechselt zu `disabled`, sobald Amazon EC2 den Bereinigungsprozess abgeschlossen hat.
- deaktivieren fehlgeschlagen – Es ist ein Fehler aufgetreten, der dazu geführt hat, dass der Bereinigungsprozess fehlschlug. Das bedeutet, dass einige vorab bereitgestellte Snapshots möglicherweise noch im Konto verbleiben.

stateTransitionReason

Der Grund, warum Status des EC2-Schnellstart-AMIs geändert wurde.

> **Note**
>
> Alle Felder in dieser Ereignisnachricht sind erforderlich.

Das folgende Beispiel zeigt ein neu aktiviertes EC2-Schnellstart-AMI, das die erste Instance gestartet hat, um den Vorabbereitstellungsprozess zu starten. Zu diesem Zeitpunkt ist der Status `enabling`. Nachdem Amazon EC2 den ersten vorab bereitgestellten Snapshot erstellt hat, ändert sich der Status zu `enabled`.

```
{
 "version": "0",
```

```
 "id": "01234567-0123-0123-0123-012345678901",
 "detail-type": "EC2 Fast Launch State-change Notification",
 "source": "aws.ec2",
 "account": "123456789012",
 "time": "2022-08-31T20:30:12Z",
 "region": "us-east-1",
 "resources": [
  "arn:aws:ec2:us-east-1:123456789012:image/ami-123456789012"
 ],
 "detail": {
  "imageId": "ami-123456789012",
  "resourceType": "snapshot",
  "state": "enabling",
  "stateTransitionReason": "Client.UserInitiated"
 }
}
```

Metriken zum EC2-Schnellstart mit CloudWatch überwachen

Amazon-EC2-AMIs mit aktiviertem EC2-Schnellstart senden Metriken an Amazon CloudWatch. Mithilfe der AWS-Managementkonsole, der AWS CLI oder einer API können Sie die Metriken auflisten, die EC2-Schnellstart an CloudWatch sendet. Der Namespace `AWS/EC2` enthält die folgenden Metriken zum EC2-Schnellstart:

Metrik	Beschreibung
NumberOfAvailableFastLaunchSnapshots	Die Anzahl der vorab bereitgestellten Snapshots, die pro AMI mit aktiviertem EC2-Schnellstart verfügbar sind.
NumberOfInstancesFastLaunched	Die Anzahl der Instances pro AMI mit aktiviert em EC2-Schnellstart, die über vorab bereitges tellte Snapshots gestartet wurden.
NumberOfInstancesNotFastLaunched	Die Anzahl der Instances pro AMI mit aktiviert em EC2-Schnellstart, die zu einem Kaltstart führten, weil zum Startzeitpunkt keine vorab bereitgestellten Snapshots verfügbar waren.
FastLaunchSnapshotUsedToRefillStartTime	Der Zeitstempel, als Amazon EC2 ein neues Image über ein EC2-Schnellstart-fähiges AMI

Metrik	Beschreibung
	gestartet hat, um einen weiteren Snapshot zu erstellen, nachdem ein bestehender Snapshot verwendet wurde.
FastLaunchSnapshotCreationTime	Misst die Zeit, die Amazon EC2 benötigt hat, um eine Instance zu starten und einen Snapshot für ein AMI mit aktiviertem EC2-Schnellstart zu erstellen.

Serviceverknüpfte Rolle für EC2-Schnellstart

Amazon EC2 nutzt serviceverknüpfte Rollen für die Berechtigungen, die für den Aufruf anderer AWS-Services in Ihrem Namen benötigt werden. Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit AWS-Service verknüpft ist. Serviceverknüpfte Rollen bieten eine sichere Möglichkeit, um Berechtigungen an AWS-Services zu delegieren, da nur der verknüpfte Service eine serviceverknüpfte Rolle annehmen kann. Weitere Informationen zur Verwendung von IAM-Rollen – einschließlich serviceverknüpfter Rollen – durch Amazon EC2 finden Sie unter IAM-Rollen für Amazon EC2.

Amazon EC2 verwendet die serviceverknüpfte Rolle namens AWSServiceRoleForEC2FastLaunch, um eine Reihe von vorab bereitgestellten Snapshots zu erstellen und zu verwalten, die die Zeit für den Start von Instances über Ihr Windows-AMI reduzieren.

Berechtigungen von AWSServiceRoleForEC2FastLaunch

Die serviceverknüpfte Rolle AWSServiceRoleForEC2FastLaunch vertraut darauf, dass der folgende Service die Rolle annimmt:

- `ec2fastlaunch.amazonaws.com`

Amazon EC2 verwendet die verwaltete Richtlinie EC2FastLaunchServiceRolePolicy, um die folgenden Aktionen auszuführen:

- AWS CloudFormation – Erlaubt EC2 Fast Launch, eine Beschreibung der zugeordenten CloudFormation-Stacks abzurufen.

- Amazon CloudWatch – Veröffentlichen von Metrikdaten, die EC2 Fast Launch zugeordnet sind, im Amazon-EC2-Namespace.
- Amazon EC2 – EC2 Fast Launch erhält Zugriff, um die folgenden Aktionen auszuführen:
  - Starten von Instances über ein Windows-Server-AMI von Amazon EC2 mit aktiviertem EC2 Fast Launch, um Bereitstellungsschritte durchzuführen. Geben Sie zusätzlich ein Ressourcenmuster an, das `ec2:RunInstances` für ein AMI ermöglicht, das License Manager zugeordnet ist.
  - Anhalten und Beenden einer Instance, die von EC2 Fast Launch gestartet wurde, nachdem sie den vorab bereitgestellten Snapshot erstellt hat.
  - Beschreiben von Image- und Instance-Typ-Ressourcen, die zum Starten von Instances über ein Windows-Server-AMI von Amazon EC2 mit aktiviertem EC2 Fast Launch dienen, und zum Erstellen von Snapshots aus diesen.
  - Beschreiben Sie Ressourcen für Startvorlagen und starten Sie Instances anhand einer Startvorlage.
  - Beschreiben Sie Instances, Instance-Attribute und Instance-Status, Volumes und Volume-Attribute.
  - Beschreiben Sie Netzwerkschnittstellen.
  - Löschen von Ressourcen, die EC2 Fast Launch erstellt hat, einschließlich Snapshots, Startvorlagen, Volumes und Netzwerkschnittstellen.
  - Markieren Sie Ressourcen, die EC2 Fast Launch für den Start und die Vorabbereitstellung von Windows-Instances erstellt, und erstellen Sie Snapshots, die für den letzten Startvorgang verwendet werden.
- Amazon EventBridge – Beinhaltet Zugriff zum Erstellen von EventBridge-Ereignisregeln und zum Abrufen von Details zu den erstellten Regeln oder zum Löschen von Regeln. EC2 Fast Launch kann auch eine Liste von Zielservices abrufen, die Ereignisse von EC2 Fast Launch empfangen, die auf der Grundlage von Ereignisregeln weitergeleitet werden, und Zielservices zu den erstellten Ereignisregeln hinzufügen oder aus diesen entfernen.
- IAM – Erlaubt EC2 Fast Launch das Erstellen der serviceverknüpften `EC2FastLaunchServiceRolePolicy`-Rolle, das Abrufen und Verwenden von Instance-Profilen, deren Name `ec2fastlaunch` enthält, und das Starten von Instances in Ihrem Namen unter Verwendung des Instance-Profils aus Ihrer Startvorlage
- AWS KMS – Beinhaltet Zugriff zum Erstellen von Erteilungen und zum Auflisten von Erteilungen, die von EC2 Fast Launch erstellt wurden und außer Betrieb genommen werden können. Erteilt außerdem den Zugriff zum Beschreiben und Verwenden von Schlüsseln zum Verschlüsseln oder

Entschlüsseln von Volumes, die an Instances angehängt sind, die von EC2 Fast Launch erstellt werden, und zur Generierung von Datenschlüsseln, die kein Klartext sind.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter EC2FastLaunchServiceRolePolicy in der Referenz zu von AWS verwalteten Richtlinien.

Weitere Informationen zur Verwendung verwalteter Richtlinien für Amazon EC2 finden Sie unter AWS verwaltete Richtlinien für Amazon EC2.

Erstellen einer serviceverknüpften Rolle

Sie müssen diese serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie mit der Verwendung von EC2-Schnellstart für Ihr AMI beginnen, erstellt Amazon EC2 die serviceverknüpfte Rolle für Sie, sofern sie noch nicht vorhanden ist.

Wenn die serviceverknüpfte Rolle aus Ihrem Konto gelöscht wird, können Sie EC2-Schnellstart für ein anderes Windows-AMI aktivieren, um die Rolle in Ihrem Konto neu zu erstellen. Alternativ können Sie EC2-Schnellstart für Ihr aktuelles AMI deaktivieren und dann erneut aktivieren. Das Deaktivieren des Features führt jedoch dazu, dass das AMI den Standardstartprozess für alle neuen Instances verwendet, während Amazon EC2 alle vorab bereitgestellten Snapshots entfernt. Nachdem alle vorab bereitgestellten Snapshots entfernt wurden, können Sie die Verwendung von EC2-Schnellstart für Ihr AMI erneut aktivieren.

Zugriff auf kundenverwaltete Schlüssel

Um EC2 Fast Launch für ein verschlüsseltes AMI zu aktivieren, das einen kundenverwalteten Schlüssel für die Verschlüsselung verwendet, müssen Sie der AWSServiceRoleForEC2FastLaunch-Rolle die Berechtigung zur Verwendung des CMK erteilen. Rufen Sie dazu den Befehl create-grant auf. Geben Sie für `--grantee-principal` den ARN für die AWSServiceRoleForEC2FastLaunch-Rolle in Ihrem Konto an. Legen Sie für `--operations` die Option `CreateGrant` fest.

```
aws kms create-grant \
    --key-id arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2FastLaunch \
    --operations CreateGrant
```

Bearbeiten einer serviceverknüpften Rolle

Amazon EC2 verhindert die Bearbeitung der serviceverknüpften Rolle AWSServiceRoleForEC2FastLaunch. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen Sie eine serviceverknüpfte Rolle

Sie können eine serviceverknüpfte Rolle nur löschen, nachdem Sie alle zugehörigen Ressourcen gelöscht haben. Das schützt die Amazon-EC2-Ressourcen, die mit Ihrem Windows-Server-AMI von Amazon EC2 mit aktiviertem EC2-Schnellstart verknüpft sind, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entfernen können.

Verwenden Sie die IAM-Konsole, die AWS CLI oder die AWS-API, um die serviceverknüpfte Rolle AWSServiceRoleForEC2FastLaunch zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen

Amazon EC2 unterstützt die serviceverknüpfte Rolle von EC2-Schnellstart in allen Regionen, in denen der Amazon-EC2-Service verfügbar ist.

Problembehebung für Windows EC2 Fast Launch

Fehlerbehebungsszenarien

Die folgenden Szenarien können Ihnen helfen, häufige Probleme zu diagnostizieren und zu beheben, die beim Versuch auftreten könnten, EC2 Fast Launch zu aktivieren.

Die Instance für die Snapshot-Erstellung konnte nicht angehalten werden

Beschreibung

Wenn Sie den EC2 Fast Launch aktivieren, startet der Service eine Reihe von Instances, die zum Erstellen der vorab bereitgestellten Snapshots verwendet werden. Jede Instance hat 30 Minuten Zeit, um den Vorgang abzuschließen. Wenn eine der Instances erfolgreich abgeschlossen wurde, setzt der Service den Status von Fast Launch für das AMI auf `Enabled`. Wenn eine Instance den Prozess jedoch nicht in der vorgesehenen Zeit abschließt und keine der anderen Instances den Prozess

abgeschlossen hat, beendet der Service alle Instances und setzt den Status von Fast Launch für das AMI auf `enabling_failed` und den Grund für den Status auf den folgenden Wert:

```
Unable to stop instance ID=i-1234567890abcdef0 for snapshot creation.
```

Ursache

In den meisten Fällen wird dies dadurch verursacht, dass versucht wird, EC2 Fast Launch für ein Windows-AMI zu aktivieren, das aus einer laufenden Instance erstellt wurde, oder für ein AMI, das nicht alle Voraussetzungen für das Einrichten von EC2-Schnellstart erfüllt.

Lösung

Stellen Sie sicher, dass das von Ihnen verwendete AMI allen Voraussetzungen für das Einrichten von EC2-Schnellstart entspricht.

Um EC2-Schnellstart für ein AMI zu konfigurieren, müssen Sie das AMI mit Sysprep mit der Option „Shutdown“ erstellen. Weitere Informationen finden Sie unter Ein Amazon-EC2-AMI mit Windows Sysprep erstellen.

Sie haben Ihr VPC-Limit erreicht

Beschreibung

Wenn Sie keine Startvorlage verwenden, um eine vorhandene VPC anzugeben, und keine Standard-VPC für Ihr Konto definiert haben, erstellt der Service automatisch einen CloudFormation-Stack, der eine VPC und andere Ressourcen enthält, wie unter Voraussetzungen für das Einrichten von EC2-Schnellstart beschrieben.

Ursache

Sie haben die maximale Anzahl von VPCs erreicht, die in Ihrem AWS-Konto für die Region zulässig sind, und Sie haben keine bestehende VPC für die Verwendung von EC2 Fast Launch angegeben. Dies führt dazu, dass der Vorgang fehlschlägt.

Lösung

Sie können das Problem mit einer der folgenden Optionen beheben:

- Sie können eine Kontingenterhöhung beantragen.
- Sie können eine Startvorlage bereitstellen, die eine vorhandene VPC angibt.

Gehen Sie wie folgt vor, um eine Erhöhung der Anzahl der VPCs zu beantragen, die Ihr Konto pro Region definieren kann:

1. Öffnen Sie die Service-Quotas-Konsole unter https://console.aws.amazon.com/servicequotas/.
2. Wählen Sie im Dashboard der Service-Konsole die Option Amazon Virtual Private Cloud (Amazon VPC) aus. Dadurch werden die VPC-Service-Quotas geöffnet.
3. Filtern Sie nach `VPCs per Region`, um direkt zum Kontingent zu gelangen.
4. Wählen Sie VPCs pro Region und Erhöhung auf Kontoebene beantragen aus.

Wenn Sie eine dringende Anfrage haben oder Ihre Anfrage zur Erhöhung des Kontingents abgelehnt wurde, wenden Sie sich an den Support, um Unterstützung zu erhalten. Weitere Informationen finden Sie unter Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Unzureichende Berechtigungen zum Aktivieren von EC2 Fast Launch

Beschreibung

Wenn Sie EC2 Fast Launch zum ersten Mal aktivieren, ohne eine Startvorlage anzugeben, erstellt EC2 Fast Launch einen eigenen CloudFormation-Stack mit Service-Standardressourcen. Die CloudFormation-Vorlagen können jedoch nicht bereitgestellt werden, wenn Ihrem IAM-Prinzipal (Rolle oder Benutzer) die erforderlichen Berechtigungen fehlen.

Die Protokollnachricht könnte zum Beispiel so aussehen:

```
Can't enable EC2 Fast Launch. The IAM credentials that you are using do not have
 sufficient permissions. Attach EC2FastLaunchFullAccess in the IAM console.
```

Ursache

Ihrem IAM-Benutzer oder Ihrer IAM-Rolle fehlen die erforderlichen Berechtigungen, um EC2 Fast Launch zu aktivieren.

Lösung

Stellen Sie sicher, dass Ihrem IAM-Prinzipal (Benutzer oder Rolle), der EC2 Fast Launch aktiviert, die Richtlinie `EC2FastLaunchFullAccess` angehängt ist. Diese AWS-verwaltete Richtlinie gewährt vollständigen Zugriff auf alle EC2-Fast-Launch-Ressourcen. Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter EC2FastLaunchFullAccess in der Referenz für AWS-verwaltete Richtlinien.

Das Windows-Administratorpasswort für eine Amazon-EC2-Instance ändern

Wenn Sie Ihre Instance von einem AWS-Windows-AMI aus starten, legen die vorinstallierten Start-Agenten das Standardkennwort wie folgt fest:

- Für Windows Server 2022 und spätere Versionen generiert EC2Launch v2 das Standardpasswort.
- Für Windows Server 2016 und 2019 generiert der EC2Launch-Agent das Standardpasswort.
- Für Windows Server 2012 R2 und früher generiert der EC2Config-Service das Standardkennwort.

> **Note**
>
> Für Windows Server 2016 und spätere AMIs ist `Password never expires` für den lokalen Administrator deaktiviert. Für AMI-Versionen vor Windows Server 2016 ist `Password never expires` für den lokalen Administrator aktiviert.

Ändern des Administratorpassworts nach dem Verbinden

Bei der ersten Anmeldung bei einer Instance empfehlen wir Ihnen, den Standardwert des Administratorpassworts zu ändern. Mithilfe des folgenden Verfahrens können Sie das Administratorpasswort für Ihre Windows-Instance ändern.

> **Important**
>
> Speichern Sie das neue Passwort an einem sicheren Ort. Sie können das neue Passwort über die Amazon EC2-Konsole nicht abrufen. Sie können nur das Standard-Passwort über die Konsole abrufen. Wenn Sie versuchen, sich nach der Änderung des Passworts mithilfe des Standard-Passworts mit der Instance zu verbinden, erhalten Sie einen Fehler "Ihre Anmeldeinformationen sind nicht korrekt".

Um das lokale Administratorpasswort zu ändern

1. Stellen Sie eine Verbindung mit der Instance her und öffnen Sie ein Eingabeaufforderungsfenster.
2. Führen Sie den folgenden Befehl aus. Wenn Ihr neues Passwort Sonderzeichen enthält, muss das Passwort zwischen doppelten Anführungszeichen stehen:

```
net user Administrator "new_password"
```

3. Speichern Sie das neue Passwort an einem sicheren Ort.

Ändern eines verlorenen oder abgelaufenen Passworts

Wenn Sie Ihr Passwort verlieren oder es abläuft, können Sie ein neues Passwort generieren. Informationen zu den Verfahren zum Zurücksetzen des Passworts erhalten Sie unter Zurücksetzen des Windows-Administratorpassworts für eine Amazon-EC2-Windows-Instance.

Optionale Windows-Server-Komponenten zu Amazon-EC2-Windows-Instances

Zum Zugreifen auf und Installieren der optionalen Komponenten müssen Sie den richtigen EBS-Snapshot für Ihre Version von Windows Server ermitteln, aus dem Snapshot ein Volume erstellen und das Volume an Ihre Instance anfügen.

Bevor Sie beginnen

Verwenden Sie die AWS-Managementkonsole oder ein Befehlszeilen-Tool, um die Instance-ID und Availability Zone Ihrer Instance abzurufen. Sie müssen Ihr EBS-Volume in derselben Availability Zone wie Ihre Instance erstellen.

Verwenden Sie eines der folgenden Verfahren, um Windows-Server-Komponenten zu Ihrer Instance hinzuzufügen.

Console

So fügen Sie Ihrer Instance Windows-Komponenten hinzu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie in der Leiste Filter die Option Public Snapshots (Öffentliche Snapshots).
4. Fügen Sie den Filter Owner Alias (Benutzeralias) hinzu und wählen Sie die Option Amazon.
5. Fügen Sie den Filter Description (Beschreibung) hinzu und geben Sie **`Windows`** ein.
6. Drücken Sie die Eingabetaste

7. Wählen Sie den Snapshot aus, der mit Ihrer Systemarchitektur und Sprachauswahl übereinstimmt. Wählen Sie beispielsweise Windows 2019 English Installation Media, wenn auf Ihrer Instance Windows Server 2019 ausgeführt wird.
8. Wählen Sie Actions (Aktionen, Create volume from snapshot (Volume aus Snapshot erstellen) aus.
9. Wählen Sie unter Availability Zone die Availability Zone aus, die Ihrer Windows-Instance entspricht. Wählen Sie Add tag (Tag hinzufügen) und geben Sie für den Tag-Schlüssel **`Name`** und einen beschreibenden Namen für den Tag-Wert an. Wählen Sie Create Volume (Volume erstellen) aus.
10. Wählen Sie in der Meldung Volume Successfully Created (Volume erfolgreich erstellt), die als grünes Banner angezeigt wird, das eben erstellte Volume aus.
11. Wählen Sie Actions (Aktionen) und Attach Volume (Volume anfügen).
12. Wählen Sie unter Instance die Instance-ID aus.
13. Geben Sie unter Device name (Gerätename) den Namen des Geräts ein, das angefügt werden soll. Wenn Sie Hilfe zum Gerätenamen benötigen, finden Sie weitere Informationen unter Gerätenamen für Volumes auf Amazon-EC2-Instances.
14. Wählen Sie Attach volume (Volume anfügen) aus.
15. Stellen Sie eine Verbindung mit Ihrer Instance her und machen Sie das Volume verfügbar. Weitere Informationen finden Sie unter Amazon-EBS-Volume für die Verwendung verfügbar machen im Amazon-EBS-Benutzerhandbuch.

    > **Important**
    >
    > Initialisieren Sie das Volume nicht.

16. Öffnen Sie die Systemsteuerung und dann Programme und Features. Wählen Sie die Option Windows-Features aktivieren oder deaktivieren. Geben Sie das EBS-Volume mit den Installationsmedien an, wenn die entsprechende Aufforderung angezeigt wird.
17. (Optional) Wenn Sie mit dem Installationsmedium fertig sind, können Sie die Zuordnung des Volumes aufheben. Nachdem Sie die Zuordnung des Volumes aufgehoben haben, können Sie es löschen.

AWS CLI

So fügen Sie Ihrer Instance Windows-Komponenten hinzu

1. Verwenden Sie den Befehl describe-snapshots mit dem Parameter `owner-ids` und dem Filter `description`, um eine Liste mit den verfügbaren Installationsmedien-Snapshots abzurufen.

```
aws ec2 describe-snapshots \
    --owner-ids amazon \
    --filters Name=description,Values=Windows*
```

2. Beachten Sie in der Ausgabe die ID des Snapshots, der mit Ihrer Systemarchitektur und Sprachauswahl übereinstimmt. Beispiel:

```
{
    "Snapshots": [
    ...
        {
            "OwnerAlias": "amazon",
            "Description": "Windows 2019 English Installation Media",
            "Encrypted": false,
            "VolumeId": "vol-be5eafcb",
            "State": "completed",
            "VolumeSize": 6,
            "Progress": "100%",
            "StartTime": "2019-10-25T20:00:47.000Z",
            "SnapshotId": "snap-22da283e",
            "OwnerId": "123456789012"
        },
    ...
   ]
}
```

3. Verwenden Sie den Befehl create-volume, um aus dem Snapshot ein Volume zu erstellen. Geben Sie dieselbe Availability Zone wie für Ihre Instance an.

```
aws ec2 create-volume \
    --snapshot-id snap-0abcdef1234567890 \
    --volume-type gp2 \
    --availability-zone us-east-1a
```

4. Notieren Sie sich in der Ausgabe die Volume-ID.

```
{
    "AvailabilityZone": "us-east-1a",
    "Encrypted": false,
    "VolumeType": "gp2",
    "VolumeId": "vol-01234567890abcdef",
    "State": "creating",
    "Iops": 100,
    "SnapshotId": "snap-0abcdef1234567890",
    "CreateTime": "2017-04-18T10:33:10.940Z",
    "Size": 6
}
```

5. Verwenden Sie den Befehl attach-volume, um das Volume an Ihre Instance anzufügen.

```
aws ec2 attach-volume \
    --volume-id vol-0c98b37f30bcbc290 \
    --instance-id i-01474ef662b89480 \
    --device xvdg
```

6. Stellen Sie eine Verbindung mit Ihrer Instance her und machen Sie das Volume verfügbar. Weitere Informationen finden Sie unter Amazon-EBS-Volume für die Verwendung verfügbar machen im Amazon-EBS-Benutzerhandbuch.

> **Important**
>
> Initialisieren Sie das Volume nicht.

7. Öffnen Sie die Systemsteuerung und dann Programme und Features. Wählen Sie die Option Windows-Features aktivieren oder deaktivieren. Geben Sie das EBS-Volume mit den Installationsmedien an, wenn die entsprechende Aufforderung angezeigt wird.
8. (Optional) Wenn Sie mit dem Installationsmedium fertig sind, heben Sie mit dem Befehl detach-volume die Zuordnung des Volumes zur Instance auf. Nachdem Sie die Zuordnung des Volumes aufgehoben haben, können Sie das Volume mit dem Befehl delete-volume löschen.

PowerShell

So fügen Sie Ihrer Instance Windows-Komponenten hinzu

1. Verwenden Sie das Get-EC2Snapshot-Cmdlet mit den Filtern `Owner` und `description`, um eine Liste mit den verfügbaren Installationsmedien-Snapshots abzurufen.

```
Get-EC2Snapshot `
    -Owner amazon `
    -Filter @{ Name="description"; Values="Windows*" }
```

2. Beachten Sie in der Ausgabe die ID des Snapshots, der mit Ihrer Systemarchitektur und Sprachauswahl übereinstimmt. Beispiel:

```
...
DataEncryptionKeyId :
Description         : Windows 2019 English Installation Media
Encrypted           : False
KmsKeyId            :
OwnerAlias          : amazon
OwnerId             : 123456789012
Progress            : 100%
SnapshotId          : snap-0abcdef1234567890
StartTime           : 10/25/2019 8:00:47 PM
State               : completed
StateMessage        :
Tags                : {}
VolumeId            : vol-01234567890abcdef
VolumeSize          : 6
...
```

3. Verwenden Sie das New-EC2Volume-Cmdlet, um aus dem Snapshot ein Volume zu erstellen. Geben Sie dieselbe Availability Zone wie für Ihre Instance an.

```
New-EC2Volume `
    -AvailabilityZone us-east-1a `
    -VolumeType gp2 `
    -SnapshotId snap-0abcdef1234567890
```

4. Notieren Sie sich in der Ausgabe die Volume-ID.

```
Attachments      : {}
```

```
AvailabilityZone : us-east-1a
CreateTime       : 4/18/2017 10:50:25 AM
Encrypted        : False
Iops             : 100
KmsKeyId         :
Size             : 6
SnapshotId       : snap-0abcdef1234567890
State            : creating
Tags             : {}
VolumeId         : vol-01234567890abcdef
VolumeType       : gp2
```

5. Verwenden Sie das Add-EC2Volume-Cmdlet, um das Volume an Ihre Instance anzufügen.

```
Add-EC2Volume `
    -InstanceId i-1234567890abcdef0 `
    -VolumeId vol-01234567890abcdef `
    -Device xvdh
```

6. Stellen Sie eine Verbindung mit Ihrer Instance her und machen Sie das Volume verfügbar. Weitere Informationen finden Sie unter Amazon-EBS-Volume für die Verwendung verfügbar machen im Amazon-EBS-Benutzerhandbuch.

> **Important**
>
> Initialisieren Sie das Volume nicht.

7. Öffnen Sie die Systemsteuerung und dann Programme und Features. Wählen Sie die Option Windows-Features aktivieren oder deaktivieren. Geben Sie das EBS-Volume mit den Installationsmedien an, wenn die entsprechende Aufforderung angezeigt wird.
8. (Optional) Wenn Sie mit dem Installationsmedium fertig sind, heben Sie mit dem Cmdlet Dismount-EC2volume die Zuordnung des Volumes zur Instance auf. Nachdem Sie die Zuordnung des Volumes aufgehoben haben, können Sie das Volume mit dem Cmdlet Remove-EC2Volume löschen.

Das Windows-Subsystem für Linux auf Ihrer EC2-Windows-Instance installieren

Das Windows-Subsystem für Linux (WSL) ist ein Feature von Microsoft Windows. Durch die Installation des WSL auf Ihrer EC2-Windows-Instance können Sie native Linux-Befehlszeilen-Tools direkt auf der Windows-Instance ausführen.

Es gibt zwei Versionen von Windows Subsystem für Linux (WSL): WSL 1 und WSL 2. Weitere Informationen finden Sie in der Dokumentation zu Windows Subsystem für Linux auf der Microsoft-Website.

Voraussetzungen

- Das Betriebssystem muss Windows Server 2019 oder höher sein.
- Sie müssen WSL 1 auf virtualisierten Windows-Instances installieren (die Instance-Größe ist nicht `.metal`).
- Sie können entweder WSL 1 oder WSL 2 auf Bare-Metal-Instances installieren (die Instance-Größe ist `.metal`). Bare-Metal-Instances bieten die erforderliche Unterstützung für verschachtelte Virtualisierung.

Installieren des WSL auf Ihrer Windows-Instance

So installieren Sie WSL 1

1. Installieren Sie das WSL. Das für Sie zutreffende Verfahren richtet sich nach der Version von Windows Server, die auf Ihrer Instance ausgeführt wird.
   - Windows Server 2022 und höher – Führen Sie den folgenden Standardinstallationsbefehl auf Ihrer EC2-Instance aus.

     ```
     wsl --install --enable-wsl1 --no-launch
     ```

   - Windows Server 2019 – Aktivieren Sie WSL installieren Sie WSL auf der Microsoft-Website, wie unter Installieren von WSL auf früheren Versionen von Windows Server beschrieben.
2. Starten Sie Ihre EC2-Instance neu.

   ```
   shutdown -r -t 20
   ```

3. Um WSL für die Verwendung von WSL 1 zu konfigurieren, führen Sie auf Ihrer Instance den folgenden Befehl aus. Dieser Schritt ist für virtualisierte Instances erforderlich (die Instance-Größe ist nicht `.metal`).

```
wsl --set-default-version 1
```

4. Installieren Sie die Standard-Distribution.

```
wsl --install
```

So installieren Sie WSL 2 (nur Bare-Metal-Instances)

Führen Sie den folgenden Standardinstallationsbefehl auf Ihrer EC2-Instance aus. Standardmäßig ist WSL 2 installiert.

```
wsl --install
```

Hilfsprogramme zur Fehlerbehebung bei EC2 Windows

Der `EC2WinUtil`-Treiber bietet die folgenden Arten von Unterstützung bei der Fehlerbehebung für Ihre Windows-Instance.

Crash-Aufrufstapel

`EC2WinUtil` sammelt grundlegende Absturzinformationen von Ihrer Instance und schreibt sie auf die serielle Konsole. Die folgende Liste enthält einige der wichtigsten Details, die das Hilfsprogramm in die Konsole schreibt.

- Identifizierung des Moduls, das den Fehler verursacht hat.
- Der dem Ereignis zugeordnete Windows-Fehler-Code.
- Ein Stack-Trace der letzten Aufrufe.

Anhand dieser Informationen können Sie eine erste Ursachenanalyse durchführen und feststellen, ob weitere Analysen erforderlich sind. Die Ausgabe an die serielle Konsole ermöglicht es AWS auch, Absturztrends für Amazon-EC2-Treiber zu verfolgen und umfangreiche Absturzereignisse zu diagnostizieren.

> **Note**
>
> `EC2WinUtil` sammelt keine Kundendaten in seinen Crash-Aufrufstapeln.

In den Ruhezustand versetzen oder die Stabilität wieder aufnehmen

`EC2WinUtil` verfolgt die Virtualisierungseinstellungen der Instance während der Ruhezustands- und Wiederaufnahmezyklen. Dies trägt dazu bei, die langfristige Stabilität von Instances zu verbessern, die den Ruhezustand aktiviert haben.

Treiber-Versionshinweise finden Sie unter Versionsverlauf des EC2-Windows-Hilfsprogramm-Treibers

Versionsverlauf des EC2-Windows-Hilfsprogramm-Treibers

Die folgende Tabelle zeigt, welche `EC2WinUtil`-Treiber Sie unter den einzelnen Versionen von Windows Server in Amazon EC2 verwenden sollten. Frühere Versionen des Betriebssystems verwenden den Treiber, der auf den AWS-Windows-Server-AMIs, von denen aus die Instance gestartet wurde, vorinstalliert ist. Bei AMIs, die für Sie freigegeben werden oder die Sie vom AWS Marketplace abonnieren, ist der Treiber nicht vorinstalliert.

Windows Server Version	EC2WinUtil-Treiber-Version
Windows Server 2025	Aktuelle Version
Windows Server 2022	Aktuelle Version
Windows Server 2019	Aktuelle Version
Windows Server 2016	Aktuelle Version

> **Note**
>
> Vor der Treiberversion 3.0.0 konnte der `EC2WinUtil`-Treiber nicht für die manuelle Installation heruntergeladen werden. Frühere Versionen waren nur als vorinstallierte Treiber für AWS-Windows-AMIs verfügbar.

Die folgende Tabelle beschreibt die veröffentlichten Versionen des `EC2WinUtil`-Treibers.

Paket-Download-Link	Treiberversion	Details	Datum der Veröffentlichung
3.0.0	3.0.0	Der Treiber für Windows 10 wurde modernisiert und Unterstützung für die Installation als primitiver Treiber hinzugefügt.	13. Juni 2024
Der Download ist für diese Version nicht verfügbar.	2.0.0	Unterstützung für die Ausgabe auf seriellen MMIO-Ports für Metal-Instance-Typen hinzugefügt. Außerdem wurde das Crash-Parsing verbessert und das Ausgabeformat aktualisiert.	23. August 2018
Der Download ist für diese Version nicht verfügbar.	1.0.1	Der Treibername wurde auf `EC2WinUtil` aufgrund eines Namespace-Konflikts mit Amazon Inspector in geändert. Es sind mehrere Fehlerkorrekturen enthalten .	1. März 2018
Der Download ist für diese Version nicht verfügbar.	1.0.0	Erstversion. Der Treiber wurde ursprünglich `AwsAgent` genannt.	28. November 2017

EC2–Windows-Instance auf eine neuere Version von Windows Server aktualisieren

Wenn es an der Zeit ist, das Windows-Server-Betriebssystem auf Ihrer EC2-Windows-Instance von einer früheren Version zu aktualisieren, können Sie eine der folgenden Methoden verwenden.

Direkt-Upgrade

Ein direktes Upgrade wird auf einer vorhandenen Instance ausgeführt. Von diesem Vorgang sind nur die Betriebssystemdateien betroffen, Ihre Einstellungen, Serverrollen und Daten bleiben jedoch erhalten.

Migration (auch bekannt als paralleles Upgrade)

Eine Migration umfasst die Erfassung von Einstellungen, Konfigurationen und Daten und deren Übertragung auf ein neueres Betriebssystem auf einer frischen EC2-Windows-Instance. Sie können Ihre Instance über ein öffentliches oder privates Windows-AMI starten, das Sie vom AWS Marketplace abonnieren, oder über ein AMI, das mit Ihnen geteilt wurde. Außerdem können Sie ein benutzerdefiniertes AMI mit EC2 Image Builder erstellen. Weitere Informationen finden Sie im Benutzerhandbuch von Image Builder.

> **Note**
>
> AWS bietet eine Reihe von öffentlich verfügbaren Amazon Machine Images (AMIs) für Windows-Server-Versionen, die auf EC2-Instances ausgeführt werden. Diese AMIs werden monatlich aktualisiert. Weitere Informationen über die aktuellen Windows-AMIs finden Sie in der AWS-Windows-AMIs-Referenz.

Microsoft hat traditionell die Migration auf eine neuere Version von Windows Server anstelle eines Upgrades empfohlen. Die Migration kann zu weniger Upgrade-Fehlern oder -Problemen führen, sie dauert jedoch möglicherweise länger als ein direktes Upgrade, da eine neue Instance bereitgestellt werden muss, Anwendungen geplant und übertragen und die Konfigurationseinstellungen auf der neuen Instance angepasst werden müssen. Ein direktes Upgrade kann schneller sein, Softwareinkompatibilität kann jedoch zu Fehlern führen.

Inhalt

- Ein direktes Upgrade auf Ihrer EC2-Windows-Instance durchführen
- Automation-Runbooks verwenden, um eine EC2-Windows-Instance zu aktualisieren
- Eine EC2-Windows-Instance zu einem Nitro-basierten Instance-Typ migrieren
- Problembehandlung bei einem Betriebssystem-Upgrade auf einer EC2-Windows-Instance

Ein direktes Upgrade auf Ihrer EC2-Windows-Instance durchführen

Bevor Sie ein direktes Upgrade ausführen, müssen Sie ermitteln, welche Netzwerktreiber die Instance ausführt. PV-Netzwerktreiber ermöglichen Ihnen den Zugriff auf Ihre Instance per Remote-Desktop. Instances verwenden entweder AWS PV, Intel Network Adapter oder die Enhanced Networking-Treiber. Weitere Informationen finden Sie unter Paravirtual-Treiber für Windows-Instances.

Bevor Sie ein direktes Upgrade beginnen

Führen Sie die folgenden Aufgaben durch und beachten Sie die folgenden wichtigen Details, bevor Sie mit Ihrem direkten Upgrade beginnen.

- Lesen Sie die Microsoft-Dokumentation, um die Upgrade-Anforderungen, bekannte Probleme und Einschränkungen zu verstehen. Sie sollten auch die offiziellen Anweisungen für Upgrades überprüfen.
  - Upgradeoptionen für Windows Server 2012
  - Upgradeoptionen für Windows Server 2012 R2
  - Upgrade- und Konvertierungsoptionen für Windows Server 2016 und höher
  - Aktualisieren von Windows Server
- Wir empfehlen, für Instances mit mindestens zwei vCPUs und 4 GB RAM ein Betriebssystem-Upgrade durchzuführen. Bei Bedarf können Sie die Instance in eine andere Größe desselben Typs ändern (z. B. t2.small in t2.large), das Upgrade durchführen und die Instance dann wieder in die Originalgröße ändern. Wenn Sie die Instance-Größe beibehalten müssen, können Sie den Fortschritt über den Instance-Konsolen-Screenshot überwachen. Weitere Informationen finden Sie unter Änderungen des EC2 Amazon-Instanztyps.
- Stellen Sie sicher, dass das Stamm-Volume auf Ihrer Windows-Instance über genügend freien Speicherplatz verfügt. Das Windows Setup warnt Sie im Fall von unzureichendem Speicherplatz möglicherweise nicht. Informationen zur benötigten Menge an Speicherplatz für das Upgrade eines bestimmten Betriebssystems finden Sie in der Microsoft-Dokumentation. Wenn das Volume nicht über genügend Speicherplatz verfügt, kann es erweitert werden. Weitere Informationen finden Sie unter Amazon EBS Elastic Volumes im Amazon-EBS-Benutzerhandbuch.
- Bestimmen Sie Ihren Upgrade-Pfad. Sie müssen das Betriebssystem auf dieselbe Architektur upgraden. Beispielsweise müssen Sie ein 32-Bit-System auf ein 32-Bit-System upgraden. Windows Server 2008 R2 und spätere Versionen sind nur 64-Bit.

- Deaktivieren Sie Antivirus- und Anti-Spyware-Software und Firewalls. Diese Arten von Software können Konflikte beim Upgrade-Prozess erzeugen. Aktivieren Sie Antivirus- und Anti-Spyware-Software und Firewalls nach dem Abschluss des Upgrades erneut.
- Installieren Sie die neuesten Treiber, so wie unter beschriebe Eine EC2-Windows-Instance zu einem Nitro-basierten Instance-Typ migrieren.
- Der Upgrade Helper Service unterstützt nur Instances, auf denen Citrix PV-Treiber ausgeführt werden. Wenn die Instance auf Red Hat-Treibern ausgeführt wird, müssen Sie zuerst diese Treiber manuell upgraden.

Direktes Upgrade einer Instance mit AWS PV, Intel Network Adapter oder den Enhanced Networking-Treibern

Verwenden Sie das folgende Verfahren, um eine Windows Server Instance mit einem AWS PV, Intel Network Adapter oder den Enhanced Networking-Treibern zu aktualisieren.

So führen Sie ein direktes Upgrade durch

1. Erstellen Sie ein AMI des Systems, das Sie entweder zu Backup- oder Testzwecken upgraden möchten. Sie können das Upgrade dann auf der Kopie ausführen, um eine Testumgebung zu simulieren. Wenn das Upgrade abgeschlossen wird, können Sie den Datenverkehr mit geringer Ausfallzeit zu dieser Instance umleiten. Wenn das Upgrade fehlschlägt, können Sie zum Backup zurückwechseln. Weitere Informationen finden Sie unter Ein Amazon-EBS-gestütztes AMI erstellen.
2. Stellen Sie sicher, dass Ihre Windows-Server-Instance die neuesten Treiber verwendet.
    a. Informationen zum Aktualisieren Ihres AWS-PV-Treibers finden Sie unter Upgrade von PV-Treibern auf EC2-Windows-Instances.
    b. Informationen zum Update Ihres ENA-Treibers finden Sie unter ENA-Treiber auf EC2-Windows-Instances installieren.
    c. Informationen zum Aktualisieren Ihrer Intel-Treiber finden Sie unter Erweitertes Netzwerk mit der Intel 82599 VF-Schnittstelle
3. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
4. Wählen Sie im Navigationsbereich Instances aus. Suchen Sie die Instance. Notieren Sie die Instance-ID und Availability Zone für die Instance. Diese Informationen werden später in diesem Verfahren benötigt.

5. Wenn Sie von Windows Server 2012 oder 2012 R2 auf Windows Server 2016 oder später aktualisieren, führen Sie die folgenden Schritte auf Ihrer Instance durch, bevor Sie fortfahren.

   a. Deinstallieren Sie den EC2Config-Service. Weitere Informationen finden Sie unter Windows Service Administration für EC2Launch-v2- und EC2Config-Agents.

   b. Installieren Sie EC2Launch v1 oder den EC2Launch-v2-Agenten. Weitere Informationen finden Sie unter Den EC2Launch-v1-Agenten verwenden, um Aufgaben während des Starts einer EC2-Windows-Instance auszuführen und Den EC2Launch-v2-Agenten verwenden, um Aufgaben während des Starts einer EC2-Windows-Instance auszuführen.

   c. Installieren Sie den AWS Systems Manager SSM Agent. Weitere Informationen finden Sie unter Manuelle Installation des SSM-Agent in Amazon EC2 für Windows Server im Benutzerhandbuch für AWS Systems Manager.

6. Erstellen Sie ein neues Volume aus einem Windows Server-Installationsmedien-Snapshot.

   a. Wählen Sie im Navigationsbereich links unter Elastic Block Store die Option Snapshots.

   b. Wählen Sie in der Filterleiste Öffentliche Schnappschüsse.

   c. Geben Sie in der Suchleiste die folgenden Filter ein:

      - Wählen Sie Owner Alias, dann = und dann Amazon.
      - Wählen Sie Beschreibung und beginnen Sie dann mit der Eingabe**`Windows`**. Wählen Sie den Windows-Filter aus, der der Systemarchitektur und der bevorzugten Sprache entspricht, auf die Sie aktualisieren möchten. Wählen Sie zum Beispiel Windows 2019 English Installation Media für ein Upgrade auf Windows Server 2019.

   d. Aktivieren Sie das Kontrollkästchen neben dem Snapshot, der der Systemarchitektur und den Spracheinstellungen entspricht, auf die Sie aktualisieren, und wählen Sie dann Aktionen, Volume aus Snapshot erstellen.

   e. Wählen Sie auf der Seite Volume erstellen die Availability Zone, die zu Ihrer Windows-Instance passt, und wählen Sie dann Volume erstellen.

7. Wählen Sie im Banner Erfolgreich erstelltes Volume vol-***`1234567890Beispiel`*** oben auf der Seite die ID des Volumes, das Sie gerade erstellt haben.

8. Wählen Sie Actions (Aktionen) und Attach Volume (Volume anfügen).

9. Wählen Sie auf der Seite Volume anhängen unter Instance die Instance-ID Ihrer Windows-Instance und wählen Sie dann Volume anhängen.

10. Stellen Sie das neue Volume zur Verwendung bereit, indem Sie die Schritte unter Stellen Sie ein Amazon EBS-Volume für die Verwendung unter Windows bereit durchführen.

> **Important**
>
> Initialisieren Sie den Datenträger nicht, da dadurch die vorhandenen Daten gelöscht werden.

11. Wechseln Sie in Windows PowerShell zum neuen Volume-Laufwerk. Beginnen Sie das Upgrade, indem Sie das Installationsmedien-Volume öffnen, das Sie an die Instance angehängt haben.

    a. Wenn Sie ein Upgrade auf Windows Server 2016 oder höher installieren, führen Sie Folgendes aus:

    ```
    .\setup.exe /auto upgrade /dynamicupdate disable
    ```

    > **Note**
    >
    > Das Ausführen von setup.exe mit deaktivierter `/dynamicupdate`-Option verhindert, dass Windows während des Windows Server-Upgrade-Prozesses Updates installiert, da die Installation von Updates während des Upgrades zu Fehlern führen kann. Sie können Updates mit Windows Update installieren, nachdem das Upgrade abgeschlossen ist.

    Wenn Sie ein Upgrade auf eine frühere Version von Windows Server installieren, führen Sie Folgendes aus:

    ```
    Sources\setup.exe
    ```

    b. Wählen Sie für Wählen Sie das Betriebssystem aus, das Sie installieren möchten die vollständige Installationsoption für Ihre Windows-Server-Instance aus und dann Weiter.

    c. Wählen Sie für Which type of installation do you want? die Option Upgrade aus.

    d. Schließen Sie den Assistenten ab.

Windows Server Setup kopiert und verarbeitet jetzt Dateien. Nach einigen Minuten wird Ihre Remote-Desktop-Sitzung beendet. Die für das Upgrade benötigte Zeit hängt von der Anzahl an Anwendungen und Serverrollen ab, die auf Ihrer Windows Server-Instance ausgeführt werden. Das Upgrade kann vielleicht nur 40 Minuten oder auch einige Stunden dauern. Während des Upgrades schlägt die

Instance eventuell bei einer oder mehreren Statusprüfungen fehl. Wenn das Upgrade abgeschlossen ist, verlaufen alle Statusprüfungen erfolgreich. Sie können die Konsolenausgabe im Systemprotokoll prüfen oder Amazon CloudWatch-Metriken für Festplatten- und CPU-Aktivitäten verwenden, um zu ermitteln, ob das Upgrade fortschreitet.

> **Note**
>
> Wenn Sie ein Upgrade auf Windows Server 2019 erstellen, können Sie nach Abschluss des Upgrades den Desktop-Hintergrund manuell ändern, um den vorherigen Namen des Betriebssystems bei Bedarf zu löschen.

Wenn die Instance nach einigen Stunden noch nicht alle Statusprüfungen erfolgreich bestanden hat, finden Sie Informationen unter Problembehandlung bei einem Betriebssystem-Upgrade auf einer EC2-Windows-Instance.

Aufgaben nach dem Upgrade

1. Melden Sie sich bei der Instance an, um ein Upgrade für das .NET Framework zu initiieren, und starten Sie das System neu, wenn Sie dazu aufgefordert werden.
2. Falls Sie dies in einem früheren Schritt noch nicht getan haben, installieren Sie den EC2Launch-v1-oder EC2Launch-v2-Agenten. Weitere Informationen finden Sie unter Den EC2Launch-v1-Agenten verwenden, um Aufgaben während des Starts einer EC2-Windows-Instance auszuführen und Den EC2Launch-v2-Agenten verwenden, um Aufgaben während des Starts einer EC2-Windows-Instance auszuführen.
3. Wenn Sie ein Upgrade auf Windows Server 2012 R2 vorgenommen haben, empfehlen wir ein Upgrade der PV-Treiber auf AWS PV-Treiber. Wenn Sie auf einer Nitro-basierten Instance ein Upgrade durchgeführt haben, empfehlen wir Ihnen, die NVME- und ENA-Treiber zu installieren oder zu aktualisieren. Weitere Informationen finden Sie unter AWS NVMe-Treiber oder Aktivieren von Enhanced Networking unter Windows.
4. Aktivieren Sie die Antivirus- und Anti-Spyware-Software und Firewalls erneut.

Automation-Runbooks verwenden, um eine EC2-Windows-Instance zu aktualisieren

Sie können ein automatisiertes Upgrade Ihrer Windows- und SQL-Server-Instances in AWS mit AWS Systems Manager-Automation-Runbooks durchführen.

Inhalt

- Zugehörige Services
- Ausführungsoptionen
- Aktualisieren von Windows Server
- Upgrade von SQL Server

Zugehörige Services

Die folgenden AWS-Services werden im automatisierten Upgrade-Prozess verwendet:

- AWS Systems Manager. AWS Systems Manager ist eine leistungsstarke, einheitliche Schnittstelle zur zentralen Verwaltung Ihrer AWS-Ressourcen. Weitere Informationen finden Sie im AWS Systems Manager-Benutzerhandbuch.
- AWS Systems Manager Agent (SSM Agent) ist eine Amazon-Software, die auf einer Amazon EC2-Instance, einem On-Premises-Server oder einer virtuellen Maschine (VM) installiert und konfiguriert werden kann. SSM Agent ermöglicht es Systems Manager, diese Ressourcen zu aktualisieren, zu verwalten und zu konfigurieren. Der Agent verarbeitet Anforderungen des Systems-Manager-Services in der AWS-Cloud und führt sie dann wie in der Anforderung angegeben aus. Weitere Informationen finden Sie unter Arbeiten mit SSM Agent im AWS Systems Manager-Benutzerhandbuch.
- AWS Systems Manager SSM-Runbooks. Ein SSM-Runbook definiert die Aktionen, die Systems Manager auf Ihren verwalteten Instances durchführt. Die SSM-Runbooks liegen im JavaScript Object Notation (JSON)- oder YAML-Format vor und enthalten die von Ihnen angegebenen Schritte und Parameter. Dieses Thema verwendet zwei Systems-Manager-SSM-Runbooks für die Automatisierung. Weitere Informationen finden Sie in der Referenz zum AWS Systems Manager-Automation-Runbook im AWS Systems Manager-Benutzerhandbuch.

Ausführungsoptionen

Wählen Sie erst Automation (Automatisierung) auf der Systems Manager-Konsole und dann Execute (Ausführen). Nachdem Sie ein Automation-Dokument ausgewählt haben, werden Sie aufgefordert, eine Option zur Automatisierungsausführung auszuwählen. Sie wählen aus den folgenden Optionen. In den Schritten für die in diesem Thema angegebenen Pfade verwenden wir die Option Simple execution (Einfache Ausführung).

Einfache Ausführung

Wählen Sie diese Option, wenn Sie eine einzelne Instance aktualisieren möchten, aber nicht jeden Automatisierungsschritt durchlaufen möchten, um die Ergebnisse zu prüfen. Diese Option wird in den folgenden Upgrade-Schritten näher erläutert.

Rate control (Ratenregelung

Wählen Sie diese Option, wenn Sie das Upgrade auf mehr als eine Instance anwenden möchten. Sie definieren die folgenden Einstellungen.

- Parameter

  Diese Einstellung, die auch in den Einstellungen für Multi-Konto und Region festgelegt ist, definiert, wie Ihre Automatisierung verzweigt ist.

- Targets (Ziele

  Wählen Sie das Ziel aus, auf das Sie die Automatisierung anwenden möchten. Diese Einstellung wird auch in den Einstellungen für Multi-Konto und Region festgelegt.

- Parameter Values (Parameterwerte

  Verwenden Sie die Werte, die in den Parametern im Automatisierungsdokument definiert sind.

- Resource Group (Ressourcengruppe

  In AWS ist eine Ressource eine Entität, mit der Sie arbeiten können. Beispiele sind Amazon EC2-Instances, AWS CloudFormation-Stacks oder Amazon S3-Buckets. Wenn Sie mit mehreren Ressourcen arbeiten, kann es hilfreich sein, diese als Gruppe zu verwalten, anstatt für jede Aufgabe von einem AWS-Service zu einem anderen zu wechseln. In einigen Fällen möchten Sie vielleicht große Anzahlen an verwandten Ressourcen verwalten, wie EC2-Instances, die eine Anwendungsebene ausmachen. In diesem Fall müssen Sie wahrscheinlich Massenaktionen auf diesen Ressourcen gleichzeitig durchführen.

- Tags

  Mit Tags (Markierungen) können Sie AWS-Ressourcen auf unterschiedliche Weise kategorisieren (z. B. nach Zweck, Besitzer oder Umgebung). Diese Kategorisierung ist nützlich, wenn Sie viele Ressourcen desselben Typs haben. Sie können eine bestimmte Ressource mit den zugewiesenen Tags (Markierungen) schnell identifizieren.

- Rate Control (Ratenregelung

Die Ratenregelung wird auch in den Einstellungen für Multi-Konto und Region festgelegt. Wenn Sie die Parameter der Ratenregelung festlegen, definieren Sie, auf wie viel Ihrer Flotte die Automatisierung angewendet wird, und zwar entweder nach Zielanzahl oder Prozentzahl der Flotte.

Multi-Account and Region (Multi-Konto und Region

Zusätzlich zu den unter der Ratenregelung angegebenen Parametern, die auch in den Einstellungen für Multi-Konto und Region verwendet werden, gibt es zwei zusätzliche Einstellungen:

- Accounts and organizational units (OUs) (Konten und Organisationseinheiten (OUs)

  Geben Sie mehrere Konten an, auf denen Sie die Automatisierung ausführen möchten.
- AWS-Regionen

  Geben Sie mehrere AWS-Regionen an, in denen Sie die Automatisierung ausführen möchten.

Manuelle Ausführung

Diese Option ähnelt der Einfachen Ausführung, allerdings können Sie jeden Automatisierungsschritt durchlaufen und die Ergebnisse prüfen.

Aktualisieren von Windows Server

Das `AWSEC2-CloneInstanceAndUpgradeWindows`-Runbook erstellt ein Amazon Machine Image (AMI) von einer Windows-Server-Instance in Ihrem Konto und aktualisiert dieses AMI auf eine unterstützte Version Ihrer Wahl. Dieser mehrschrittige Prozess kann bis zu zwei Stunden dauern.

Es sind zwei AMIs im automatisierten Upgrade-Prozess enthalten:

- Aktuell ausgeführte Instance. Das erste AMI ist die aktuell ausgeführte Instance, die nicht aktualisiert wird. Diese AMI wird verwendet, um eine andere Instance zu starten, damit diese das direkte Upgrade ausführt. Wenn der Vorgang abgeschlossen ist, wird dieses AMI aus Ihrem Konto gelöscht, es sei denn, sie geben speziell an, dass Sie die Original-Instance behalten möchten. Diese Einstellung wird vom Parameter gehandhabt `KeepPreUpgradeImageBackUp` (der Standardwert ist `false`, was bedeutet, dass das AMI standardmäßig gelöscht wird).
- Aktualisiertes AMI. Dieses AMI ist das Ergebnis des Automatisierungsvorgangs.

Das Endergebnis ist ein AMI, welches die aktualisierte Instance des AMI ist.

Wenn das Upgrade abgeschlossen ist, können Sie die Anwendung testen, indem Sie das neue AMI in Ihrer Amazon VPC starten. Nachdem Sie den Test abgeschlossen haben und bevor Sie eine weitere Aktualisierung durchführen, planen Sie die Anwendungsausfallzeit ein, bevor Sie vollständig zu der aktualisierten Instance wechseln.

Voraussetzungen

Um Ihr Windows-Server-Upgrade mithilfe des AWS Systems Manager-Automatisierungsdokuments zu automatisieren, müssen Sie die folgenden Aufgaben ausführen:

- Erstellen Sie eine IAM-Rolle mit den angegebenen IAM-Richtlinien, damit Systems Manager Automatisierungsaufgaben auf Ihren Amazon EC2-Instances durchführen und überprüfen kann, dass Sie die Voraussetzungen für die Verwendung von Systems Manager erfüllen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im AWS Identity and Access Management-Benutzerhandbuch.
- Wählen Sie die Option aus, wie die Automatisierung ausgeführt werden soll. Die Optionen für die Ausführung sind Simple execution (Einfache Ausführung), Rate control (Ratenregelung), Multi-account and Region (Multi-Konto und Region) und Manual execution (Manuelle Ausführung). Weitere Informationen zu diesen Optionen finden Sie unter Ausführungsoptionen.
- Stellen Sie sicher, dass SSM Agent auf Ihrer Instance installiert ist. Weitere Informationen finden Sie unter Installation und Konfiguration von SSM Agent auf Amazon-EC2-Instances für Windows Server.
- Windows PowerShell 3.0 oder höher muss auf Ihrer Instance installiert sein.
- Für Instances, die einer Microsoft Active Directory-Domain angehören, empfehlen wir, eine `SubnetId` anzugeben, die keine Verbindung zu Ihren Domain-Cntrollern aufweist, um Hostnamenkonflikte zu vermeiden.
- Das Instance-Subnetz muss über eine ausgehende Verbindung zum Internet verfügen, die Zugriff auf AWS-Services wie Amazon S3 und den Zugriff auf Download-Patches von Microsoft ermöglicht. Diese Anforderung ist erfüllt, wenn das Subnetz entweder ein öffentliches Subnetz ist und die Instance eine öffentliche IP-Adresse hat, oder wenn es sich bei dem Subnetz um ein privates Subnetz mit einer Route handelt, die Internetverkehr an ein öffentliches NAT-Gerät sendet.
- Diese Automatisierung funktioniert mit Instances, auf denen Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016 und Windows Server 2019 ausgeführt wird.
- Stellen Sie sicher, dass die Instance 20 GB freien Speicherplatz auf dem Boot-Datenträger hat.

- Wenn die Instance nicht mit einer von AWS bereitgestellten Windows-Lizenz versehen ist, geben Sie eine Amazon-EBS-Snapshot-ID mit Windows-Server-2012-R2-Installationsmedien an. So gehen Sie vor:
  1. Überprüfen Sie, ob die Amazon-EC2-Instance Windows Server 2012 oder höher ausführt.
  2. Erstellen Sie ein Amazon-EBS-Volume mit 6 GB in derselben Availability Zone, in der die Instance ausgeführt wird. Fügen Sie das Volume der Instance an. Mounten Sie dies beispielsweise als Laufwerk D.
  3. Klicken Sie mit der rechten Maustaste auf die ISO, und mounten Sie es für eine Instance, beispielsweise als Laufwerk E.
  4. Kopieren Sie den Inhalt der ISO von Laufwerk E:\ zu Laufwerk D:\.
  5. Erstellen Sie einen Amazon-EBS-Snapshot des 6 GB-Volumes, das Sie oben in Schritt 2 erstellt haben.

Einschränkungen für Windows Server Upgrade

Diese Automatisierung unterstützt keine Upgrades von Windows-Domain-Controllern, Clustern oder Windows-Desktopbetriebssystemen. Diese Automation unterstützt außerdem keine Amazon–EC2-Instances für Windows Server mit den folgenden installierten Rollen:

- Remote Desktop Session Host (RDSH)
- Remote Desktop Connection Broker (RDCB)
- Remote Desktop Virtualization Host (RDVH)
- Remote Desktop Web Access (RDWA)

Schritte zum Durchführen eines automatisierten Upgrades von Windows Server

Gehen Sie folgendermaßen vor, um ein Upgrade Ihrer Windows-Server-Instance mit dem Automation-Runbook AWSEC2-CloneInstanceAndUpgradeSQLServer durchzuführen.

1. Öffnen Sie Systems Manager von der AWS Management Console aus.
2. Wählen Sie im linken Navigationsbereich unter Änderungsmanagement Automatisierung aus.
3. Wählen Sie Execute automation (Automatisierung ausführen).
4. Suchen Sie nach dem Automatisierungsdokument mit der Bezeichnung `AWSEC2-CloneInstanceAndUpgradeWindows`.

5. Wenn der Dokumentenname angezeigt wird, wählen Sie ihn aus. Anschließend werden die Dokumentendetails angezeigt.
6. Klicken Sie auf Execute automation (Automatisierung ausführen), um die Parameter für dieses Dokument einzugeben. Lassen Sie Simple execution (Einfache Ausführung) oben auf der Seite ausgewählt.
7. Geben Sie die angeforderten Parameter basierend auf den folgenden Hinweisen ein.

   - `InstanceID`

     Typ: Zeichenfolge

     (Erforderlich) Die Instance, auf der Windows Server 2008 R2, 2012 R2, 2016, oder 2019 ausgeführt wird, auf der SSM Agent installiert ist.

   - `InstanceProfile`.

     Typ: Zeichenfolge

     (Erforderlich) Das IAM-Instance-Profil. Dies ist die IAM-Rolle zur Durchführung der Systems-Manager-Automatisierung für die Amazon-EC2-Instance und AWS-AMIs. Weitere Informationen finden Sie unter EC2-Instance-Berechtigungen konfigurieren im Benutzerhandbuch für AWS Systems Manager.

   - `TargetWindowsVersion`

     Typ: Zeichenfolge

     (Erforderlich) Wählen Sie die Windows-Zielversion aus.

   - `SubnetId`

     Typ: Zeichenfolge

     (Erforderlich) Dies ist das Subnetz für den Upgrade-Prozess und der Ort, an dem sich Ihre Quell-EC2-Instance befindet. Stellen Sie sicher, dass das Subnetz über ausgehende Konnektivität zu AWS-Services, einschließlich Amazon S3, und Microsoft (zum Herunterladen von Patches) verfügt.

   - `KeepPreUpgradedBackUp`

     Typ: Zeichenfolge

(Optional) Wenn dieser Parameter auf `true` gesetzt ist, behält die Automatisierung das von der Instance erstellte Image bei. Die Standardeinstellung lautet `false`.

- `RebootInstanceBeforeTakingImage`

  Typ: Zeichenfolge

  (Optional) Der Standardwert ist `false` (kein Reboot). Wenn dieser Parameter auf `true` gesetzt ist, startet Systems Manager die Instance neu, bevor ein AMI für das Upgrade erstellt wird.

8. Nachdem Sie die Parameter eingegeben haben, wählen Sie Execute (Ausführen) aus. Wenn die Automatisierung beginnt, können Sie den Ausführungsfortschritt überwachen.
9. Wenn die Automatisierung abgeschlossen ist, sehen Sie die AMI-ID. Sie können das AMI starten, um zu überprüfen, ob das Windows-Betriebssystem aktualisiert wurde.

   > **Note**
   >
   > Es ist nicht notwendig, dass die Automatisierung alle Schritte ausführt. Die Schritte basieren bedingt auf dem Verhalten der Automatisierung und der Instance. Der Systems Manager überspringt möglicherweise einige Schritte, die nicht erforderlich sind. Darüber hinaus können einige Schritte ausfallen. Systems Manager versucht, alle aktuellen Patches zu aktualisieren und zu installieren. Manchmal wird bei einigen Patches aber auch die Zeit basierend auf einer definierbaren Zeitüberschreitungs-Einstellung für diesen Schritt überschritten. Wenn dies geschieht, fährt die Systems Manager-Automatisierung mit dem nächsten Schritt fort, um sicherzustellen, dass das interne Betriebssystem auf die Windows Server-Zielversion aktualisiert wird.

10. Nachdem die Automatisierung abgeschlossen wurde, können Sie eine Amazon EC2-Instance mit der AMI-ID starten, um Ihr Upgrade zu überprüfen. Weitere Informationen zum Erstellen einer Amazon-EC2-Instance aus einem AWS-AMI finden Sie unter Wie starte ich eine EC2 Instance aus einem benutzerdefinierten AMI?

Upgrade von SQL Server

Das Skript AWSEC2-CloneInstanceAndUpgradeSQLServer erstellt ein AMI aus einer Amazon-EC2-Instance, auf der SQL Server in Ihrem Konto ausgeführt wird, und aktualisiert dann das AMI auf eine aktuellere Version von SQL Server. Dieser mehrschrittige Prozess kann bis zu zwei Stunden dauern.

In diesem Workflow, die Automatisierung erstellt ein AMI aus der Instance und startet dann das neu erstellte AMI in dem Subnetz, das Sie bereitstellen. Die Automatisierung führt dann ein direktes Upgrade von SQL Server durch. Nach dem Upgrade erstellt die Automatisierung ein neues AMI, bevor die aktualisierte Instance beendet wird.

Es sind zwei AMIs im automatisierten Upgrade-Prozess enthalten:

- Aktuell ausgeführte Instance. Das erste AMI ist die aktuell ausgeführte Instance, die nicht aktualisiert wird. Diese AMI wird verwendet, um eine andere Instance zu starten, damit diese das direkte Upgrade ausführt. Wenn der Vorgang abgeschlossen ist, wird dieses AMI aus Ihrem Konto gelöscht, es sei denn, sie geben speziell an, dass Sie die Original-Instance behalten möchten. Diese Einstellung wird vom Parameter gehandhabt `KeepPreUpgradeImageBackUp` (der Standardwert ist `false`, was bedeutet, dass das AMI standardmäßig gelöscht wird).
- Aktualisiertes AMI. Dieses AMI ist das Ergebnis des Automatisierungsvorgangs.

Das Endergebnis ist ein AMI, welches die aktualisierte Instance des AMI ist.

Wenn das Upgrade abgeschlossen ist, können Sie die Anwendung testen, indem Sie das neue AMI in Ihrer Amazon VPC starten. Nachdem Sie den Test abgeschlossen haben und bevor Sie eine weitere Aktualisierung durchführen, planen Sie die Anwendungsausfallzeit ein, bevor Sie vollständig zu der aktualisierten Instance wechseln.

Voraussetzungen

Um Ihr SQL-Server-Upgrade mithilfe des AWS Systems Manager-Automatisierungsdokuments zu automatisieren, müssen Sie die folgenden Aufgaben ausführen:

- Erstellen Sie eine IAM-Rolle mit den angegebenen IAM-Richtlinien, damit Systems Manager Automatisierungsaufgaben auf Ihren Amazon EC2-Instances durchführen und überprüfen kann, dass Sie die Voraussetzungen für die Verwendung von Systems Manager erfüllen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im AWS Identity and Access Management-Benutzerhandbuch.
- Wählen Sie die Option aus, wie die Automatisierung ausgeführt werden soll. Die Optionen für die Ausführung sind Simple execution (Einfache Ausführung), Rate control (Ratenregelung), Multi-account and Region (Multi-Konto und Region) und Manual execution (Manuelle Ausführung). Weitere Informationen zu diesen Optionen finden Sie unter Ausführungsoptionen.
- Die Amazon-EC2-Instance muss Windows Server 2008 R2 oder höher und SQL Server 2008 oder höher verwenden.

- Stellen Sie sicher, dass SSM Agent auf Ihrer Instance installiert ist. Weitere Informationen finden Sie unter Arbeiten mit SSM-Agent auf Amazon-EC2-Instances für Windows Server.
- Überprüfen Sie, ob die Instance über genügend freien Speicherplatz verfügt:
  - Wenn Sie ein Upgrade von Windows Server 2008 R2 auf 2012 R2 oder von Windows Server 2012 R2 auf ein neueres Betriebssystem durchführen, stellen Sie sicher, dass Sie über 20 GB freien Festplattenspeicher auf der Startdiskette der Instance verfügen.
  - Wenn Sie ein Upgrade von Windows Server 2008 R2 auf 2016 oder höher durchführen, stellen Sie sicher, dass die Instance über 40 GB freien Festplattenspeicher auf der Startdiskette der Instance verfügt.
- Für Instances, die eine Bring Your Own License (BYOL) SQL Server-Version verwenden, gelten die folgenden zusätzlichen Voraussetzungen:
  - Stellen Sie eine Amazon-EBS-Snapshot-ID mit den Installationsmedien des Ziel-SQL-Servers berei. So gehen Sie vor:
    1. Überprüfen Sie, ob die Amazon-EC2-Instance Windows Server 2008 R2 oder höher ausführt.
    2. Erstellen Sie ein Amazon-EBS-Volume mit 6 GB in derselben Availability Zone, in der die Instance ausgeführt wird. Fügen Sie das Volume der Instance an. Mounten Sie dies beispielsweise als Laufwerk D.
    3. Klicken Sie mit der rechten Maustaste auf die ISO, und mounten Sie es für eine Instance, beispielsweise als Laufwerk E.
    4. Kopieren Sie den Inhalt der ISO von Laufwerk E:\ zu Laufwerk D:\.
    5. Erstellen Sie einen Amazon-EBS-Snapshot des 6 GB-Volumes, das Sie in Schritt 2 erstellt haben.

Einschränkungen für automatisierte Upgrades von SQL Server

Bei der Verwendung des Runbooks AWSEC2-CloneInstanceAndUpgradeSQLServer zum Ausführen eines automatisierten Upgrades gelten die folgenden Beschränkungen:

- Das Upgrade ist nur auf einem SQL Server mit Windows-Authentifizierung möglich.
- Stellen Sie sicher, dass keine Sicherheits-Patch-Updates auf den Instances ausstehen. Öffnen Sie Control Panel (Systemsteuerung), und wählen Sie dann Check for updates (Auf Aktualisierungen prüfen).
- SQL Server-Bereitstellungen in HA und der Spiegelungsmodus werden nicht unterstützt.

Schritte zum Durchführen eines automatisierten Upgrades von SQL Server

Gehen Sie folgendermaßen vor, um ein Upgrade von SQL Server mit dem Automatisierungs-Runbook AWSEC2-CloneInstanceAndUpgradeSQLServer durchzuführen.

1. Wenn Sie dies nicht bereits getan haben, laden Sie die SQL Server 2016 .iso-Datei herunter und mounten Sie sie auf dem Quellserver.
2. Nachdem die .iso-Datei gemountet wurde, kopieren Sie alle Komponentendateien und platzieren Sie sie auf dem Volume Ihrer Wahl.
3. Erstellen Sie einen Amazon-EBS-Snapshot des Volumes und kopieren Sie die Snapshot-ID für eine spätere Verwendung in die Zwischenablage. Weitere Informationen finden Sie unter Amazon-EBS-Snapshots erstellen im Amazon-EC2-Benutzerhandbuch.
4. Fügen Sie das Instance-Profil an die Amazon-EC2-Quell-Instance an. Dadurch kann Systems Manager mit der EC2-Instance kommunizieren und darauf Befehle ausführen, nachdem sie zum AWS Systems Manager-Service hinzugefügt wurde. Für dieses Beispiel haben wir die Rolle `SSM-EC2-Profile-Role` genannt, wobei die `AmazonSSMManagedInstanceCore` -Richtlinie der Rolle angefügt ist.
5. Wählen Sie in der AWS Systems Manager-Konsole im linken Navigationsbereich Managed Instances (Verwaltete Instances) aus. Überprüfen Sie, dass sich Ihre EC2-Instance in der Liste der verwalteten Instances befindet. Wenn Ihre Instance nach einigen Minuten nicht angezeigt wird, lesen Sie unter Wo sind meine Instances? im AWS Systems Manager-Benutzerhandbuch nach.
6. Wählen Sie im linken Navigationsbereich unter Änderungsmanagement Automatisierung aus.
7. Wählen Sie Execute automation (Automatisierung ausführen).
8. Suchen Sie nach dem Automatisierungsdokument mit der Bezeichnung `AWSEC2-CloneInstanceAndUpgradeSQLServer`.
9. Rufen Sie das `AWSEC2-CloneInstanceAndUpgradeSQLServer`-SSM-Dokument auf und wählen Sie dann Next (Weiter).
10. Stellen Sie sicher, dass die Option Simple execution (Einfache Ausführung) ausgewählt ist.
11. Geben Sie die angeforderten Parameter basierend auf den folgenden Hinweisen ein.

    - `InstanceId`

      Typ: Zeichenfolge

      (Erforderlich) Die Instance, die SQL Server 2008 R2 (oder höher) ausführt.

- `IamInstanceProfile`

  Typ: Zeichenfolge

  (Erforderlich) Das IAM-Instance-Profil.

- `SQLServerSnapshotId`

  Typ: Zeichenfolge

  (Erforderlich) Die Snapshot-ID für die Installationsmedien des Ziel-SQL-Servers. Dieser Parameter ist für Instances mit SQL-Server-Lizenzen nicht erforderlich.

- `SubnetId`

  Typ: Zeichenfolge

  (Erforderlich) Dies ist das Subnetz für den Upgrade-Prozess und der Ort, an dem sich Ihre Quell-EC2-Instance befindet. Stellen Sie sicher, dass das Subnetz über ausgehende Konnektivität zu AWS-Services, einschließlich Amazon S3, und Microsoft (zum Herunterladen von Patches) verfügt.

- `KeepPreUpgradedBackUp`

  Typ: Zeichenfolge

  (Optional) Wenn dieser Parameter auf `true` gesetzt ist, behält die Automatisierung das von der Instance erstellte Image bei. Die Standardeinstellung lautet `false`.

- `RebootInstanceBeforeTakingImage`

  Typ: Zeichenfolge

  (Optional) Der Standardwert ist `false` (kein Reboot). Wenn dieser Parameter auf `true` gesetzt ist, startet Systems Manager die Instance neu, bevor ein AMI für das Upgrade erstellt wird.

- `TargetSQLVersion`

  Typ: Zeichenfolge

  (Optional) Die Zielversion von SQL Server. Der Standardwert ist `2016`.

12. Nachdem Sie die Parameter eingegeben haben, wählen Sie Execute (Ausführen) aus. Wenn die Automatisierung beginnt, können Sie den Ausführungsfortschritt überwachen.

13. Wenn der Execution Status (Ausführungsstatus) Success (Erfolg) anzeigt, erweitern Sie Outputs (Ausgaben), um die AMI-Informationen anzuzeigen. Sie können Ihre SQL-Server-Instance für die VPC Ihrer Wahl mit der AMI-ID starten.
14. Öffnen Sie die Amazon EC2-Konsole. Wählen Sie im linken Navigationsbereich AMIs aus. Das neue AMI sollte angezeigt werden.
15. Um zu überprüfen, ob die neue Version von SQL Server erfolgreich installiert wurde, wählen Sie das neue AMI aus und klicken Sie auf Launch (Starten).
16. Wählen Sie den Typ der Instance, den das AMI haben soll, die VPC und das Subnetz, in das Sie bereitstellen möchten, und den Speicher, den Sie verwenden möchten. Da Sie die neue Instance von einem AMI starten, werden Ihnen die Volumes als Option angeboten, die in die neue EC2-Instance, die Sie starten, aufgenommen werden kann. Sie können alle diese Volumes entfernen oder Volumes hinzufügen.
17. Fügen Sie ein Tag (Markierung) hinzu, damit Sie Ihre Instance leichter identifizieren können.
18. Fügen Sie die Sicherheitsgruppe oder Gruppen zur Instance hinzu.
19. Wählen Sie Launch Instance aus.
20. Wählen Sie den Tag (Markierung)-Namen für die Instance und anschließend Connect (Verbinden) im Dropdown-Menü Actions (Aktionen) aus.
21. Vergewissern Sie sich, dass die neue SQL-Server-Version die Datenbank-Engine auf der neuen Instance ist.

Eine EC2-Windows-Instance zu einem Nitro-basierten Instance-Typ migrieren

Die AWS-Windows-AMIs sind mit den von den Microsoft-Installationsmedien verwendeten Standardeinstellungen konfiguriert, mit einigen Anpassungen. Die Anpassungen umfassen Treiber und Konfigurationen, die Nitro-basierte Instances wie M5 und C5 unterstützen.

Bei der Migration von Xen-basierten zu Nitro-basierten Instances, einschließlich Bare-Metal-Instances, empfehlen wir Ihnen, die Schritte in diesem Thema in den folgenden Fällen auszuführen:

- Wenn Sie Instances von benutzerdefinierten Windows-AMIs starten
- Wenn Sie Instances von Windows-AMIs von Amazon starten, die vor August 2018 erstellt wurden

Alternativ können Sie mit dem Automatisierungsdokument `AWSSupport-UpgradeWindowsAWSDrivers` die in Teil 1, Teil 2 und Teil 3 beschriebenen Verfahren

automatisieren. Wenn Sie sich für das automatisierte Verfahren entscheiden, lesen Sie (Alternativ) Aktualisieren der AWS-PV-, ENA- und NVMe-Treiber mit AWS Systems Manager. Fahren Sie dann mit Teil 4 und Teil 5 fort.

Weitere Informationen finden Sie unter Amazon EC2-Update – zusätzliche Instance-Typen, Nitro-System und CPU-Optionen.

> **Note**
>
> Die folgenden Migrationsverfahren können unter Windows Server Version 2016 und höher ausgeführt werden. Frühere Betriebssystemversionen, deren Lebensdauer abgelaufen ist, wurden nicht getestet und sind möglicherweise nicht mit den neuesten Instance-Typen kompatibel.
> Informationen zur Migration von Linux-Instances finden Sie unter the section called “Änderungen des Instance-Typs”.

Inhalt

- Teil 1: Installieren und aktualisieren von AWS PV-Treibern
- Teil 2: Installieren und aktualisieren von ENA
- Teil 3: Aktualisieren von AWS NVMe-Treibern
- Teil 4: Aktualisieren von EC2Config und EC2Launch
- Teil 5: Installieren des Treibers für den seriellen Port für Bare Metal-Instances
- Teil 6: Aktualisieren der Energieverwaltungseinstellungen
- Teil 7: Aktualisieren von Intel-Chipsatz-Treibern für neue Instance-Typen
- (Alternativ) Aktualisieren der AWS-PV-, ENA- und NVMe-Treiber mit AWS Systems Manager

Bevor Sie beginnen

Bei diesem Verfahren wird davon ausgegangen, dass Sie eine Xen-basierte Instance, z. B. eine M4 oder C4, haben und auf eine Nitro-basierte Instance migrieren.

Sie müssen PowerShell Version 3.0 oder höher verwenden, um das Upgrade erfolgreich durchzuführen.

> **Note**
>
> Bei der Migration können die statischen IP- oder benutzerdefinierten DNS-Netzwerkeinstellungen auf der vorhandenen Netzwerkkarte verloren gehen, da die Instance standardmäßig auf ein neues Enhanced-Networking-Adapter-Gerät umgestellt wird.

Bevor Sie die Schritte in diesem Verfahren durchführen, empfehlen wir das Erstellen eines Backups der Instance. Wählen Sie in der EC2-Konsole die Instance aus, die die Migration benötigt, und öffnen Sie das Kontextmenü (rechte Maustaste), wählen Sie die Option Instance-Status und dann Stopp.

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Um Daten auf Instance-Speicher-Volumes zu erhalten, stellen Sie sicher, dass Sie die Daten in einem persistenten Speicher sichern.

Öffnen Sie das Kontextmenü (rechte Maustaste) für die Instance in der EC2-Konsole, wählen Sie die Option Image und dann Image erstellen.

> **Note**
>
> Die Teile 4 und 5 dieser Anweisungen können nach der Migration oder Änderung des Instance-Typs abgeschlossen werden. Wir empfehlen jedoch den Abschluss vor der Migration, wenn Sie spezifisch zu einem Bare-Metal-Instance-Typ migrieren.

Teil 1: Installieren und aktualisieren von AWS PV-Treibern

Obwohl in Nitro System keine AWS PV-Treiber verwendet werden, sollten Sie sie dennoch aktualisieren, wenn Sie frühere Versionen von Citrix PV oder AWS PV verwenden. Die neuesten AWS PV-Treiber beheben Bugs in früheren Versionen der Treiber, die möglicherweise im Nitro-System auftreten oder falls Sie zurück zu einer Xen-basierten Instance migrieren. Als bewährte Methode empfehlen wir stets die Aktualisierung auf die neuesten Treiber für Windows-Instances bei AWS.

Führen Sie die folgenden Schritte aus, um ein direktes Upgrade der AWS PV-Treiber oder ein Upgrade von Citrix PV-Treibern auf AWS PV-Treiber unter Windows Server 2008 R2, Windows

Server 2012, Windows Server 2012 R2, Windows Server 2016 oder Windows Server 2019 durchzuführen. Weitere Informationen finden Sie unter Upgrade von PV-Treibern auf EC2-Windows-Instances.

Informationen zum Upgrade eines Domain-Controllers finden Sie unter Upgrade für einen Domain-Controller (AWS PV-Upgrade).

So führen Sie ein Upgrade von oder auf AWS PV-Treiber durch

1. Stellen Sie über Remote Desktop eine Verbindung mit der Instance her und bereiten Sie die Instance für das Upgrade vor. Schalten Sie den Systemdatenträger offline, bevor Sie das Upgrade durchführen. Wenn Sie eine direkte Aktualisierung der AWS PV-Treiber durchführen, ist dieser Schritt nicht erforderlich. Setzen Sie die Start-Option für alle nicht erforderlichen Services in der Services-Konsole auf Manual.
2. Laden Sie das aktuelle Treiberpaket in die Instance herunter.
3. Extrahieren Sie den Inhalt des Ordners und führen Sie die Datei au `AWSPVDriverSetup.msi`.

Wenn Sie die MSI-Datei ausgeführt haben, wird die Instance automatisch neu gestartet und das Upgrade des Treibers durchgeführt. Die Instance kann für die Dauer von bis zu 15 Minuten nicht verfügbar sein.

Wenn das Upgrade abgeschlossen wurde und die Instance beide Zustandsprüfungen in der Amazon EC2-Konsole bestanden hat, stellen Sie über Remote Desktop eine Verbindung mit der Instance her und prüfen Sie, ob der neue Treiber installiert wurde. Suchen Sie im Geräte-Manager unter Storage Controllers den AWS PV Storage Host Adapter. Vergewissern Sie sich, dass die Treiberversion identisch mit der aktuellen Version in der Tabelle für den Treiber-Versionsverlauf ist. Weitere Informationen finden Sie unter AWS PV-Treiber – Paketverlauf.

Teil 2: Installieren und aktualisieren von ENA

Führen Sie ein Upgrade auf den Elastic Network Adapter-Treiber durch, um sicherzustellen, dass alle Netzwerkfeatures unterstützt werden. Wenn Sie Ihre Instance gestartet haben und sie nicht über ein bereits aktiviertes erweitertes Netzwerk verfügt, müssen Sie den erforderlichen Netzwerkadaptertreiber auf Ihre Instance herunterladen und installieren. Setzen Sie dann das Attribut der enaSupport-Instance auf activate enhanced networking. Sie können dieses Attribut nur aus unterstützten Instance-Typen und nur bei installiertem ENA-Treiber aktivieren. Weitere Informationen finden Sie unter Ermöglichen Sie Enhanced Networking mit ENA auf Ihren EC2 Instances.

1. Laden Sie den aktuellen Treiber in die Instance herunter. Wenn Sie eine frühere Version des Treibers benötigen, finden Sie weitere Informationen unter Versionsverlauf für den ENA-Windows-Treiber.
2. Extrahieren Sie die ZIP-Datei.
3. Installieren Sie den Treiber, indem Sie das `install.ps1`-PowerShell-Skript im extrahierten Ordner ausführen.

   > **Note**
   >
   > Führen Sie das `install.ps1`-Skript als Administrator aus, um Fehler bei der Installation zu vermeiden.

4. Überprüfen Sie, ob für Ihr AMI enaSupport aktiviert ist. Wenn nicht, fahren Sie fort, indem Sie der Dokumentation in folge Ermöglichen Sie Enhanced Networking mit ENA auf Ihren EC2 Instances.

Teil 3: Aktualisieren von AWS NVMe-Treibern

AWS-NVMe-Treiber werden für die Interaktion mit Amazon-EBS- und SSD-Instance-Speicher-Volumes verwendet, die im Nitro-System zur Verbesserung der Leistung als NVMe-Blockgeräte verfügbar gemacht werden.

> **Important**
>
> Die folgenden Anweisungen wurden speziell für den Fall geändert, dass Sie AWS-NVMe auf einer Xen-basierten Instance installieren oder aktualisieren, um die Instance auf eine Nitro-basierte Instance zu migrieren.

1. Laden Sie das aktuelle Treiberpaket in die Instance herunter.

   Wenn Sie eine frühere Version des Treibers benötigen, finden Sie Informationen in NVMe-Windows-Treiberversionen zu den unterstützten Versionen.
2. Extrahieren Sie die ZIP-Datei.
3. Installieren Sie den Treiber wie in `Readme.txt` beschrieben.
4. Öffnen Sie eine PowerShell-Sitzung und führen Sie den folgenden Befehl aus:

```
PS C:\> start rundll32.exe sppnp.dll,Sysprep_Generalize_Pnp -wait
```

> **Note**
>
> Um den Befehl anzuwenden, müssen Sie die PowerShell-Sitzung als Administrator ausführen. PowerShell(x86)-Versionen führen zu einem Fehler.
> Dieser Befehl führt nur sysprep auf den Gerätetreibern aus. Es wird nicht die gesamte Sysprep-Vorbereitung ausgeführt.

5. Fahren Sie für Windows Server 2008 R2 und Windows Server 2012 die Instance herunter, ändern Sie den Instance-Typ und starten Sie diese. Fahren Sie dann mit Teil 4 fort. Wenn Sie die Instance vor der Migration auf einen Nitro-basierten Instance-Typ erneut auf einem Xen-basierten Instance-Typ starten, wird sie nicht gebootet. Bei anderen unterstützten Windows-AMIs können Sie den Instance-Typ nach dem sysprep-Befehl für das Gerät jederzeit ändern.

Teil 4: Aktualisieren von EC2Config und EC2Launch

Für Windows-Instances bieten EC2Config und EC2Launch zusätzliche Funktionen und Informationen bei Ausführung im Nitro-System, einschließlich EC2 Bare Metal. Der EC2Config-Service ist standardmäßig in AMIs für Windows Server-Versionen vor Windows Server 2016 enthalten. EC2Launch ersetzt den EC2Config-Service auf AMIs mit Windows Server 2016 und höher.

Wenn der EC2Config- und der EC2Launch-Service aktualisiert werden, verfügen neue Windows-AMIs in AWS über die aktuelle Version des Service. Sie müssen jedoch Ihre eigenen Windows-AMIs und Instances mit der aktuellen Version von EC2Config und EC2Launch aktualisieren.

So installieren oder aktualisieren Sie EC2Config

1. Laden Sie das EC2Config-Installationsprogramm herunter und entzippen Sie es.
2. Führen Sie `EC2Install.exe`. Eine vollständige Liste der verfügbaren Optionen erhalten Sie, wenn Sie `EC2Install` mit der Option `/?` ausführen. Standardmäßig werden Eingabeaufforderungen angezeigt. Um den Befehl ohne Eingabeaufforderungen auszuführen, verwenden Sie die Option `/quiet`.

Weitere Informationen finden Sie unter Installieren der neuesten Version von EC2Config.

So installieren oder aktualisieren Sie EC2Launch

1. Wenn Sie EC2Launch bereits auf einer Instance installiert und konfiguriert haben, erstellen Sie ein Backup der EC2Launch-Konfigurationsdatei. Beim Installationsprozess werden Änderungen an dieser Datei nicht übernommen. Standardmäßig befindet sich die Datei im Verzeichnis `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. Laden Sie die Datei EC2-Windows-Launch.zip in ein Verzeichnis auf der Instance herunter.
3. Laden Sie die Datei install.ps1 in dasselbe Verzeichnis herunter, in das Sie `EC2-Windows-Launch.zip` heruntergeladen haben.
4. Führen Sie `install.ps1`.

   > **Note**
   >
   > Führen Sie das `install.ps1`-Skript als Administrator aus, um Fehler bei der Installation zu vermeiden.

5. Wenn Sie ein Backup der EC2Launch-Konfigurationsdatei erstellt haben, kopieren Sie sie in das Verzeichnis `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Weitere Informationen finden Sie unter Den EC2Launch-v1-Agenten verwenden, um Aufgaben während des Starts einer EC2-Windows-Instance auszuführen.

Teil 5: Installieren des Treibers für den seriellen Port für Bare Metal-Instances

Der `i3.metal`-Instance-Typ nutzt anstelle eines auf dem I/O-Port basierenden seriellen Geräts ein PCI-basiertes serielles Gerät. Die neuesten Windows-AMIs verwenden automatisch PCI-basierte serielle Geräte und haben den Treiber für den seriellen Port installiert. Falls Sie keine Instance verwenden, die über eine von Amazon bereitgestellte Windows-AMI mit Datum vom 2018.04.11 oder später gestartet wurde, müssen Sie den Treiber für den seriellen Port installieren, um das serielle Gerät für EC2-Features zu aktivieren, wie etwa Passwortgenerierung und Konsolenausgabe. Die neuesten EC2Config- und EC2Launch-Utilities unterstützen auch i3.metal und bieten zusätzliche Funktionen. Folgen Sie den Schritten in Teil 4, wenn Sie dies noch nicht getan haben.

So installieren Sie den Treiber für die serielle Schnittstelle

1. Laden Sie das Paket für den seriellen Treiber in die Instance herunter.

2. Extrahieren Sie die Inhalte des Ordners, klicken Sie mit der rechten Maustaste auf `aws_ser.INF` und wählen Sie Installieren aus.
3. Klicken Sie auf Okay.

Teil 6: Aktualisieren der Energieverwaltungseinstellungen

Mit der folgenden Aktualisierung werden die Energiespareinstellungen so konfiguriert, dass Bildschirme nie ausgeschaltet werden. So kann das Betriebssystem auf Nitro-Systemen korrekt heruntergefahren werden. Alle von Amazon seit 2018.11.28 bereitgestellten Windows-AMIs verfügen bereits über diese Standardkonfiguration.

1. Öffnen Sie eine Eingabeaufforderung oder PowerShell-Sitzung.
2. Führen Sie die folgenden Befehle aus:

```
powercfg /setacvalueindex 381b4222-f694-41f0-9685-ff5bb260df2e 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex a1841308-3541-4fab-bc81-f71556f20b4a 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
```

Teil 7: Aktualisieren von Intel-Chipsatz-Treibern für neue Instance-Typen

Bei den Instance-Typen `u-6tb1.metal`, `u-9tb1.metal` und `u-12tb1.metal` wird Hardware verwendet, für die Chipsatz-Treiber erforderlich sind, die zuvor nicht auf Windows-AMIs installiert waren. Falls Sie keine Instance verwenden, die über ein von Amazon bereitgestelltes Windows-AMI mit der Datumsangabe 2018.11.19 oder später gestartet wurde, müssen Sie die Treiber mit Intel Chipset INF Utility installieren.

So installieren Sie die Chipsatz-Treiber

1. Chipsatz-INF-Hilfsprogramm für die Instance.
2. Extrahieren Sie die Dateien.
3. Führen Sie `SetupChipset.exe`.
4. Akzeptieren Sie die Software-Lizenzvereinbarung von Intel und installieren Sie die Chipsatz-Treiber.
5. Starten Sie die Instance neu.

(Alternativ) Aktualisieren der AWS-PV-, ENA- und NVMe-Treiber mit AWS Systems Manager

Das Automatisierungsdokument `AWSSupport-UpgradeWindowsAWSDrivers` automatisiert die in Teil 1, Teil 2 und Teil 3 beschriebenen Schritte. Diese Methode kann auch eine Instance reparieren, bei der die Treiber-Upgrades fehlgeschlagen sind.

Das Automatisierungsdokument `AWSSupport-UpgradeWindowsAWSDrivers` aktualisiert oder repariert AWS Speicher- und Netzwerktreiber in der angegebenen EC2-Instance. Das Dokument versucht, die neuesten Versionen der AWS-Treiber online zu installieren, indem es AWS Systems Manager Agent (SSM Agent) aufruft. Wenn SSM Agent nicht erreichbar ist, kann das Dokument auf ausdrückliche Anforderung eine Offline-Installation der AWS-Treiber durchführen.

> **Note**
>
> Dieses Verfahren schlägt auf einem Domain-Controller fehl. Weitere Informationen zum Aktualisieren der Treiber auf einem Domain-Controller finden Sie unter Upgrade für einen Domain-Controller (AWS PV-Upgrade).

So aktualisieren Sie die AWS PV-, ENA- und NVMe-Treiber automatisch mit AWS Systems Manager

1. Öffnen Sie die Systems Manager-Konsole unter https://console.aws.amazon.com/systems-manager.
2. Wählen Sie Automation und dann Execute Automation.
3. Suchen Sie nach dem Automatisierungsdokument AWSSupport-UpgradeWindowsAWSDrivers, wählen Sie es aus und wählen Sie dann Automatisierung ausführen aus.
4. Konfigurieren Sie im Abschnitt Eingabeparameter die folgenden Optionen:

   Instance-ID

   Geben Sie die eindeutige ID der zu aktualisierenden Instance ein.

   AllowOffline

   (Optional) Wählen Sie eine der folgenden Optionen:

   - `True` — Wählen Sie diese Option, um eine Offline-Installation durchzuführen. Die Instance wird während des Upgrade-Prozesses gestoppt und neu gestartet.

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Um Daten auf Instance-Speicher-Volumes zu erhalten, stellen Sie sicher, dass Sie die Daten in einem persistenten Speicher sichern.

- `False` — (Default (Standard)) Lassen Sie diese Option aktiviert. um eine Online-Installation durchzuführen. Die Instance wird während des Upgrade-Prozesses neu gestartet.

> **Important**
>
> Online- und Offline-Upgrades erstellen ein AMI, bevor sie den Upgrade-Vorgang durchführen. Das AMI bleibt auch nach Abschluss der Automatisierung erhalten. Sichern Sie sich Ihren Zugriff auf das AMI oder löschen Sie es, wenn es nicht mehr benötigt wird.

SubnetId

(Optional) Geben Sie einen der folgenden Werte ein:

- `SelectedInstanceSubnet` (Default (Standard)) Der Upgrade-Prozess startet die Instance helper im selben Subnetz wie die zu aktualisierende Instance. Das Subnetz muss die Kommunikation zu den Systems Manager-Endpunkten () ermöglic (`ssm.*`).
- `CreateNewVPC` — Der Upgrade-Prozess startet die Instance helper in einer neuen VPC. Verwenden Sie diese Option, wenn Sie nicht sicher sind, ob das Subnetz der Ziel-Instance die Kommunikation mit den `ssm.*`-Endpunkten zulässt. Ihr -Benutzer muss die Berechtigung haben, eine VPC zu erstellen.
- Eine bestimmte Subnetz-ID — Geben Sie die ID eines bestimmten Subnetzes an, in dem die Instance helper gestartet werden soll. Das Subnetz muss sich in der gleichen Availability Zone wie die zu aktualisierende Instance befinden und die Kommunikation mit den `ssm.*`-Endpunkten ermöglichen.

5. Wählen Sie Ausführen.
6. Warten Sie auf den Abschluss des Upgrades. Es kann bis zu 10 Minuten dauern, ein Online-Upgrade durchzuführen. Es kann bis zu 25 Minuten dauern, ein Offline-Upgrade durchzuführen.

Problembehandlung bei einem Betriebssystem-Upgrade auf einer EC2-Windows-Instance

AWS stellt Upgrade-Unterstützung für Fehler oder Probleme mit dem Upgrade Helper Service bereit, einem AWS-Dienstprogramm, mit dem Sie direkte Upgrades mit Citrix PV-Treibern ausführen können.

Nach dem Upgrade verzeichnet die Instance möglicherweise eine überdurchschnittlich hohe CPU-Nutzung, während der .NET Runtime Optimization Service das .Net Framework optimiert. Dieses Verhalten wird erwartet.

Wenn die Instance nach einigen Stunden noch nicht alle Statusprüfungen erfolgreich bestanden hat, überprüfen Sie Folgendes.

- Wenn Sie ein Upgrade auf Windows Server 2008 vorgenommen haben und nach einigen Stunden alle Statusprüfungen fehlschlagen, ist das Upgrade möglicherweise fehlgeschlagen und der Prompt Wählen Sie OK wird zum Bestätigen des Zurücksetzens angezeigt. Da in diesem Status nicht auf die Konsole zugegriffen werden kann, ist es nicht möglich, auf die Schaltfläche zu klicken. Führen Sie einen Neustart über die Amazon EC2-Konsole oder API aus, um dies zu umgehen. Die Initiierung des Neustarts dauert zehn Minuten oder länger. Die Instance ist möglicherweise nach 25 Minuten verfügbar.
- Entfernen Sie Anwendungen oder Serverrollen vom Server und versuchen Sie es erneut.

Wenn die Instance nach dem Entfernen der Anwendungen oder Serverrollen vom Server nicht alle Statusprüfungen erfolgreich besteht, führen Sie die folgenden Schritte aus.

- Beenden Sie die Instance und fügen Sie das Stamm-Volume an eine andere Instance an. Weitere Informationen finden Sie in der Beschreibung zum Beenden und Anfügen des Stamm-Volumes an eine andere Instance in Warten auf Metadaten-Service.
- Analysieren Sie die Windows-Setup-Protokolldateien und -Ereignisprotokolle hinsichtlich Fehlern.

Bei anderen Fehlern oder Problemen mit einem Betriebssystem-Upgrade oder der Migration empfehlen wir die Lektüre der in aufgelisteten Artike Bevor Sie ein direktes Upgrade beginnen.

Tutorial: Verbinden einer Amazon-EC2-Instance mit einer Amazon-RDS-Datenbank

Tutorial-Ziel

Ziel dieses Tutorials ist es, zu lernen, wie Sie eine sichere Verbindung zwischen einer Amazon-EC2-Instance und einer Amazon-RDS-Datenbank mithilfe der AWS-Managementkonsole konfigurieren.

Es gibt verschiedene Möglichkeiten, die Verbindung zu konfigurieren. In diesem Tutorial untersuchen wir die folgenden drei Optionen:

- Option 1: Automatisches Verbinden einer Instance mit einer RDS-Datenbank über die EC2-Konsole

  Verwenden Sie das automatische Verbindungsfeature in der EC2-Konsole, um die Verbindung zwischen Ihrer EC2-Instance und Ihrer RDS-Datenbank automatisch zu konfigurieren, um Datenverkehr zwischen der EC2-Instance und der RDS-Datenbank zuzulassen.
- Option 2: Automatisches Verbinden einerInstance mit einer RDS-Datenbank mithilfe der RDS-Konsole

  Verwenden Sie das automatische Verbindungsfeature in der RDS-Konsole, um die Verbindung zwischen Ihrer EC2-Instance und Ihrer RDS-Datenbank automatisch zu konfigurieren, um Datenverkehr zwischen der EC2-Instance und der RDS-Datenbank zuzulassen.
- Option 3: Manuelles Verbinden einer Instance mit einer RDS-Datenbank, durch Erstellen von Sicherheitsgruppen

  Konfigurieren Sie die Verbindung zwischen Ihrer EC2-Instance und Ihrer RDS-Datenbank, indem Sie die Sicherheitsgruppen manuell konfigurieren und zuweisen. Damit reproduzieren Sie die Konfiguration, die durch das automatische Verbindungsfeature in Option 1 und Option 2 automatisch erstellt wird.

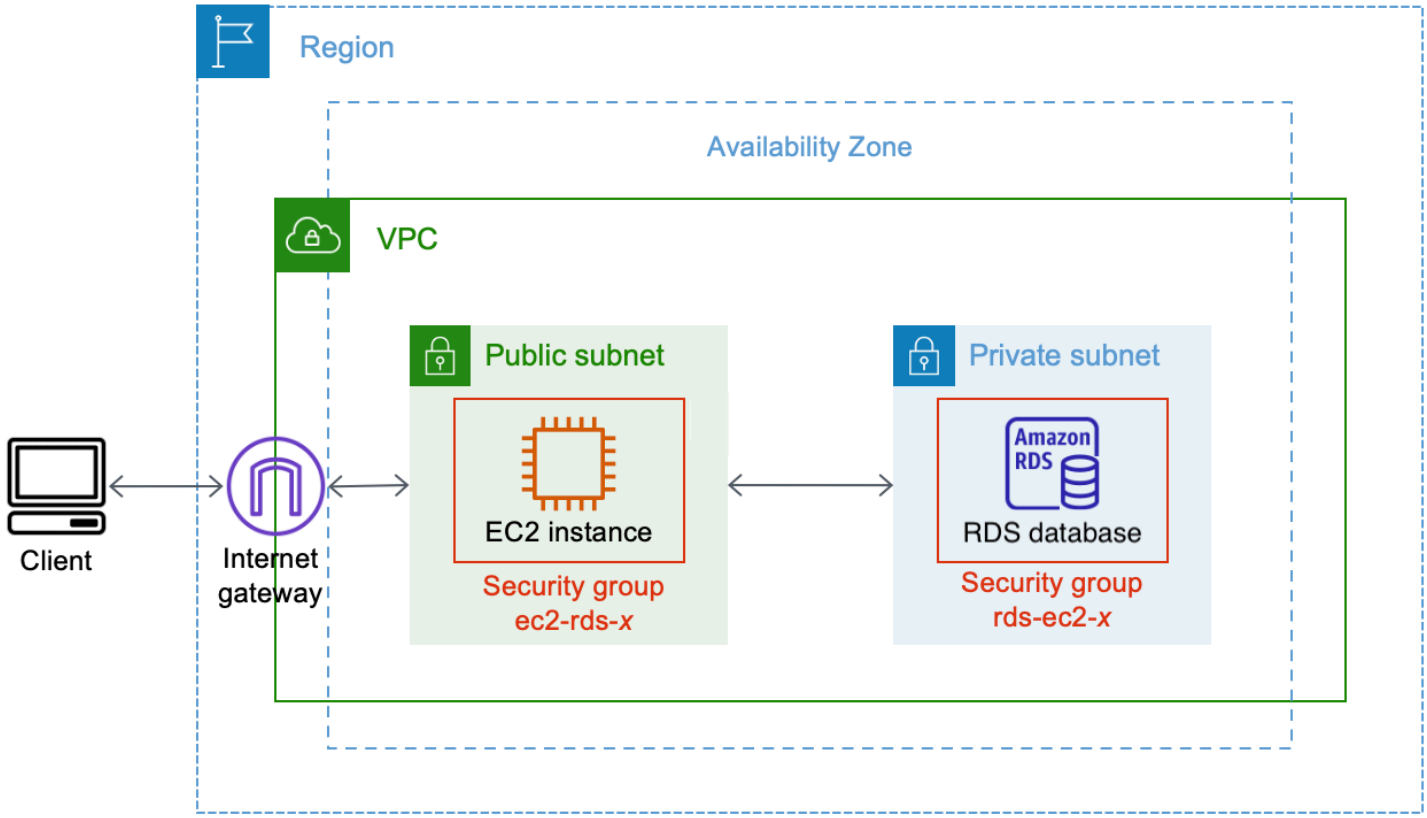
Kontext

Als Kontext dafür, warum Sie eine Verbindung zwischen Ihrer EC2-Instance und einer RDS-Datenbank konfigurieren möchten, betrachten wir das folgende Szenario: Ihre Website zeigt Ihren Benutzern ein Formular zum Ausfüllen an. Sie müssen die Formulardaten in einer Datenbank erfassen. Sie können Ihre Website auf einer EC2-Instance hosten, die als Webserver konfiguriert wurde, und Sie können die Formulardaten in einer RDS-Datenbank erfassen. Die EC2-Instance und

die RDS-Datenbank müssen miteinander verbunden sein, damit die Formulardaten von der EC2-Instance in die RDS-Datenbank übertragen werden können. In diesem Tutorial wird erklärt, wie Sie diese Verbindung konfigurieren. Beachten Sie, dass dies nur ein Beispiel für einen Anwendungsfall zum Verbinden einer EC2-Instance und einer RDS-Datenbank ist.

Architektur

Das folgende Diagramm zeigt die erstellten Ressourcen und die architektonische Konfiguration, die sich aus der Ausführung aller Schritte in diesem Tutorial ergibt.



Das Diagramm veranschaulicht die folgenden Ressourcen, die Sie erstellen werden:

- Sie erstellen eine EC2-Instance und eine RDS-Datenbank in derselben AWS-Region, VPC und Availability Zone.
- Sie erstellen die EC2-Instance in einem öffentlichen Subnetz.
- Sie erstellen die RDS-Datenbank in einem privaten Subnetz.

  Wenn Sie die RDS-Konsole verwenden, um die RDS-Datenbank zu erstellen und die EC2-Instance automatisch zu verbinden, werden die VPC, die DB-Subnetzgruppe und die Einstellungen für

den öffentlichen Zugriff für die Datenbank automatisch ausgewählt. Die RDS-Datenbank wird automatisch in einem privaten Subnetz innerhalb derselben VPC wie die EC2-Instance erstellt.

- Internetbenutzer können sich mithilfe von SSH oder HTTP/HTTPS über ein Internet-Gateway mit der EC2-Instance verbinden.
- Internetbenutzer können keine direkte Verbindung mit der RDS-Datenbank herstellen. Nur die EC2-Instance ist mit der RDS-Datenbank verbunden.
- Wenn Sie das automatische Verbindungsfeature verwenden, um Datenverkehr zwischen der EC2-Instance und der RDS-Datenbank zuzulassen, werden die folgenden Sicherheitsgruppen automatisch erstellt und hinzugefügt:
  - Die Sicherheitsgruppe ec2-rds- ***x*** wird erstellt und der EC2-Instance hinzugefügt. Es verfügt über eine ausgehende Regel, die auf die Sicherheitsgruppe rds-ec2-***x*** als Ziel verweist. Dadurch kann der Datenverkehr von der EC2-Instance die RDS-Datenbank mit der Sicherheitsgruppe rds-ec2-***x*** erreichen.
  - Die Sicherheitsgruppe rds-ec2-***x*** wird erstellt und der RDS-Datenbank hinzugefügt. Es verfügt über eine eingehende Regel, die auf die Sicherheitsgruppe ec2-rds-***x*** als Quelle verweist. Dadurch kann der Datenverkehr von der EC2-Instance mit der Sicherheitsgruppe ec2-rds-***x*** die RDS-Datenbank erreichen.

  Durch die Verwendung getrennter Sicherheitsgruppen (eine für die EC2-Instance und eine für die RDS-Datenbank) haben Sie eine bessere Kontrolle über die Sicherheit der Instance und der Datenbank. Wenn Sie dieselbe Sicherheitsgruppe sowohl für die Instance als auch für die Datenbank verwenden und dann die Sicherheitsgruppe beispielsweise nur für die Datenbank anpassen würden, würde sich die Änderung sowohl auf die Instance als auch auf die Datenbank auswirken. Mit anderen Worten, wenn Sie eine Sicherheitsgruppe verwenden würden, könnten Sie unbeabsichtigt die Sicherheit einer Ressource (entweder der Instance oder der Datenbank) ändern, da Sie vergessen haben, dass die Sicherheitsgruppe an sie angefügt war.

  Die Sicherheitsgruppen, die automatisch erstellt werden, respektieren auch die geringsten Berechtigungen, da sie nur die gegenseitige Verbindung für diesen Workload auf dem Datenbankport zulassen, indem sie ein Workload-spezifisches Sicherheitsgruppenpaar erstellen.

Überlegungen

Beachten Sie bei Durchführung der Aufgaben in diesem Tutorial Folgendes:

- Two consoles (Zwei Konsolen) – Sie werden die folgenden zwei Konsolen für dieses Tutorial verwenden:
  - Amazon-EC2-Konsole – Sie verwenden die EC2-Konsole zum Starten von Instances, zum automatischen Verbinden einer EC2-Instance mit einer RDS-Datenbank und für die manuelle Option zum Konfigurieren der Verbindung durch Erstellen der Sicherheitsgruppen.
  - Amazon-RDS-Konsole – Sie verwenden die RDS-Konsole, um eine RDS-Datenbank zu erstellen und eine EC2-Instance automatisch mit einer RDS-Datenbank zu verbinden.
- One VPC (Eine VPC) – Um das automatische Verbindungsfeature zu verwenden, müssen sich Ihre EC2-Instance und Ihre RDS-Datenbank in derselben VPC befinden.

  Wenn Sie die Verbindung zwischen Ihrer EC2-Instance und Ihrer RDS-Datenbank manuell konfigurieren, können Sie Ihre EC2-Instance in einer VPC und Ihre RDS-Datenbank in einer anderen VPC starten. Allerdings müssen Sie zusätzliches Routing und eine VPC-Konfiguration einrichten. Dieses Szenario wird in diesem Tutorial nicht behandelt.
- EineAWS-Region – Die EC2-Instance und die RDS-Datenbank müssen sich in derselben Region befinden.
- Two security groups (Zwei Sicherheitsgruppen) – Die Verbindung zwischen der EC2-Instance und der RDS-Datenbank wird durch zwei Sicherheitsgruppen konfiguriert – eine Sicherheitsgruppe für Ihre EC2-Instance und eine Sicherheitsgruppe für Ihre RDS-Datenbank.

  Wenn Sie das automatische Verbindungsfeature in der EC2-Konsole oder RDS-Konsole verwenden, um die Verbindung zu konfigurieren (Option 1 und Option 2 dieses Tutorials), werden die Sicherheitsgruppen automatisch erstellt und der EC2-Instance und RDS-Datenbank zugewiesen.

  Wenn Sie das automatische Verbindungsfeature nicht verwenden, müssen Sie die Sicherheitsgruppen manuell erstellen und zuweisen. Sie tun dies in Option 3 dieses Tutorials.

Zeit zur Absolvierung des Tutorials

30 Minuten

Sie können das gesamte Tutorial in einer Sitzung abschließen oder eine Aufgabe nach der anderen erledigen.

Kosten

Bei Absolvierung dieses Tutorials können Kosten für die von Ihnen erstellten AWS-Ressourcen anfallen.

Sie können Amazon EC2 mit dem kostenlosen Kontingent verwenden, sofern Ihr AWS-Konto für das kostenlose Kontingent berechtigt ist und Sie Ihre Ressourcen gemäß den Anforderungen des kostenlosen Kontingents konfigurieren. Weitere Informationen finden Sie unter ., Vorteile des kostenlosen Kontingents vor und nach dem 15. Juli 2025.

Wenn sich Ihre EC2-Instance und Ihre RDS-Datenbank in unterschiedlichen Availability Zones befinden, fallen Datenübertragungsgebühren an. Um diese Gebühren zu vermeiden, müssen sich die EC2-Instance und die RDS-Datenbank in derselben Availability Zone befinden. Weitere Informationen zu den Datenübertragungsgebühren finden Sie unter Datenübertragung auf der Seite Amazon-EC2-On-Demand-Preise.

Um Kosten zu vermeiden, nachdem Sie das Tutorial abgeschlossen haben, löschen Sie die Ressourcen, wenn sie nicht mehr benötigt werden. Die Schritte zum Löschen der Ressourcen finden Sie unter Aufgabe 4 (Optional): Aufräumen.

Option 1: Automatisches Verbinden einer Instance mit einer RDS-Datenbank über die EC2-Konsole

Das Ziel von Option 1 ist es, das automatische Verbindungsfeature in der EC2-Konsole zu erkunden, die die Verbindung zwischen Ihrer EC2-Instance und der RDS-Datenbank automatisch konfiguriert, damit Datenverkehr von der EC2-Instance zur RDS-Datenbank zugelassen wird. In Option 3 erfahren Sie, wie Sie die Verbindung manuell konfigurieren.

Aufgaben

- Bevor Sie beginnen
- Aufgabe 1: (Optional) RDS-Datenbank erstellen
- Aufgabe 2: (Optional) EC2-Instance starten
- Aufgabe 3: Automatisches Verbinden Ihrer EC2-Instance mit Ihrer RDS-Datenbank
- Aufgabe 4: Überprüfen der Verbindungskonfiguration
- Aufgabe 5 (Optional): Aufräumen

Bevor Sie beginnen

Sie benötigen Folgendes, um dieses Tutorial abzuschließen:

- Eine RDS-Datenbank, die sich in derselben VPC wie die EC2-Instance befindet. Sie können entweder eine vorhandene RDS-Datenbank verwenden oder die Schritte in Aufgabe 1 ausführen, um eine neue RDS-Datenbank zu erstellen.
- Eine EC2-Instance, die sich in derselben VPC wie die RDS-Datenbank befindet. Sie können entweder eine vorhandene EC2-Instance verwenden oder die Schritte in Aufgabe 2 ausführen, um eine neue EC2-Instance zu erstellen.
- Berechtigungen zum Aufrufen der folgenden Operationen:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Aufgabe 1: (Optional) RDS-Datenbank erstellen

> **Note**
>
> Das Erstellen einer Amazon-RDS-Datenbank steht nicht im Mittelpunkt dieses Tutorials. Wenn Sie bereits über eine RDS-Datenbank verfügen und diese für dieses Tutorial verwenden möchten, können Sie diese Aufgabe überspringen.
> Wenn Sie eine vorhandene RDS-Datenbank verwenden, stellen Sie sicher, dass sie sich in derselben VPC wie Ihre EC2-Instance befindet, damit Sie das automatische Verbindungsfeature verwenden können.

Ziel dieser Aufgabe ist es, eine RDS-Datenbank zu erstellen, damit Sie Aufgabe 3 abschließen können, in der Sie die Verbindung zwischen Ihrer EC2-Instance und Ihrer RDS-Datenbank konfigurieren. Mit den Schritten in dieser Aufgabe wird die RDS-Datenbank wie folgt konfiguriert:

- Engine-Typ: MySQL
- Vorlage: Kostenloses Kontingent
- DB-Instance-Kennung: **`tutorial-database-1`**
- DB-Instance-Klasse: `db.t3.micro`

> **Important**
>
> In einer Produktionsumgebung sollten Sie Ihre Instance so konfigurieren, dass sie Ihren speziellen Anforderungen entspricht.

So erstellen Sie eine MySQL-RDS-Datenbank

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie in der Regionsauswahl (oben rechts) eine AWS-Region aus. Die Datenbank und die EC2-Instance müssen sich in derselben Region befinden, um das automatische Verbindungsfeature in der EC2-Konsole verwenden zu können.
3. Wählen Sie im Dashboard Create database (Datenbank erstellen) aus.
4. Überprüfen Sie unter Choose a database creation method (Datenbankerstellungsmethode auswählen), ob Standard create (Standarderstellung) ausgewählt ist. Wenn Sie Easy create (Einfache Erstellung) wählen, ist der VPC-Selektor nicht verfügbar. Sie müssen sicherstellen, dass sich Ihre Datenbank in derselben VPC wie Ihre EC2-Instance befindet, um das automatische Verbindungsfeature in der EC2-Konsole verwenden zu können.
5. Wählen Sie unter Engine options (Engine-Optionen) für Engine type (Engine-Typ) die Option MySQL aus.
6. Wählen Sie unter Templates (Vorlagen) eine Beispielvorlage aus, die Ihren Anforderungen entspricht. Wählen Sie für dieses Tutorial die Option Free tier (Kostenloses Kontingent), um kostenlos eine Datenbank zu erstellen. Beachten Sie jedoch, dass das kostenlose Kontingent nur für Konten verfügbar ist, die sich für das kostenlose Kontingent qualifizieren. Sie können mehr darüber erfahren, indem Sie auf den Info-Link im Feld Free tier (Kostenloses Kontingent) klicken.
7. Führen Sie unter Settings (Einstellungen) die folgenden Schritte aus:

a. Geben Sie unter DB instance identifier (DB-Instance-Kennung) einen Namen für die Datenbank ein. Geben Sie für dieses Tutorial ein **`tutorial-database-1`**.

b. Behalten Sie für Master username (Master-Benutzername) den Standardnamen **`admin`** bei.

c. Geben Sie unter Master password (Master-Passwort) ein Passwort ein, das Sie sich für dieses Tutorial merken können, und geben Sie dann unter Confirm password (Passwort bestätigen) das Passwort erneut ein.

8. Behalten Sie unter Instance-Konfiguration für DB-Instance-Klasse den Standardwert db.t3.micro bei. Wenn Ihr Konto für das kostenlose Kontingent berechtigt ist, können Sie diese Datenbankklasse kostenlos nutzen. Weitere Informationen finden Sie unter Kostenloses AWS-Kontingent.

9. Wählen Sie unter Connectivity (Verbindung) für Compute resource (Rechenressource) die Option Don't connect to an EC2 compute resource (Keine Verbindung zu einer EC2-Rechenressource herstellen) aus, da Sie die EC2-Instance und die RDS-Datenbank später in Aufgabe 3 miteinander verbinden werden.

   (Später, in Option 2 dieses Tutorials, werden Sie das automatische Verbindungsfeature in der RDS-Konsole ausprobieren, indem Sie Connect to an EC2 compute resource (Mit einer EC2-Rechenressource verbinden) auswählen.)

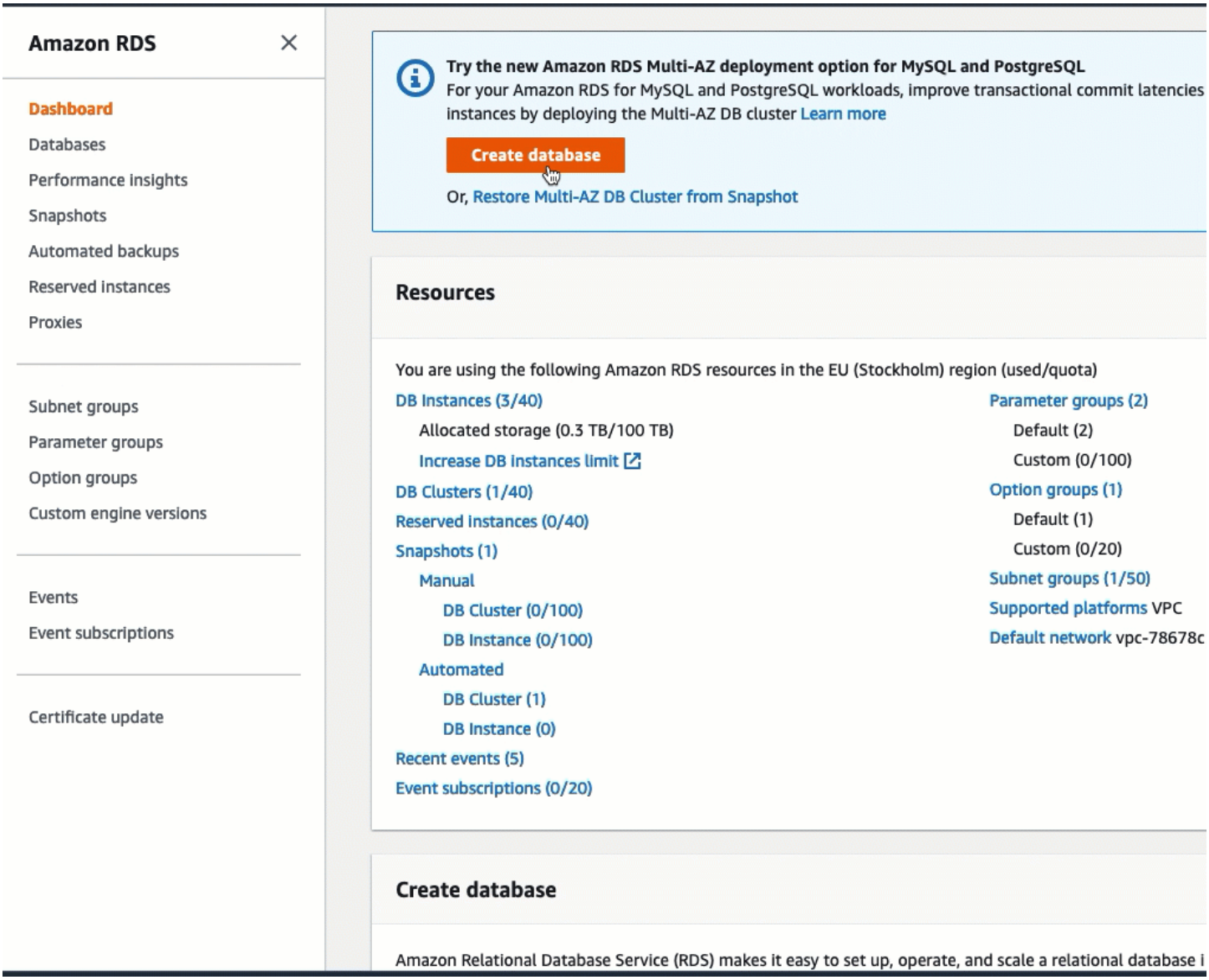
10. Wählen Sie unter Virtual Private Cloud (VPC) eine VPC aus. Die VPC muss über eine DB-Subnetzgruppe verfügen. Um das automatische Verbindungsfeature verwenden zu können, müssen sich Ihre EC2-Instance und die RDS-Datenbank in derselben VPC befinden.

11. Behalten Sie alle Standardwerte für die anderen Felder auf dieser Seite bei.

12. Wählen Sie Datenbank erstellen aus.

    Auf dem Bildschirm Databases (Datenbanken) lautet der Status der neuen Datenbank Creating (Wird erstellt), bis die Datenbank einsatzbereit ist. Wenn sich der Status in Available (Verfügbar) ändert, können Sie eine Verbindung zur Datenbank herstellen. Abhängig von der Klasse der Datenbank und vom verfügbaren Speicherplatz kann es bis zu 20 Minuten dauern, bis die neue Datenbank verfügbar ist.

Animation anzeigen: Erstellen einer RDS-Datenbank



Aufgabe 2: (Optional) EC2-Instance starten

> **Note**
>
> Das Starten einer Instance steht nicht im Mittelpunkt dieses Tutorials. Wenn Sie bereits über eine Amazon-EC2-Instance verfügen und diese in diesem Tutorial verwenden möchten, können Sie diese Aufgabe überspringen.
> Wenn Sie eine vorhandene EC2-Instance verwenden, stellen Sie sicher, dass sie sich in derselben VPC wie Ihre RDS-Datenbank befindet, damit Sie das automatische Verbindungsfeature verwenden können.

Ziel dieser Aufgabe ist es, eine EC2-Instance zu starten, damit Sie Aufgabe 3 abschließen können, in der Sie die Verbindung zwischen Ihrer EC2-Instance und Ihrer Amazon RDS-Datenbank konfigurieren. Mit den Schritten in dieser Aufgabe wird die EC2-Instance wie folgt konfiguriert:

- Instance-Name: **`tutorial-instance-1`**
- AMI: Amazon Linux 2
- Instance-Typ: `t2.micro`
- Öffentliche IP automatisch zuweisen: Aktiviert
- Sicherheitsgruppe mit den folgenden drei Regeln:
  - SSH von Ihrer IP-Adresse zulassen
  - HTTPS-Datenverkehr von überall zulassen
  - HTTP-Datenverkehr von überall zulassen

> **Important**
>
> In einer Produktionsumgebung sollten Sie Ihre Instance so konfigurieren, dass sie Ihren speziellen Anforderungen entspricht.

Starten Sie EC2-Instances wie folgt:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Regionsauswahl (oben rechts) eine AWS-Region aus. Die Datenbank und die EC2-Instance müssen sich in derselben Region befinden, um das automatische Verbindungsfeature in der EC2-Konsole verwenden zu können.
3. Wählen Sie im EC2-Dashboard die Option Launch Instance (Instance starten) aus.
4. Geben Sie unter Name and tags (Name und Tags) für Name einen Namen ein, um Ihre Instance zu identifizieren. Geben Sie für dieses Tutorial der Instance den Namen **`tutorial-instance-1`**. Der Instance-Name ist zwar nicht obligatorisch, aber wenn Sie Ihre Instance in der EC2-Konsole auswählen, können Sie sie anhand des Namens leicht identifizieren.
5. Wählen Sie unter Application and OS Images (Anwendungs- und Betriebssystem-Images) ein AMI aus, das Ihren Webserver-Anforderungen entspricht. Dieses Tutorial verwendet Amazon Linux 2.

6. Wählen Sie unter Instance type (Instance-Typ) für Instance type (Instance-Typ) einen Instance-Typ aus, der Ihren Webserver-Anforderungen entspricht. In diesem Tutorial wird ein verwendet `t2.micro`.

> **Note**
>
> Abhängig davon, wann Sie Ihr Konto erstellt haben, kann es sein, dass Sie Amazon EC2 im Rahmen des kostenlosen Kontingents verwenden können.
> Wenn Sie Ihr AWS-Konto vor dem 15. Juli 2025 erstellt haben und es weniger als 12 Monate alt ist, können Sie Amazon EC2 im kostenlosen Kontingent verwenden, indem Sie den Instance-Typ t2.micro auswählen, oder den Instance-Typ t3.micro in Regionen, in denen t2.micro nicht verfügbar ist. Beachten Sie, dass beim Starten einer t3.micro-Instance standardmäßig der Modus Unlimited verwendet wird, wodurch je nach CPU-Auslastung zusätzliche Gebühren anfallen können. Wenn ein Instance-Typ unter dem kostenlosen Kontingent berechtigt ist, ist er als Für das kostenlose Kontingent berechtigt gekennzeichnet.
> Wenn Sie Ihr AWS-Konto am oder nach dem 15. Juli 2025 erstellt haben, können Sie die Instance-Typen t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large und m7i-flex.large 6 Monate verwenden, oder bis Ihr Guthaben aufgebraucht ist.
> Weitere Informationen finden Sie unter Vorteile des kostenlosen Kontingents vor und nach dem 15. Juli 2025.

7. Wählen Sie unter Key pair (login) (Schlüsselpaar (Anmeldung)) für Key pair name (Schlüsselpaar-Name) Ihr Schlüsselpaar aus.
8. Führen Sie unter Network settings (Netzwerkeinstellungen) die folgenden Schritte aus:

   a. Wenn Sie für Network (Netzwerk) und Subnet (Subnetz) keine Änderungen an Ihrer Standard-VPC oder Ihren Subnetzen vorgenommen haben, können Sie die Standardeinstellungen beibehalten.

      Wenn Sie Änderungen an Ihrer Standard-VPC oder Ihren Subnetzen vorgenommen haben, überprüfen Sie Folgendes:

      i. Die Instance muss sich in derselben VPC wie die RDS-Datenbank befinden, um das automatische Verbindungsfeature verwenden zu können. Standardmäßig haben Sie nur eine VPC.

ii. Die VPC, in der Sie Ihre Instance starten, muss mit einem Internet-Gateway verbunden sein, damit Sie über das Internet auf Ihren Webserver zugreifen können. Ihre Standard-VPC wird automatisch mit einem Internet-Gateway eingerichtet.

iii. Um sicherzustellen, dass Ihre Instance eine öffentliche IP-Adresse erhält, überprüfen Sie für Auto-assign public IP (Automatische Zuweisung öffentlicher IP), dass Enable (Aktivieren) ausgewählt ist. Wenn Disable (Deaktivieren) ausgewählt ist, wählen Sie Edit (Bearbeiten) (rechts neben Network Settings (Netzwerkeinstellungen)) und dann für Auto-assign public IP (Öffentliche IP automatisch zuweisen) die Option Enable (Aktivieren) aus.

b. Um mithilfe von SSH eine Verbindung zu Ihrer Instance herzustellen, benötigen Sie eine Sicherheitsgruppenregel, die SSH- (Linux) oder RDP-Datenverkehr (Windows) von der öffentlichen IPv4-Adresse Ihres Computers autorisiert. Wenn Sie eine Instance starten, wird standardmäßig eine neue Sicherheitsgruppe mit einer Regel erstellt, die eingehenden SSH-Datenverkehr von überall zulässt.

   Um sicherzustellen, dass nur Ihre IP-Adresse eine Verbindung zu Ihrer Instance herstellen kann, wählen Sie unter (Firewall (Sicherheitsgruppen) in der Dropdown-Liste neben dem Kontrollkästchen SSH-Verkehr zulassen von die Option Meine IP aus.

c. Um Datenverkehr aus dem Internet zu Ihrer Instance zuzulassen, aktivieren Sie die folgenden Kontrollkästchen:

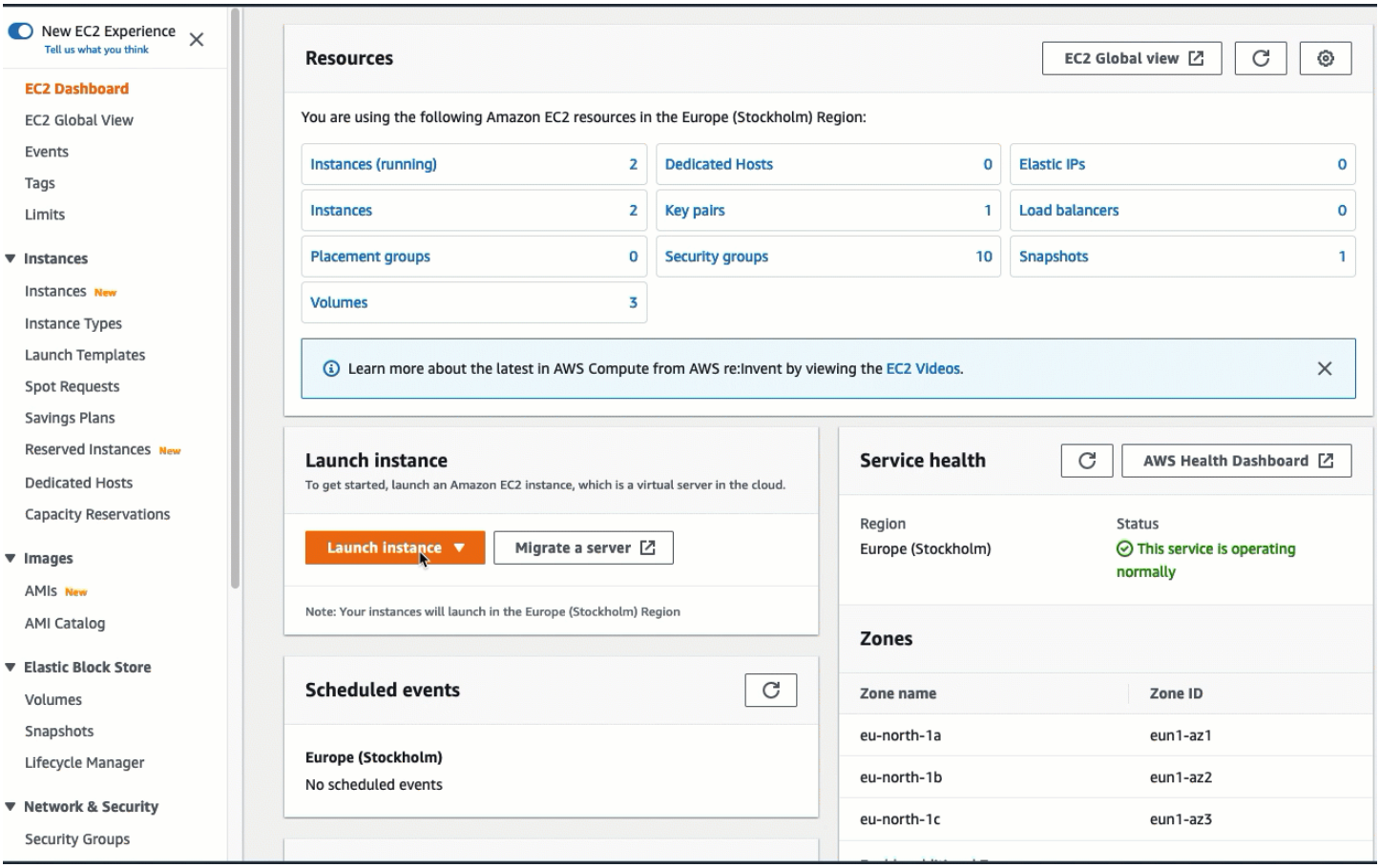
   - Allow HTTPs traffic from the internet (HTTPs-Datenverkehr aus dem Internet zulassen
   - Allow HTTP traffic from the internet (HTTP-Datenverkehr aus dem Internet zulassen

9. Überprüfen Sie im Bereich Summary (Übersicht) Ihre Instance-Konfiguration und wählen Sie dann Launch instance (Instance starten) aus.
10. Lassen Sie die Bestätigungsseite geöffnet. Sie benötigen es im nächsten Schritt, wenn Sie Ihre Instance automatisch mit Ihrer Datenbank verbinden.

    Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Fehlerbehebung bei Amazon-EC2-Instances.

Weitere Informationen über das Starten einer Instance finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten.

Animation anzeigen: Starten einer EC2-Instance



Aufgabe 3: Automatisches Verbinden Ihrer EC2-Instance mit Ihrer RDS-Datenbank

Ziel dieser Aufgabe ist es, das automatische Verbindungsfeature in der EC2-Konsole zu verwenden, um die Verbindung zwischen Ihrer EC2-Instance und Ihrer RDS-Datenbank automatisch zu konfigurieren.

So verbinden Sie eine EC2-Instance automatisch mit einer RDS-Datenbank mithilfe der EC2-Konsole

1. Wählen Sie auf der Bestätigungsseite für den Start der Instance (sie sollte von der vorherigen Aufgabe geöffnet sein) die Option Connect an RDS database (Mit einer RDS-Datenbank verbinden) aus.

   Wenn Sie die Bestätigungsseite geschlossen haben, gehen Sie wie folgt vor:

   a. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

   b. Wählen Sie im Navigationsbereich Instances aus.

c. Wählen Sie die EC2-Instance, die Sie gerade erstellt haben, und wählen Sie dann Actions (Aktionen), Networking (Netzwerk), Connect RDS database (RDS-Datenbank verbinden) aus.

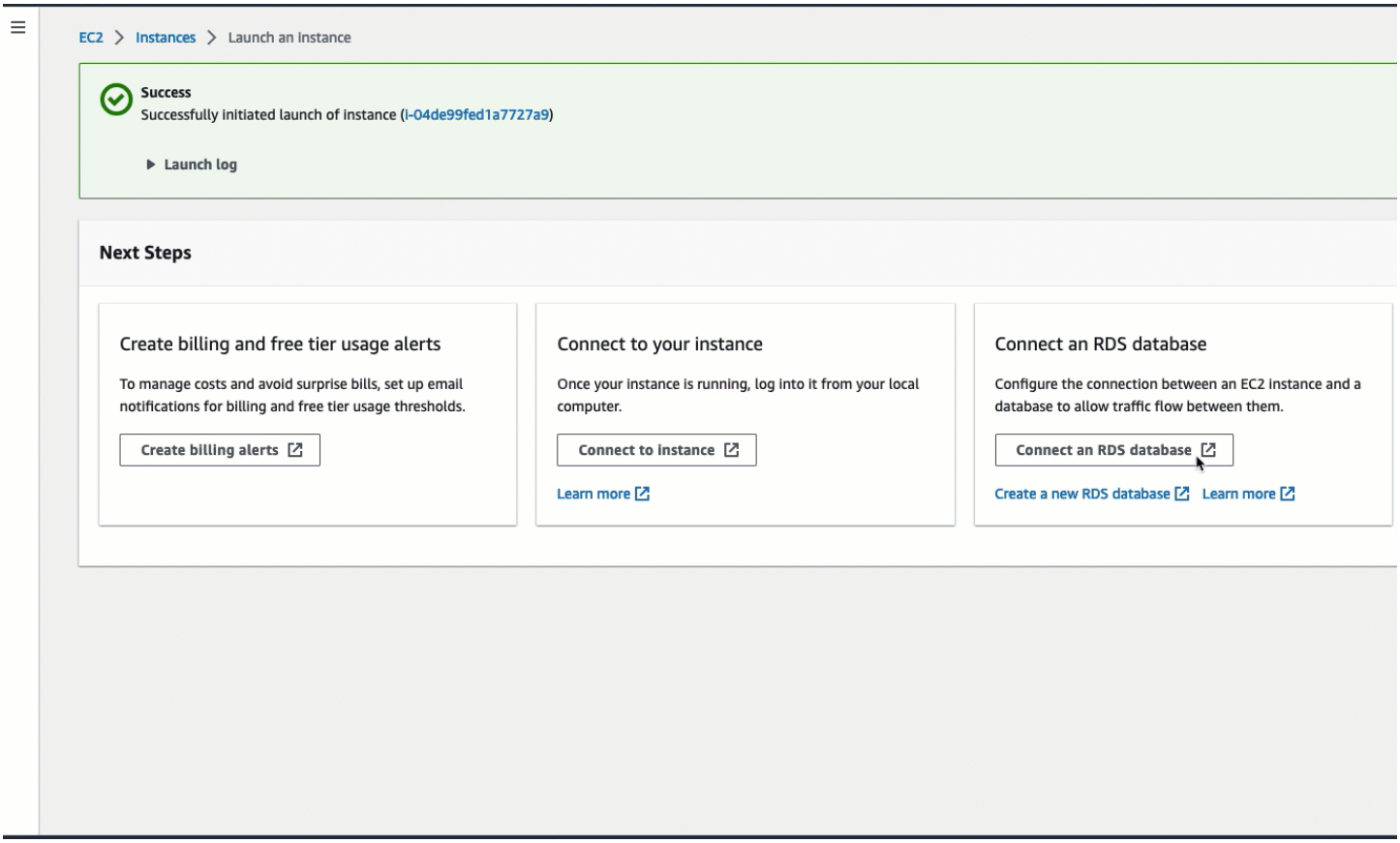
   Wenn Connect RDS database (RDS-Datenbank verbinden) nicht verfügbar ist, überprüfen Sie, ob sich die EC2-Instance im Status Running (Ausgeführt) befindet.

2. Wählen Sie für Database role (Datenbankrolle) die Option Instance aus. Instance bezieht sich in diesem Fall auf die Datenbank-Instance.
3. Wählen Sie unter RDS database (RDS-Datenbank) die RDS-Datenbank aus, die Sie in Aufgabe 1 erstellt haben.

> **Note**
>
> Die EC2-Instances und die RDS-Datenbank müssen sich in derselben VPC befinden, um eine Verbindung miteinander herzustellen.

4. Wählen Sie Connect aus.

Animation anzeigen: Automatisches Verbinden einer neu gestarteten EC2-Instance mit einer RDS-Datenbank



Aufgabe 4: Überprüfen der Verbindungskonfiguration

Ziel dieser Aufgabe ist es, zu überprüfen, ob die beiden Sicherheitsgruppen erstellt und der Instance und Datenbank zugewiesen wurden.

Wenn Sie das automatische Verbindungs-Feature in der RDS-Konsole verwenden, um die Verbindung zu konfigurieren, werden die Sicherheitsgruppen automatisch erstellt und der Instance und Datenbank wie folgt zugewiesen:

- Die Sicherheitsgruppe rds-ec2-*x* wird erstellt und der RDS-Datenbank hinzugefügt. Es verfügt über eine eingehende Regel, die auf die Sicherheitsgruppe ec2-rds-*x* als Quelle verweist. Dadurch kann der Datenverkehr von der EC2-Instance mit der Sicherheitsgruppe ec2-rds-*x* die RDS-Datenbank erreichen.
- Die Sicherheitsgruppe ec2-rds-*x* wird erstellt und der EC2-Instance hinzugefügt. Es verfügt über eine ausgehende Regel, die auf die Sicherheitsgruppe rds-ec2-*x* als Ziel verweist. Dadurch kann

der Datenverkehr von der EC2-Instance die RDS-Datenbank mit der Sicherheitsgruppe rds-ec2-*x* erreichen.

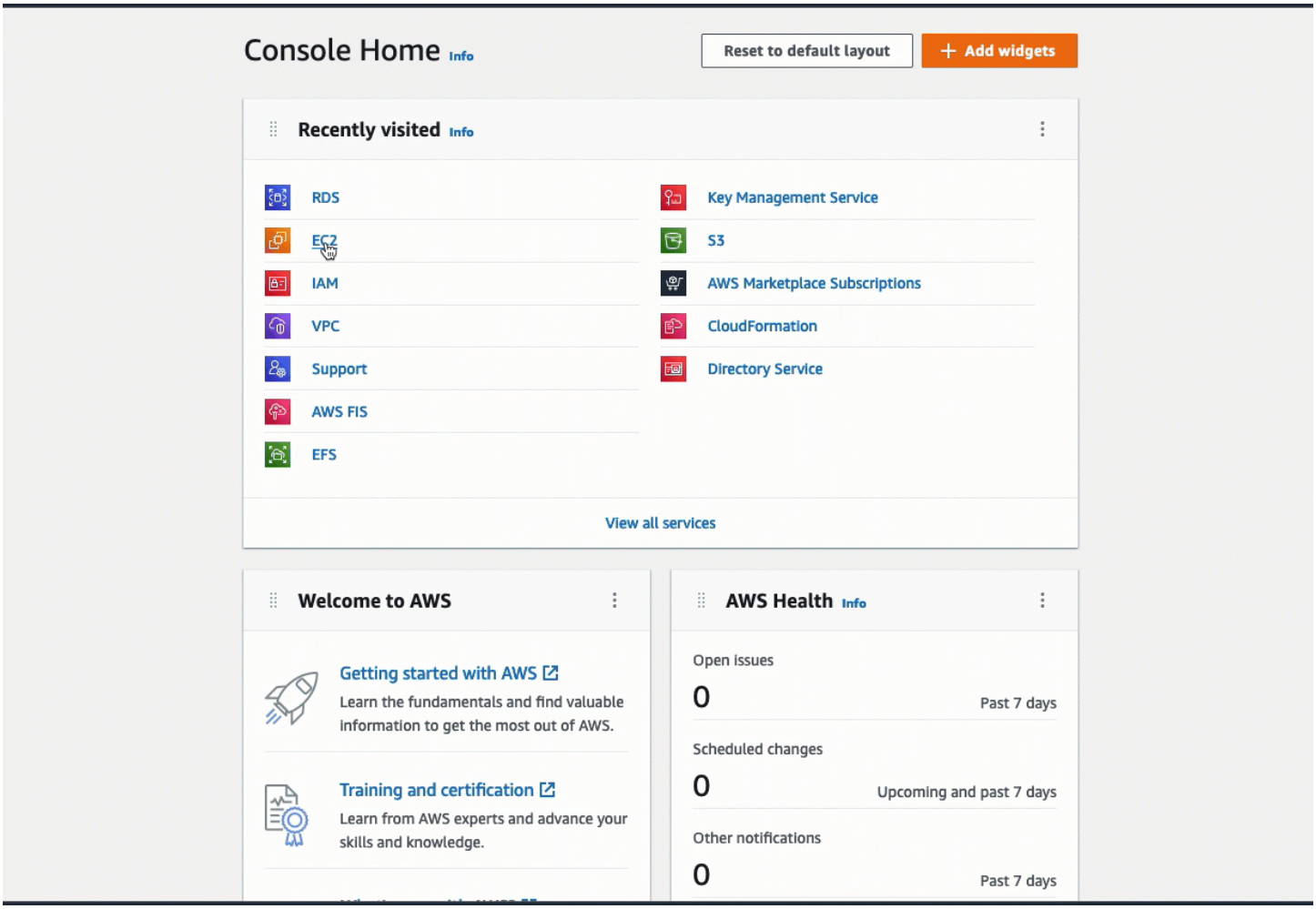
So überprüfen Sie die Verbindungskonfiguration mithilfe der Konsole

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie die RDS-Datenbank aus, die Sie für dieses Tutorial erstellt haben.
4. Überprüfen Sie auf der Registerkarte Verbindung und Sicherheit unter Sicherheit, VPC-Sicherheitsgruppen, dass eine Sicherheitsgruppe mit dem Namen rds-ec2-*x* angezeigt wird.
5. Wählen Sie die Sicherheitsgruppe rds-ec2-*x* aus. Der Bildschirm Security Groups (Sicherheitsgruppen) in der EC2-Konsole wird geöffnet.
6. Wählen Sie die Sicherheitsgruppe rds-ec2-*x* aus, um sie zu öffnen.
7. Wählen Sie die Registerkarte Inbound rules (Regeln für eingehenden Datenverkehr) aus.
8. Stellen Sie wie folgt sicher, dass die folgende Sicherheitsgruppenregel vorhanden ist:
   - Typ: MYSQL/Aurora
   - Portbereich: 3306
   - Quelle: *sg-0987654321example* / ec2-rds-*x* – Dies ist die Sicherheitsgruppe, die der EC2-Instance zugewiesen ist, die Sie in den vorherigen Schritten überprüft haben.
   - Beschreibung: Rule to allow connections from EC2 instances with *sg-1234567890example* attached (Regel zum Zulassen von Verbindungen von EC2-Instances mit angefügtem sg-1234567890example)
9. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
10. Wählen Sie im Navigationsbereich Instances aus.
11. Wählen Sie die EC2-Instance aus, die Sie in der vorherigen Aufgabe für die Verbindung mit der RDS-Datenbank ausgewählt haben, und wählen Sie die Registerkarte Security (Sicherheit) aus.
12. Überprüfen Sie unter Sicherheitsdetails, Sicherheitsgruppen, dass eine Sicherheitsgruppe mit dem Namen ec2-rds-*x* in der Liste enthalten ist. *x* ist eine Zahl.
13. Wählen Sie die Sicherheitsgruppe ec2-rds-*x*, um sie zu öffnen.
14. Wählen Sie die Registerkarte Outbound rules (Ausgehende Regeln).
15. Stellen Sie wie folgt sicher, dass die folgende Sicherheitsgruppenregel vorhanden ist:

- Typ: MYSQL/Aurora
- Portbereich: 3306
- Ziel: ***sg-1234567890example*** / rds-ec2-***x***
- Beschreibung: Regel zum Zulassen von Verbindungen zu **`database-tutorial`** von allen Instances, an denen diese Sicherheitsgruppe angefügt ist

Indem Sie überprüfen, ob diese Sicherheitsgruppen und Sicherheitsgruppenregeln vorhanden sind und ob sie der RDS-Datenbank und der EC2-Instance wie in diesem Verfahren beschrieben zugewiesen sind, können Sie überprüfen, ob die Verbindung automatisch konfiguriert wurde, indem Sie das automatische Verbindungsfeature verwenden.

Animation anzeigen: Überprüfen der Verbindungskonfiguration



Sie haben Option 1 dieses Tutorials abgeschlossen. Sie können nun entweder Option 2 abschließen, in der Sie lernen, wie Sie die RDS-Konsole verwenden, um eine EC2-Instance automatisch mit einer

RDS-Datenbank zu verbinden oder Sie können Option 3 abschließen, in der Sie lernen, wie Sie die Sicherheitsgruppen, die in Option 1 automatisch erstellt wurden, manuell konfigurieren.

Aufgabe 5 (Optional): Aufräumen

> **Warning**
>
> Das Beenden einer Instance ist dauerhaft und irreversibel.
> Nachdem Sie eine Instance beendet haben, können Sie keine Verbindung mehr zu ihr herstellen und sie kann nicht wiederhergestellt werden. Alle angehängten Amazon-EBS-Volumes, die so konfiguriert sind, dass sie beim Beenden gelöscht werden, werden ebenfalls dauerhaft gelöscht und können nicht wiederhergestellt werden. Alle auf den Instance-Speicher-Volumes gespeicherten Daten gehen dauerhaft verloren. Weitere Informationen finden Sie unter Wie die Kündigung von Instances funktioniert.
> Bevor Sie eine Instance beenden, stellen Sie sicher, dass Sie alle Daten, die Sie nach der Beendigung behalten müssen, im persistenten Speicher gesichert haben.

Nachdem Sie das Tutorial abgeschlossen haben, empfiehlt es sich, alle Ressourcen zu bereinigen (zu löschen), die Sie nicht mehr verwenden möchten. Das Bereinigen von AWS-Ressourcen verhindert, dass weitere Gebühren für Ihr Konto anfallen.

Wenn Sie eine EC2-Instance speziell für dieses Tutorial gestartet haben, können Sie sie beenden, damit keine damit verbundenen Gebühren anfallen.

Um eine Instance mithilfe der Konsole zu beenden

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus, die Sie für dieses Tutorial erstellt haben, und wählen Sie Instance state (Instance-Status), Terminate instance (Instance beenden) aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Beenden aus.

Wenn Sie eine RDS-Datenbank speziell für dieses Tutorial erstellt haben, können Sie sie löschen, damit keine damit verbundenen Gebühren anfallen.

Löschen einer RDS-Datenbank mithilfe der Konsole

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie die RDS-Datenbank aus, die Sie für dieses Tutorial erstellt haben, und wählen Sie Actions (Aktionen), Delete (Löschen) aus.
4. Geben Sie **`delete me`** in das Feld ein und wählen Sie dann Delete (Löschen).

Option 2: Automatisches Verbinden einerInstance mit einer RDS-Datenbank mithilfe der RDS-Konsole

Das Ziel von Option 2 ist es, das automatische Verbindungsfeature in der RDS-Konsole zu erkunden, die automatisch die Verbindung zwischen Ihrer EC2-Instance und der RDS-Datenbank konfiguriert, damit Datenverkehr von der EC2-Instance zur RDS-Datenbank zugelassen wird. In Option 3 erfahren Sie, wie Sie die Verbindung manuell konfigurieren.

Aufgaben

- Bevor Sie beginnen
- Aufgabe 1: (Optional) Eine EC2-Instance starten
- Aufgabe 2: Erstellen einer RDS-Datenbank und automatisches Verbinden mit Ihrer EC2-Instance
- Aufgabe 3: Überprüfen der Verbindungskonfiguration
- Aufgabe 4 (Optional): Aufräumen

Bevor Sie beginnen

Sie benötigen Folgendes, um dieses Tutorial abzuschließen:

- Eine EC2-Instance, die sich in derselben VPC wie die RDS-Datenbank befindet. Sie können entweder eine vorhandene EC2-Instance verwenden oder die Schritte in Aufgabe 1 ausführen, um eine neue Instance zu erstellen.
- Berechtigungen zum Aufrufen der folgenden Operationen:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`

- `ec2:CreateSecurityGroup`
- `ec2:CreateSubnet`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:RevokeSecurityGroupEgress`

Aufgabe 1: (Optional) Eine EC2-Instance starten

> **Note**
>
> Das Starten einer Instance steht nicht im Mittelpunkt dieses Tutorials. Wenn Sie bereits über eine Amazon-EC2-Instance verfügen und diese in diesem Tutorial verwenden möchten, können Sie diese Aufgabe überspringen.

Ziel dieser Aufgabe ist es, eine EC2-Instance zu starten, damit Sie Aufgabe 2 abschließen können, in der Sie die Verbindung zwischen Ihrer EC2-Instance und Ihrer Amazon RDS-Datenbank konfigurieren. Mit den Schritten in dieser Aufgabe wird die EC2-Instance wie folgt konfiguriert:

- Instance-Name: **`tutorial-instance-2`**
- AMI: Amazon Linux 2
- Instance-Typ: `t2.micro`
- Öffentliche IP automatisch zuweisen: Aktiviert
- Sicherheitsgruppe mit den folgenden drei Regeln:
  - SSH von Ihrer IP-Adresse zulassen
  - HTTPS-Datenverkehr von überall zulassen
  - HTTP-Datenverkehr von überall zulassen

> **Important**
>
> In einer Produktionsumgebung sollten Sie Ihre Instance so konfigurieren, dass sie Ihren speziellen Anforderungen entspricht.

Starten Sie EC2-Instances wie folgt:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im EC2-Dashboard die Option Launch Instance (Instance starten) aus.
3. Geben Sie unter Name and tags (Name und Tags) für Name einen Namen ein, um Ihre Instance zu identifizieren. Geben Sie für dieses Tutorial der Instance den Namen **`tutorial-instance-2`**. Der Instance-Name ist zwar nicht obligatorisch, aber wenn Sie Ihre Instance in der RDS-Konsole auswählen, können Sie sie anhand des Namens leicht identifizieren.
4. Wählen Sie unter Application and OS Images (Anwendungs- und Betriebssystem-Images) ein AMI aus, das Ihren Webserver-Anforderungen entspricht. Dieses Tutorial verwendet Amazon Linux.
5. Wählen Sie unter Instance type (Instance-Typ) für Instance type (Instance-Typ) einen Instance-Typ aus, der Ihren Webserver-Anforderungen entspricht. In diesem Tutorial wird ein verwendet `t2.micro`.

   > **Note**
   >
   > Abhängig davon, wann Sie Ihr Konto erstellt haben, kann es sein, dass Sie Amazon EC2 im Rahmen des kostenlosen Kontingents verwenden können.
   > Wenn Sie Ihr AWS-Konto vor dem 15. Juli 2025 erstellt haben und es weniger als 12 Monate alt ist, können Sie Amazon EC2 im kostenlosen Kontingent verwenden, indem Sie den Instance-Typ t2.micro auswählen, oder den Instance-Typ t3.micro in Regionen, in denen t2.micro nicht verfügbar ist. Beachten Sie, dass beim Starten einer t3.micro-Instance standardmäßig der Modus Unlimited verwendet wird, wodurch je nach CPU-Auslastung zusätzliche Gebühren anfallen können. Wenn ein Instance-Typ unter dem kostenlosen Kontingent berechtigt ist, ist er als Für das kostenlose Kontingent berechtigt gekennzeichnet.
   > Wenn Sie Ihr AWS-Konto am oder nach dem 15. Juli 2025 erstellt haben, können Sie die Instance-Typen t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large und m7i-flex.large 6 Monate verwenden, oder bis Ihr Guthaben aufgebraucht ist.

Weitere Informationen finden Sie unter Vorteile des kostenlosen Kontingents vor und nach dem 15. Juli 2025.

6. Wählen Sie unter Key pair (login) (Schlüsselpaar (Anmeldung)) für Key pair name (Schlüsselpaar-Name) Ihr Schlüsselpaar aus.
7. Führen Sie unter Network settings (Netzwerkeinstellungen) die folgenden Schritte aus:

   a. Wenn Sie für Network (Netzwerk) und Subnet (Subnetz) keine Änderungen an Ihrer Standard-VPC oder Ihren Subnetzen vorgenommen haben, können Sie die Standardeinstellungen beibehalten.

      Wenn Sie Änderungen an Ihrer Standard-VPC oder Ihren Subnetzen vorgenommen haben, überprüfen Sie Folgendes:

      i. Die Instance muss sich in derselben VPC wie die RDS-Datenbank befinden, um die automatische Verbindungskonfiguration verwenden zu können. Standardmäßig haben Sie nur eine VPC.

      ii. Die VPC, in der Sie Ihre Instance starten, muss mit einem Internet-Gateway verbunden sein, damit Sie über das Internet auf Ihren Webserver zugreifen können. Ihre Standard-VPC wird automatisch mit einem Internet-Gateway eingerichtet.

      iii. Um sicherzustellen, dass Ihre Instance eine öffentliche IP-Adresse erhält, überprüfen Sie für Auto-assign public IP (Automatische Zuweisung öffentlicher IP), dass Enable (Aktivieren) ausgewählt ist. Wenn Disable (Deaktivieren) ausgewählt ist, wählen Sie Edit (Bearbeiten) (rechts neben Network Settings (Netzwerkeinstellungen)) und dann für Auto-assign public IP (Öffentliche IP automatisch zuweisen) die Option Enable (Aktivieren) aus.

   b. Um mithilfe von SSH eine Verbindung zu Ihrer Instance herzustellen, benötigen Sie eine Sicherheitsgruppenregel, die SSH- (Linux) oder RDP-Datenverkehr (Windows) von der öffentlichen IPv4-Adresse Ihres Computers autorisiert. Wenn Sie eine Instance starten, wird standardmäßig eine neue Sicherheitsgruppe mit einer Regel erstellt, die eingehenden SSH-Datenverkehr von überall zulässt.

      Um sicherzustellen, dass nur Ihre IP-Adresse eine Verbindung zu Ihrer Instance herstellen kann, wählen Sie unter (Firewall (Sicherheitsgruppen) in der Dropdown-Liste neben dem Kontrollkästchen SSH-Verkehr zulassen von die Option Meine IP aus.

   c. Um Datenverkehr aus dem Internet zu Ihrer Instance zuzulassen, aktivieren Sie die folgenden Kontrollkästchen:

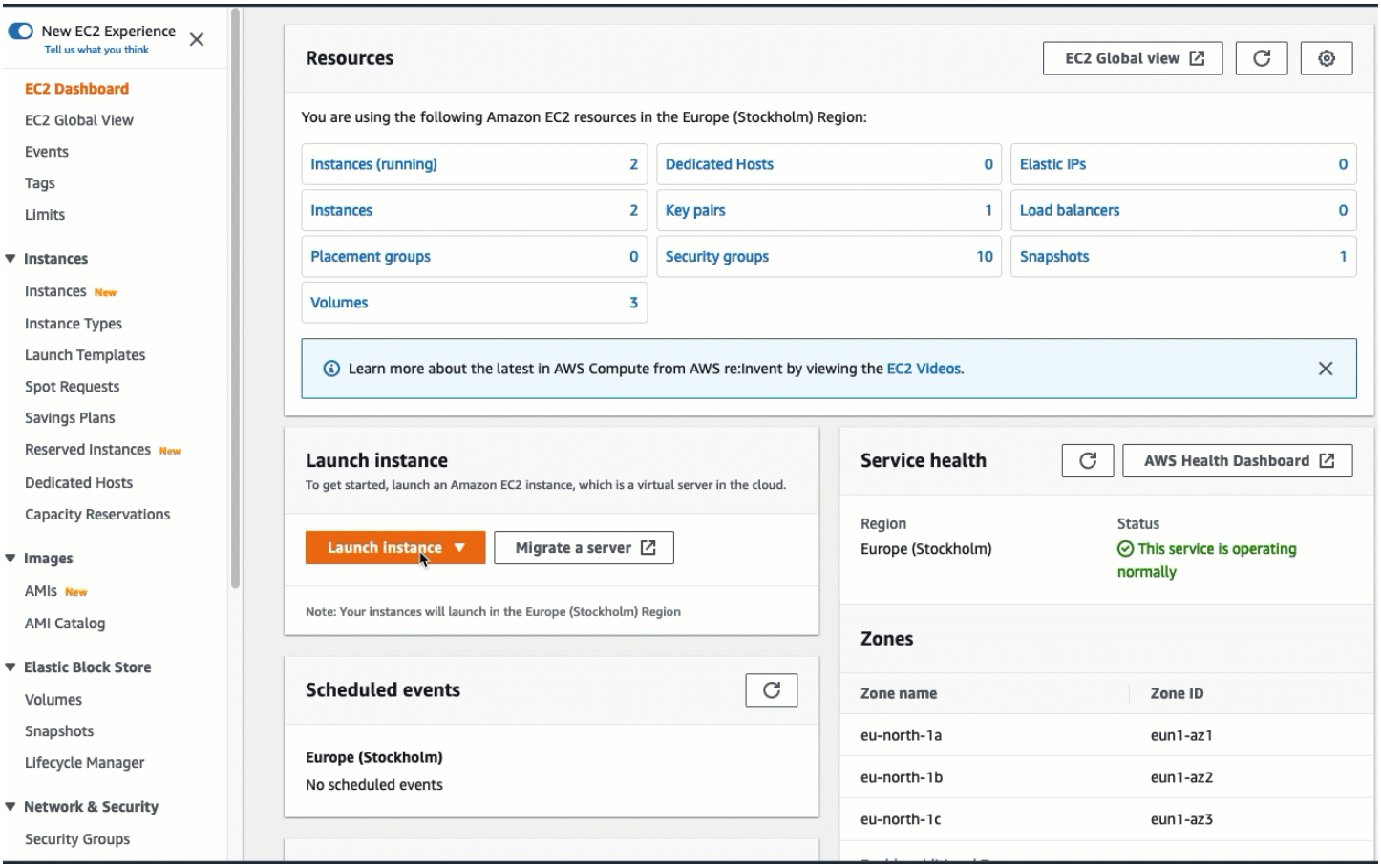
- Allow HTTPs traffic from the internet (HTTPs-Datenverkehr aus dem Internet zulassen
- Allow HTTP traffic from the internet (HTTP-Datenverkehr aus dem Internet zulassen

8. Überprüfen Sie im Bereich Summary (Übersicht) Ihre Instance-Konfiguration und wählen Sie dann Launch instance (Instance starten) aus.
9. Wählen Sie View all Instances (Alle Instances anzeigen) aus, um die Bestätigungsseite zu schließen und zur Konsole zurückzukehren. Ihre Instance befindet sich zunächst in einem `pending`-Status und wechselt dann in den `running`-Status.

   Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Fehlerbehebung bei Amazon-EC2-Instances.

Weitere Informationen über das Starten einer Instance finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten.

Animation anzeigen: Starten einer EC2-Instance



Aufgabe 2: Erstellen einer RDS-Datenbank und automatisches Verbinden mit Ihrer EC2-Instance

Ziel dieser Aufgabe ist es, eine RDS-Datenbank zu erstellen und das automatische Verbindungsfeature in der RDS-Konsole zu verwenden, um die Verbindung zwischen Ihrer EC2-Instance und Ihrer RDS-Datenbank automatisch zu konfigurieren. Mit den Schritten in dieser Aufgabe wird die DB-Instance wie folgt konfiguriert:

- Engine-Typ: MySQL
- Vorlage: Kostenloses Kontingent
- DB-Instance-Kennung: **`tutorial-database`**
- DB-Instance-Klasse: `db.t3.micro`

> **Important**
>
> In einer Produktionsumgebung sollten Sie Ihre Instance so konfigurieren, dass sie Ihren speziellen Anforderungen entspricht.

So erstellen Sie eine RDS-Datenbank und verbinden sie automatisch mit einer EC2-Instance

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie in der Regionsauswahl (oben rechts) die AWS-Region aus, in der Sie die EC2-Instance erstellt haben. Die EC2-Instance und die RDS-Datenbank müssen sich in der gleichen Region befinden.
3. Wählen Sie im Dashboard Create database (Datenbank erstellen) aus.
4. Überprüfen Sie unter Choose a database creation method (Datenbankerstellungsmethode auswählen), ob Standard create (Standarderstellung) ausgewählt ist. Wenn Sie Easy create (Einfache Erstellung) wählen, ist das automatische Verbindungsfeature nicht verfügbar.
5. Wählen Sie unter Engine options (Engine-Optionen) für Engine type (Engine-Typ) die Option MySQL aus.
6. Wählen Sie unter Templates (Vorlagen) eine Beispielvorlage aus, die Ihren Anforderungen entspricht. Wählen Sie für dieses Tutorial die Option Free tier (Kostenloses Kontingent), um kostenlos eine Datenbank zu erstellen. Beachten Sie jedoch, dass das kostenlose Kontingent

nur verfügbar ist, wenn Ihr Konto für das kostenlose Kontingent qualifiziert ist. Sie können mehr darüber erfahren, indem Sie auf den Info-Link im Feld Free tier (Kostenloses Kontingent) klicken.

7. Führen Sie unter Settings (Einstellungen) die folgenden Schritte aus:

   a. Geben Sie unter DB instance identifier (DB-Instance-Kennung) einen Namen für die Datenbank ein. Geben Sie für dieses Tutorial ein **`tutorial-database`**.

   b. Behalten Sie für Master username (Master-Benutzername) den Standardnamen **`admin`** bei.

   c. Geben Sie unter Master password (Master-Passwort) ein Passwort ein, das Sie sich für dieses Tutorial merken können, und geben Sie dann unter Confirm password (Passwort bestätigen) das Passwort erneut ein.

8. Behalten Sie unter Instance-Konfiguration für die DB-Instance-Klasse die Standardeinstellung bei, welche db.t3.micro ist. Wenn Ihr Konto für das kostenlose Kontingent qualifiziert ist, können Sie diese Instance kostenlos verwenden. Weitere Informationen finden Sie unter Kostenloses AWS-Kontingent.

9. Wählen Sie unter Connectivity (Verbindung) für Compute resource (Rechenressource) die Option Connect to an EC2 compute resource (Mit einer EC2-Rechenressource verbinden) aus. Dies ist das automatische Verbindungsfeature in der RDS-Konsole.

10. Wählen Sie für die EC2 instance (EC2-Instance), die EC2-Instance aus, zu der Sie eine Verbindung herstellen möchten. Für die Zwecke dieses Tutorials können Sie entweder die Instance wählen, die Sie in der vorherigen Aufgabe erstellt haben und die Sie **`tutorial-instance`** genannt haben oder eine andere bereits vorhandene Instance wählen. Wenn Ihre Instance nicht in der Liste angezeigt wird, wählen Sie das Aktualisierungssymbol rechts neben Connectivity (Verbindung) aus.

    Wenn Sie das automatische Verbindungsfeature verwenden, wird dieser EC2-Instance eine Sicherheitsgruppe hinzugefügt, und der RDS-Datenbank wird eine weitere Sicherheitsgruppe hinzugefügt. Die Sicherheitsgruppen werden automatisch so konfiguriert, dass der Datenverkehr zwischen der EC2-Instance und der RDS-Datenbank zugelassen wird. In der nächsten Aufgabe überprüfen Sie, ob die Sicherheitsgruppen erstellt und der EC2-Instance und der RDS-Datenbank zugewiesen wurden.

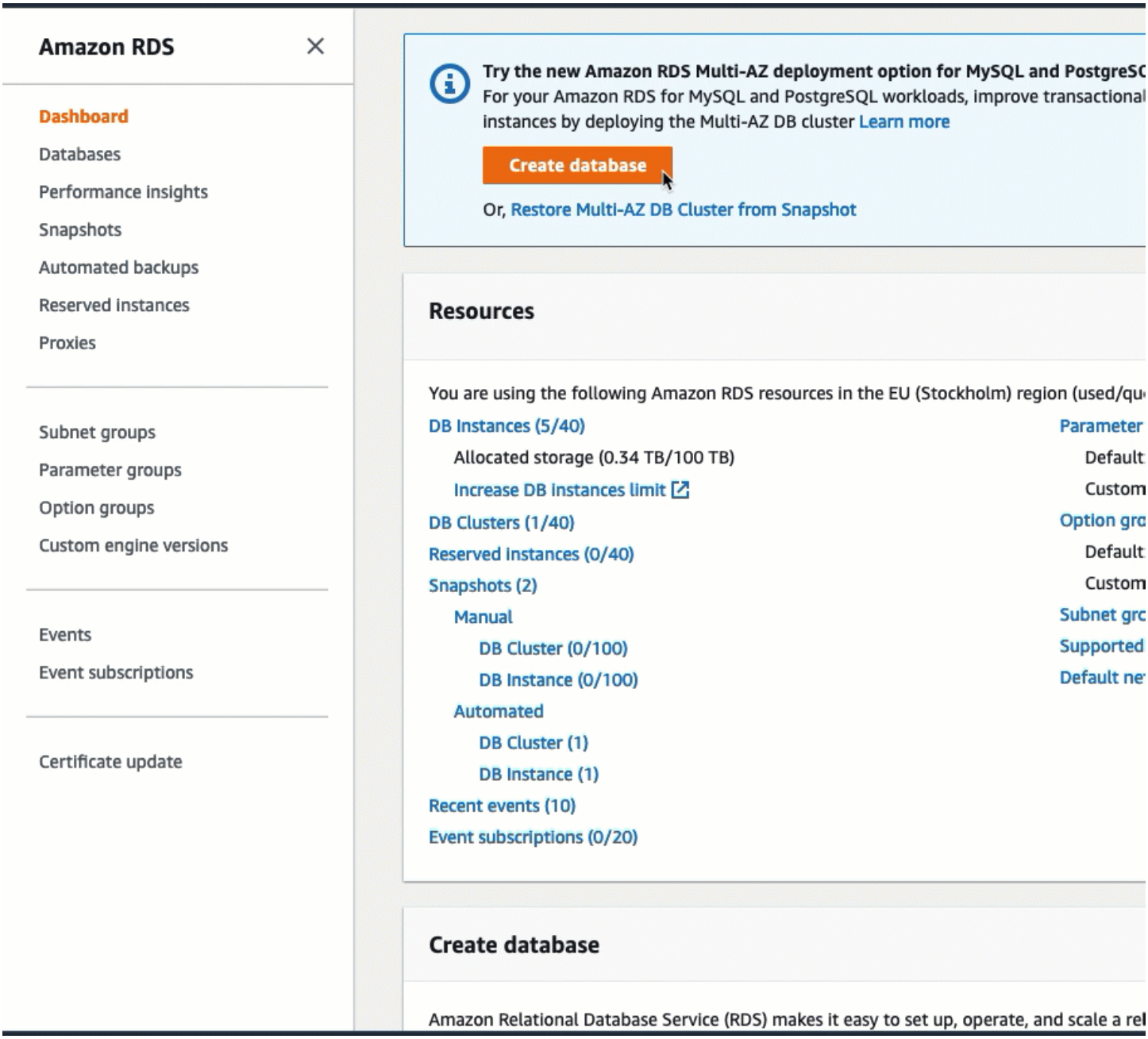
11. Wählen Sie Datenbank erstellen aus.

    Auf dem Bildschirm Databases (Datenbanken) lautet der Status der neuen Datenbank Creating (Wird erstellt), bis die Datenbank einsatzbereit ist. Wenn sich der Status in Available (Verfügbar) ändert, können Sie eine Verbindung zur Datenbank herstellen. Abhängig von der Klasse der

Datenbank und vom verfügbaren Speicherplatz kann es bis zu 20 Minuten dauern, bis die neue Datenbank verfügbar ist.

Weitere Informationen finden Sie unter Konfigurieren der automatischen Netzwerkverbindung mit einer EC2-Instance im Amazon-RDS-Benutzerhandbuch.

Animation anzeigen: Erstellen einer RDS-Datenbank und automatisches Verbinden mit einer EC2-Instance



Aufgabe 3: Überprüfen der Verbindungskonfiguration

Ziel dieser Aufgabe ist es, zu überprüfen, ob die beiden Sicherheitsgruppen erstellt und der Instance und Datenbank zugewiesen wurden.

Wenn Sie das automatische Verbindungs-Feature in der RDS-Konsole verwenden, um die Verbindung zu konfigurieren, werden die Sicherheitsgruppen automatisch erstellt und der Instance und Datenbank wie folgt zugewiesen:

- Die Sicherheitsgruppe rds-ec2-***x*** wird erstellt und der RDS-Datenbank hinzugefügt. Es verfügt über eine eingehende Regel, die auf die Sicherheitsgruppe ec2-rds-***x*** als Quelle verweist. Dadurch kann der Datenverkehr von der EC2-Instance mit der Sicherheitsgruppe ec2-rds-***x*** die RDS-Datenbank erreichen.
- Die Sicherheitsgruppe ec2-rds-***x*** wird erstellt und der EC2-Instance hinzugefügt. Es verfügt über eine ausgehende Regel, die auf die Sicherheitsgruppe rds-ec2-***x*** als Ziel verweist. Dadurch kann der Datenverkehr von der EC2-Instance die RDS-Datenbank mit der Sicherheitsgruppe rds-ec2-***x*** erreichen.

So überprüfen Sie die Verbindungskonfiguration mithilfe der Konsole

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie die RDS-Datenbank aus, die Sie für dieses Tutorial erstellt haben.
4. Überprüfen Sie auf der Registerkarte Verbindung und Sicherheit unter Sicherheit, VPC-Sicherheitsgruppen, dass eine Sicherheitsgruppe mit dem Namen rds-ec2-***x*** angezeigt wird.
5. Wählen Sie die Sicherheitsgruppe rds-ec2-***x*** aus. Der Bildschirm Security Groups (Sicherheitsgruppen) in der EC2-Konsole wird geöffnet.
6. Wählen Sie die Sicherheitsgruppe rds-ec2-***x*** aus, um sie zu öffnen.
7. Wählen Sie die Registerkarte Inbound rules (Regeln für eingehenden Datenverkehr) aus.
8. Stellen Sie wie folgt sicher, dass die folgende Sicherheitsgruppenregel vorhanden ist:
   - Typ: MYSQL/Aurora
   - Portbereich: 3306
   - Quelle: ***sg-0987654321example*** / ec2-rds-***x*** – Dies ist die Sicherheitsgruppe, die der EC2-Instance zugewiesen ist, die Sie in den vorherigen Schritten überprüft haben.

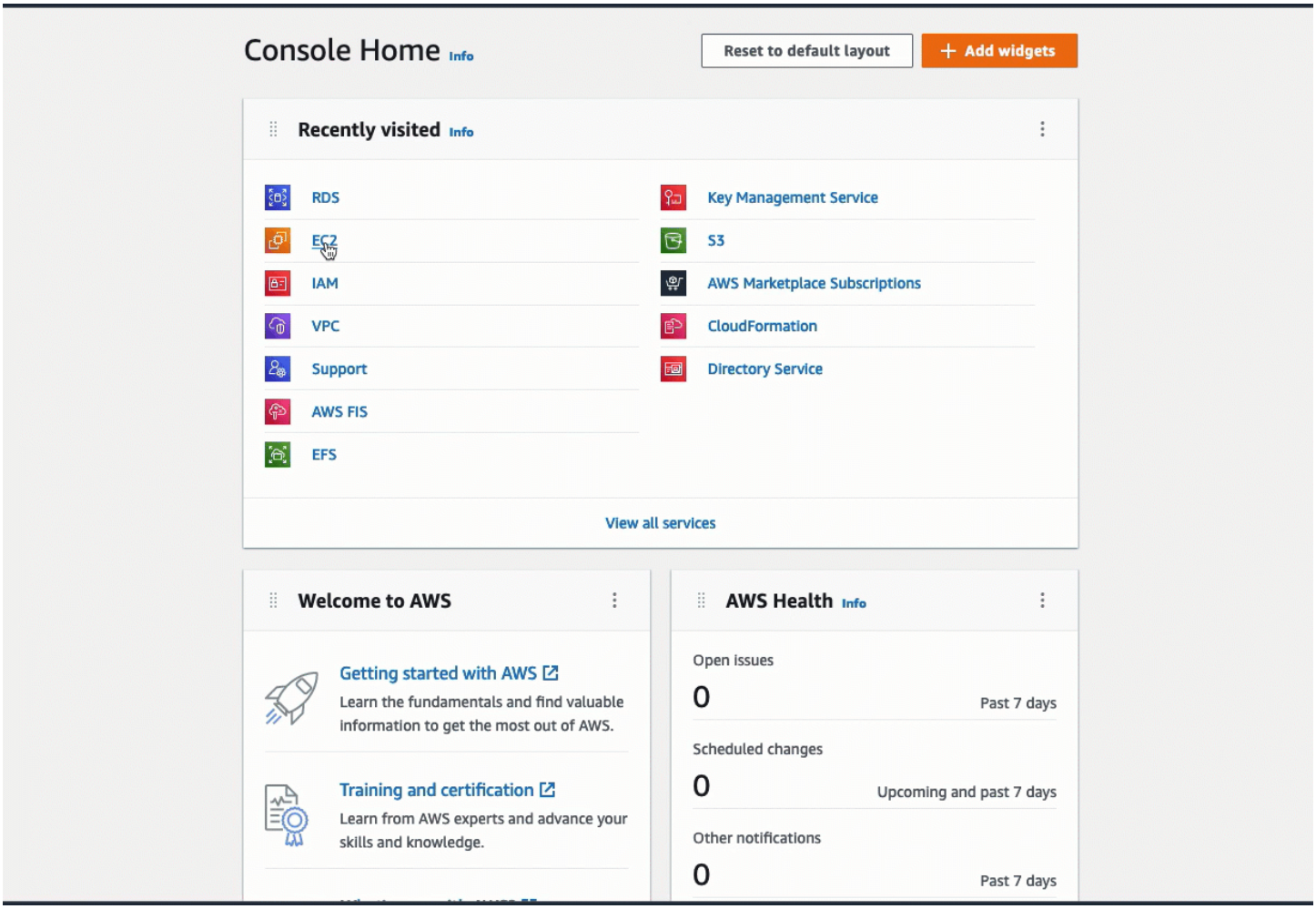
- Beschreibung: Rule to allow connections from EC2 instances with ***sg-1234567890example*** attached (Regel zum Zulassen von Verbindungen von EC2-Instances mit angefügtem sg-1234567890example)

9. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
10. Wählen Sie im Navigationsbereich Instances aus.
11. Wählen Sie die EC2-Instance aus, die Sie in der vorherigen Aufgabe für die Verbindung mit der RDS-Datenbank ausgewählt haben, und wählen Sie die Registerkarte Security (Sicherheit) aus.
12. Überprüfen Sie unter Sicherheitsdetails, Sicherheitsgruppen, dass eine Sicherheitsgruppe mit dem Namen ec2-rds-***x*** in der Liste enthalten ist. *x* ist eine Zahl.
13. Wählen Sie die Sicherheitsgruppe ec2-rds-***x***, um sie zu öffnen.
14. Wählen Sie die Registerkarte Outbound rules (Ausgehende Regeln).
15. Stellen Sie wie folgt sicher, dass die folgende Sicherheitsgruppenregel vorhanden ist:

    - Typ: MYSQL/Aurora
    - Portbereich: 3306
    - Ziel: ***sg-1234567890example*** / rds-ec2-***x***
    - Beschreibung: Regel zum Zulassen von Verbindungen zu **`database-tutorial`** von allen Instances, an denen diese Sicherheitsgruppe angefügt ist

Indem Sie überprüfen, ob diese Sicherheitsgruppen und Sicherheitsgruppenregeln vorhanden sind und ob sie der RDS-Datenbank und der EC2-Instance wie in diesem Verfahren beschrieben zugewiesen sind, können Sie überprüfen, ob die Verbindung automatisch konfiguriert wurde, indem Sie das automatische Verbindungsfeature verwenden.

Animation anzeigen: Überprüfen der Verbindungskonfiguration



Sie haben Option 2 dieses Tutorials abgeschlossen. Sie können jetzt Option 3 abschließen, in der Sie erfahren, wie Sie die Sicherheitsgruppen, die automatisch in Option 2 erstellt wurden, manuell konfigurieren.

Aufgabe 4 (Optional): Aufräumen

> **Warning**
>
> Das Beenden einer Instance ist dauerhaft und irreversibel.
> Nachdem Sie eine Instance beendet haben, können Sie keine Verbindung mehr zu ihr herstellen und sie kann nicht wiederhergestellt werden. Alle angehängten Amazon-EBS-Volumes, die so konfiguriert sind, dass sie beim Beenden gelöscht werden, werden ebenfalls dauerhaft gelöscht und können nicht wiederhergestellt werden. Alle auf den Instance-Speicher-Volumes gespeicherten Daten gehen dauerhaft verloren. Weitere Informationen finden Sie unter Wie die Kündigung von Instances funktioniert.

Bevor Sie eine Instance beenden, stellen Sie sicher, dass Sie alle Daten, die Sie nach der Beendigung behalten müssen, im persistenten Speicher gesichert haben.

Nachdem Sie das Tutorial abgeschlossen haben, empfiehlt es sich, alle Ressourcen zu bereinigen (zu löschen), die Sie nicht mehr verwenden möchten. Das Bereinigen von AWS-Ressourcen verhindert, dass weitere Gebühren für Ihr Konto anfallen.

Wenn Sie eine EC2-Instance speziell für dieses Tutorial gestartet haben, können Sie sie beenden, damit keine damit verbundenen Gebühren anfallen.

Um eine Instance mithilfe der Konsole zu beenden

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus, die Sie für dieses Tutorial erstellt haben, und wählen Sie Instance state (Instance-Status), Terminate instance (Instance beenden) aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Beenden aus.

Wenn Sie eine RDS-Datenbank speziell für dieses Tutorial erstellt haben, können Sie sie löschen, damit keine damit verbundenen Gebühren anfallen.

Löschen einer RDS-Datenbank mithilfe der Konsole

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie die RDS-Datenbank aus, die Sie für dieses Tutorial erstellt haben, und wählen Sie Actions (Aktionen), Delete (Löschen) aus.
4. Geben Sie **`delete me`** in das Feld ein und wählen Sie dann Delete (Löschen).

Option 3: Manuelles Verbinden einer Instance mit einer RDS-Datenbank, durch Erstellen von Sicherheitsgruppen

Das Ziel von Option 3 besteht darin, zu lernen, wie die Verbindung zwischen einer EC2-Instance und einer RDS-Datenbank manuell konfiguriert wird, indem die Konfiguration des automatischen Verbindungsfeatures manuell reproduziert wird.

Aufgaben

- Bevor Sie beginnen
- Aufgabe 1: (Optional) Eine EC2-Instance starten
- Aufgabe 2 (Optional): Erstellen einer RDS-Datenbank
- Aufgabe 3: Manuelles Verbinden Ihrer EC2-Instance mit Ihrer RDS-Datenbank, durch Erstellen von Sicherheitsgruppen und deren Zuweisung zu den Instances
- Aufgabe 4 (Optional): Aufräumen

Bevor Sie beginnen

Sie benötigen Folgendes, um dieses Tutorial abzuschließen:

- Eine EC2-Instance, die sich in derselben VPC wie die RDS-Datenbank befindet. Sie können entweder eine vorhandene EC2-Instance verwenden oder die Schritte in Aufgabe 1 ausführen, um eine neue Instance zu erstellen.
- Eine RDS-Datenbank, die sich in derselben VPC wie die EC2-Instance befindet. Sie können entweder eine vorhandene RDS-Datenbank verwenden oder die Schritte in Aufgabe 2 ausführen, um eine neue Datenbank zu erstellen.
- Berechtigungen zum Aufrufen der folgenden Operationen:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Aufgabe 1: (Optional) Eine EC2-Instance starten

> **Note**
>
> Das Starten einer Instance steht nicht im Mittelpunkt dieses Tutorials. Wenn Sie bereits über eine Amazon-EC2-Instance verfügen und diese in diesem Tutorial verwenden möchten, können Sie diese Aufgabe überspringen.

Ziel dieser Aufgabe ist es, eine EC2-Instance zu starten, damit Sie Aufgabe 3 abschließen können, in der Sie die Verbindung zwischen Ihrer EC2-Instance und Ihrer Amazon RDS-Datenbank konfigurieren. Mit den Schritten in dieser Aufgabe wird die EC2-Instance wie folgt konfiguriert:

- Instance-Name: **`tutorial-instance`**
- AMI: Amazon Linux 2
- Instance-Typ: `t2.micro`
- Öffentliche IP automatisch zuweisen: Aktiviert
- Sicherheitsgruppe mit den folgenden drei Regeln:
  - SSH von Ihrer IP-Adresse zulassen
  - HTTPS-Datenverkehr von überall zulassen
  - HTTP-Datenverkehr von überall zulassen

> **Important**
>
> In einer Produktionsumgebung sollten Sie Ihre Instance so konfigurieren, dass sie Ihren speziellen Anforderungen entspricht.

Starten Sie EC2-Instances wie folgt:

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/EC2/.
2. Wählen Sie im EC2-Dashboard die Option Launch Instance (Instance starten) aus.
3. Geben Sie unter Name and tags (Name und Tags) für Name einen Namen ein, um Ihre Instance zu identifizieren. Geben Sie für dieses Tutorial der Instance den Namen **`tutorial-`**

`instance-manual-1`. Der Instance-Name ist zwar nicht obligatorisch, aber er hilft Ihnen bei der Identifizierung.

4. Wählen Sie unter Application and OS Images (Anwendungs- und Betriebssystem-Images) ein AMI aus, das Ihren Webserver-Anforderungen entspricht. Dieses Tutorial verwendet Amazon Linux.
5. Wählen Sie unter Instance type (Instance-Typ) für Instance type (Instance-Typ) einen Instance-Typ aus, der Ihren Webserver-Anforderungen entspricht. In diesem Tutorial wird ein verwendet `t2.micro`.

> **Note**
>
> Abhängig davon, wann Sie Ihr Konto erstellt haben, kann es sein, dass Sie Amazon EC2 im Rahmen des kostenlosen Kontingents verwenden können.
> Wenn Sie Ihr AWS-Konto vor dem 15. Juli 2025 erstellt haben und es weniger als 12 Monate alt ist, können Sie Amazon EC2 im kostenlosen Kontingent verwenden, indem Sie den Instance-Typ t2.micro auswählen, oder den Instance-Typ t3.micro in Regionen, in denen t2.micro nicht verfügbar ist. Beachten Sie, dass beim Starten einer t3.micro-Instance standardmäßig der Modus Unlimited verwendet wird, wodurch je nach CPU-Auslastung zusätzliche Gebühren anfallen können. Wenn ein Instance-Typ unter dem kostenlosen Kontingent berechtigt ist, ist er als Für das kostenlose Kontingent berechtigt gekennzeichnet.
> Wenn Sie Ihr AWS-Konto am oder nach dem 15. Juli 2025 erstellt haben, können Sie die Instance-Typen t3.micro, t3.small, t4g.micro, t4g.small, c7i-flex.large und m7i-flex.large 6 Monate verwenden, oder bis Ihr Guthaben aufgebraucht ist.
> Weitere Informationen finden Sie unter Vorteile des kostenlosen Kontingents vor und nach dem 15. Juli 2025.

6. Wählen Sie unter Key pair (login) (Schlüsselpaar (Anmeldung)) für Key pair name (Schlüsselpaar-Name) Ihr Schlüsselpaar aus.
7. Führen Sie unter Network settings (Netzwerkeinstellungen) die folgenden Schritte aus:

   a. Wenn Sie für Network (Netzwerk) und Subnet (Subnetz) keine Änderungen an Ihrer Standard-VPC oder Ihren Subnetzen vorgenommen haben, können Sie die Standardeinstellungen beibehalten.

      Wenn Sie Änderungen an Ihrer Standard-VPC oder Ihren Subnetzen vorgenommen haben, überprüfen Sie Folgendes:

i. Die Instance muss sich in derselben VPC befinden wie die RDS-Datenbank. Standardmäßig haben Sie nur eine VPC.

ii. Die VPC, in der Sie Ihre Instance starten, muss mit einem Internet-Gateway verbunden sein, damit Sie über das Internet auf Ihren Webserver zugreifen können. Ihre Standard-VPC wird automatisch mit einem Internet-Gateway eingerichtet.

iii. Um sicherzustellen, dass Ihre Instance eine öffentliche IP-Adresse erhält, überprüfen Sie für Auto-assign public IP (Automatische Zuweisung öffentlicher IP), dass Enable (Aktivieren) ausgewählt ist. Wenn Disable (Deaktivieren) ausgewählt ist, wählen Sie Edit (Bearbeiten) (rechts neben Network Settings (Netzwerkeinstellungen)) und dann für Auto-assign public IP (Öffentliche IP automatisch zuweisen) die Option Enable (Aktivieren) aus.

b. Um mithilfe von SSH eine Verbindung zu Ihrer Instance herzustellen, benötigen Sie eine Sicherheitsgruppenregel, die SSH- (Linux) oder RDP-Datenverkehr (Windows) von der öffentlichen IPv4-Adresse Ihres Computers autorisiert. Wenn Sie eine Instance starten, wird standardmäßig eine neue Sicherheitsgruppe mit einer Regel erstellt, die eingehenden SSH-Datenverkehr von überall zulässt.

   Um sicherzustellen, dass nur Ihre IP-Adresse eine Verbindung zu Ihrer Instance herstellen kann, wählen Sie unter (Firewall (Sicherheitsgruppen) in der Dropdown-Liste neben dem Kontrollkästchen SSH-Verkehr zulassen von die Option Meine IP aus.

c. Um Datenverkehr aus dem Internet zu Ihrer Instance zuzulassen, aktivieren Sie die folgenden Kontrollkästchen:

   - Allow HTTPs traffic from the internet (HTTPs-Datenverkehr aus dem Internet zulassen
   - Allow HTTP traffic from the internet (HTTP-Datenverkehr aus dem Internet zulassen

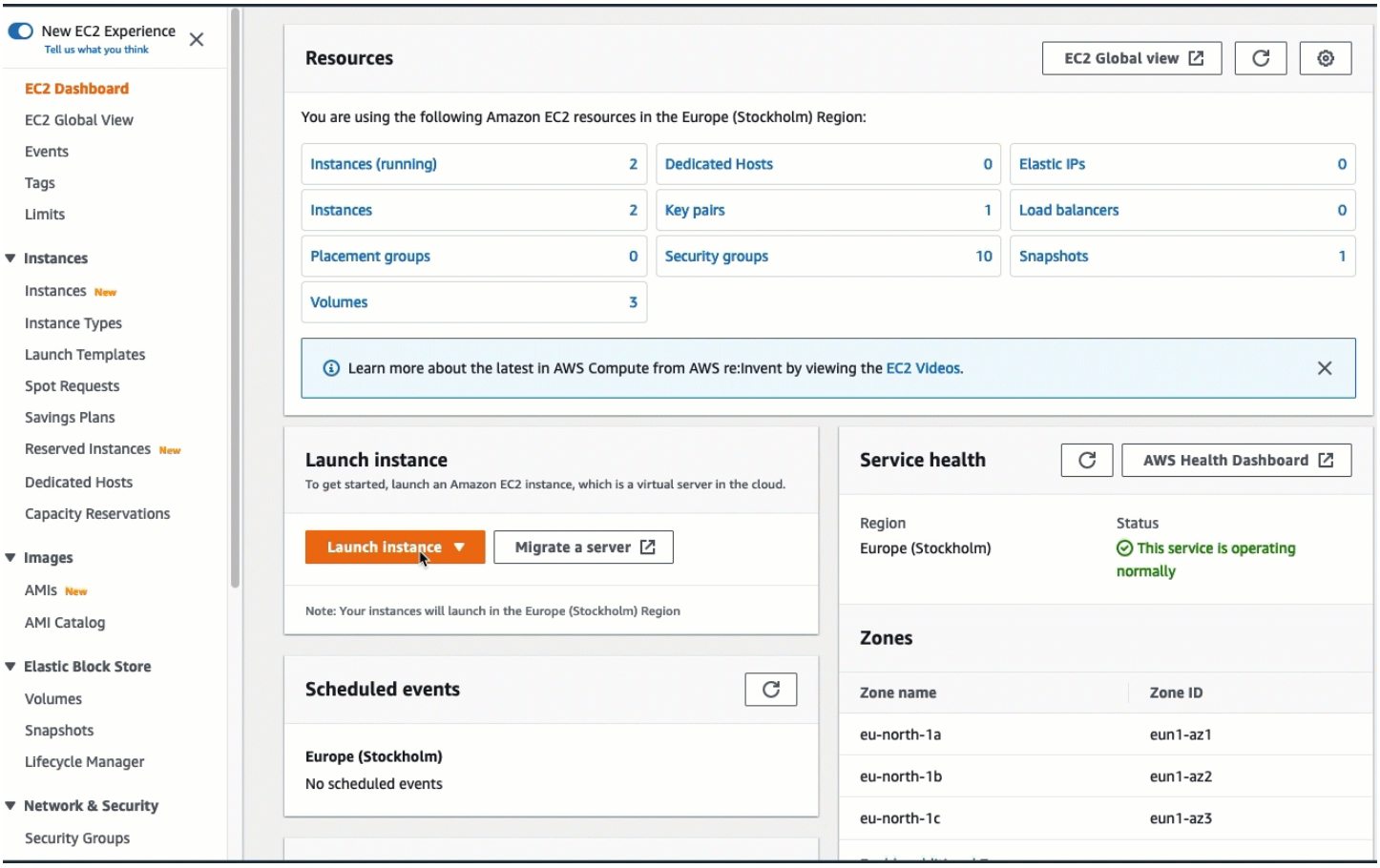
8. Überprüfen Sie im Bereich Summary (Übersicht) Ihre Instance-Konfiguration und wählen Sie dann Launch instance (Instance starten) aus.

9. Wählen Sie View all Instances (Alle Instances anzeigen) aus, um die Bestätigungsseite zu schließen und zur Konsole zurückzukehren. Ihre Instance befindet sich zunächst in einem `pending`-Status und wechselt dann in den `running`-Status.

   Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Fehlerbehebung bei Amazon-EC2-Instances.

Weitere Informationen über das Starten einer Instance finden Sie unter [EC2-Instance mit dem Launch Instance Wizard in der Konsole starten].

Animation anzeigen: Starten einer EC2-Instance



Aufgabe 2 (Optional): Erstellen einer RDS-Datenbank

> **Note**
>
> Das Erstellen einer RDS-Datenbank steht in diesem Teil des Tutorials nicht im Mittelpunkt. Wenn Sie bereits über eine RDS-Datenbank verfügen und diese für dieses Tutorial verwenden möchten, können Sie diese Aufgabe überspringen.

Ziel dieser Aufgabe ist es, eine RDS-Datenbank zu erstellen. Sie verwenden diese Instance in Aufgabe 3, wenn Sie sie mit Ihrer EC2-Instance verbinden. Mit den Schritten in dieser Aufgabe wird die RDS-Datenbank wie folgt konfiguriert:

- Engine-Typ: MySQL
- Vorlage: Kostenloses Kontingent
- DB-Instance-Kennung: **`tutorial-database-manual`**
- DB-Instance-Klasse: `db.t3.micro`

> **Important**
>
> In einer Produktionsumgebung sollten Sie Ihre Instance so konfigurieren, dass sie Ihren speziellen Anforderungen entspricht.

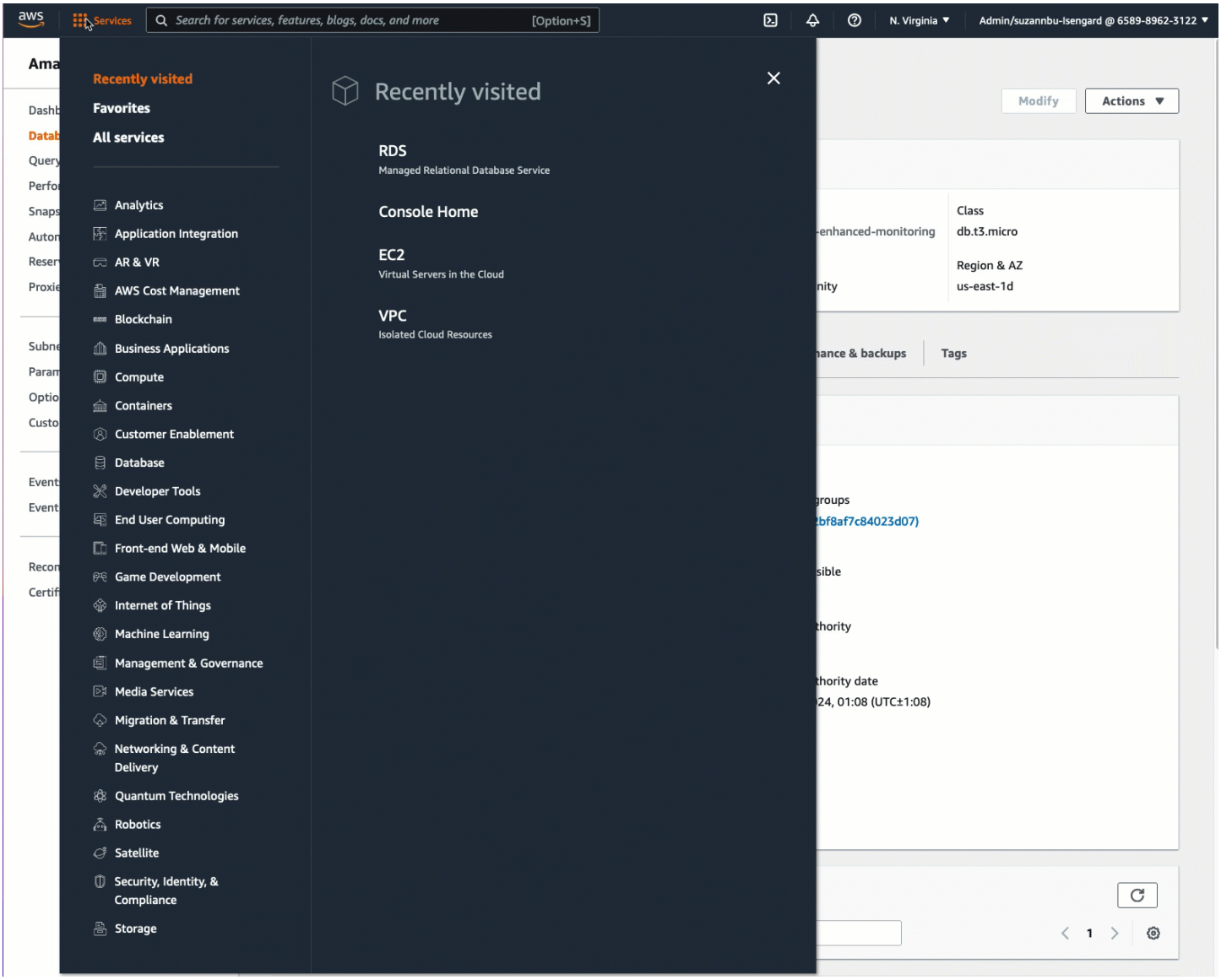
So erstellen Sie eine MySQL-DB-Instance

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie in der Regionsauswahl (oben rechts) die AWS-Region aus, in der Sie die EC2-Instance erstellt haben. Die EC2-Instance und die DB-Instance müssen sich in derselben Region befinden.
3. Wählen Sie im Dashboard Create database (Datenbank erstellen) aus.
4. Wählen Sie unter Choose a database creation method (Eine Datenbankerstellungsmethode auswählen) die Option Easy create (Einfache Erstellung) aus. Wenn Sie diese Option wählen, ist das automatische Verbindungsfeature zum automatischen Konfigurieren der Verbindung nicht verfügbar.
5. Wählen Sie unter Engine options (Engine-Optionen) für Engine type (Engine-Typ) die Option MySQL aus.
6. Wählen Sie in DB-Instance-Größe die Option Kostenloses Kontingent aus.
7. Geben Sie unter DB instance identifier (DB-Instance-Kennung) einen Namen für die Datenbank ein. Geben Sie für dieses Tutorial ein **`tutorial-database-manual`**.
8. Behalten Sie für Master username (Master-Benutzername) den Standardnamen **`admin`** bei.
9. Geben Sie unter Master password (Master-Passwort) ein Passwort ein, das Sie sich für dieses Tutorial merken können, und geben Sie dann unter Confirm password (Passwort bestätigen) das Passwort erneut ein.
10. Wählen Sie Datenbank erstellen aus.

    Auf dem Bildschirm Databases (Datenbanken) lautet der Status der neuen DB-Instance Creating (Wird erstellt), bis die DB-Instance einsatzbereit ist. Wenn sich der Status in Available

(Verfügbar) ändert, können Sie die Verbindung zur DB-Instance herstellen. Abhängig von der Klasse der DB-Instance und vom verfügbaren Speicherplatz kann es bis zu 20 Minuten dauern, bis die neue DB-Instance verfügbar ist.

Animation anzeigen: Erstellen einer DB-Instance



Aufgabe 3: Manuelles Verbinden Ihrer EC2-Instance mit Ihrer RDS-Datenbank, durch Erstellen von Sicherheitsgruppen und deren Zuweisung zu den Instances

Ziel dieser Aufgabe ist es, die Verbindungskonfiguration des automatischen Verbindungsfeatures zu reproduzieren, indem Sie Folgendes manuell ausführen: Sie erstellen zwei neue Sicherheitsgruppen und fügen dann jeweils eine Sicherheitsgruppe zur EC2-Instance und zur RDS-Datenbank hinzu.

So erstellen Sie zwei neue Sicherheitsgruppen und weisen jeweils eine der EC2-Instance und der RDS-Datenbank zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Erstellen Sie zuerst die Sicherheitsgruppe, die der EC2-Instance hinzugefügt werden soll, wie folgt:
   a. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
   b. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus.
   c. Geben Sie unter Security group name (Name der Sicherheitsgruppe) einen aussagekräftigen Namen für die Sicherheitsgruppe ein. Geben Sie für dieses Tutorial ein **`ec2-rds-manual-configuration`**.
   d. Geben Sie unter Description (Beschreibung) eine kurze Beschreibung ein. Geben Sie für dieses Tutorial ein **`EC2 instance security group to allow EC2 instance to securely connect to RDS database`**.
   e. Wählen Sie Sicherheitsgruppe erstellen aus. Sie kehren zu dieser Sicherheitsgruppe zurück, um eine ausgehende Regel hinzuzufügen, nachdem Sie die Sicherheitsgruppe der RDS-Datenbank erstellt haben.
3. Erstellen Sie nun die Sicherheitsgruppe, die Sie der RDS-Datenbank hinzufügen möchten, wie folgt:
   a. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
   b. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus.
   c. Geben Sie unter Security group name (Name der Sicherheitsgruppe) einen aussagekräftigen Namen für die Sicherheitsgruppe ein. Geben Sie für dieses Tutorial ein **`rds-ec2-manual-configuration`**.
   d. Geben Sie unter Description (Beschreibung) eine kurze Beschreibung ein. Geben Sie für dieses Tutorial ein **`RDS database security group to allow EC2 instance to securely connect to RDS database`**.
   e. Wählen Sie unter Inbound rules (Eingehende Regeln) die Option Add rule (Regel hinzufügen) aus und gehen Sie wie folgt vor:
      i. Wählen Sie für Type (Typ) die Option MySQL/Aurora.
      ii. Wählen Sie als Source (Quelle) die EC2-Instance-Sicherheitsgruppe ec2-rds-manual-configuration aus, die Sie in Schritt 2 dieses Verfahrens erstellt haben.

f. Wählen Sie Sicherheitsgruppe erstellen aus.

4. Bearbeiten Sie die EC2-Instance-Sicherheitsgruppe wie folgt, um eine Regel für ausgehenden Datenverkehr hinzuzufügen:

   a. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.

   b. Wählen Sie die EC2-Instance-Sicherheitsgruppe (Sie haben sie **`ec2-rds-manual-configuration`** benannt) und wählen Sie die Registerkarte Outbound rules (Ausgehende Regeln) aus.

   c. Wählen Sie Edit outbound rules (Ausgehende Regeln bearbeiten).

   d. Wählen Sie Add rule (Regel hinzufügen) und gehen Sie wie folgt vor:

      i. Wählen Sie für Type (Typ) die Option MySQL/Aurora.

      ii. Wählen Sie als Quelle die RDS-Datenbank-Sicherheitsgruppe rds-ec2-manual-configuration, die Sie in Schritt 3 dieses Verfahrens erstellt haben

      iii. Wählen Sie Save rules (Regeln speichern) aus.

5. Fügen Sie die EC2-Instance-Sicherheitsgruppe wie folgt zur EC2-Instance hinzu:

   a. Wählen Sie im Navigationsbereich Instances aus.

   b. Wählen Sie Ihre EC2-Instance aus und wählen Sie Actions (Aktionen), Security (Sicherheit), Change security groups (Sicherheitsgruppen ändern) aus.

   c. Wählen Sie unter Associated security groups (Zugeordnete Sicherheitsgruppen) das Feld Select security groups (Sicherheitsgruppen auswählen), wählen Sie ec2-rds-manual-configuration aus, die Sie zuvor erstellt haben, und wählen Sie dann Add security group (Sicherheitsgruppe hinzufügen) aus.

   d. Wählen Sie Speichern.

6. Fügen Sie die RDS-Datenbanksicherheitsgruppe wie folgt zur RDS-Datenbank hinzu:

   a. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.

   b. Wählen Sie im Navigationsbereich Databases (Datenbanken) und wählen Sie Ihre Datenbank aus.

   c. Wählen Sie Ändern aus.

   d. Wählen Sie unter Connectivity (Verbindung) für die Security group (Sicherheitsgruppe), rds-ec2-manual-configuration aus, die Sie zuvor erstellt haben, und wählen Sie dann Continue (Fortfahren) aus.

e. Wählen Sie unter Scheduling of modifications (Planung von Änderungen) die Option Apply immediately (Sofort anwenden) aus.

f. Wählen Sie Modify DB Instance (DB-Instance ändern) aus.

Sie haben jetzt die manuellen Schritte abgeschlossen, die die automatischen Schritte nachahmen, die bei der Verwendung des automatischen Verbindungsfeatures ausgeführt werden.

Sie haben Option 3 dieses Tutorials abgeschlossen. Wenn Sie die Optionen 1, 2 und 3 abgeschlossen haben und die in diesem Tutorial erstellten Ressourcen nicht mehr benötigen, sollten Sie sie löschen, um unnötige Kosten zu vermeiden. Weitere Informationen finden Sie unter Aufgabe 4 (Optional): Aufräumen.

Aufgabe 4 (Optional): Aufräumen

> **Warning**
>
> Das Beenden einer Instance ist dauerhaft und irreversibel.
> Nachdem Sie eine Instance beendet haben, können Sie keine Verbindung mehr zu ihr herstellen und sie kann nicht wiederhergestellt werden. Alle angehängten Amazon-EBS-Volumes, die so konfiguriert sind, dass sie beim Beenden gelöscht werden, werden ebenfalls dauerhaft gelöscht und können nicht wiederhergestellt werden. Alle auf den Instance-Speicher-Volumes gespeicherten Daten gehen dauerhaft verloren. Weitere Informationen finden Sie unter Wie die Kündigung von Instances funktioniert.
> Bevor Sie eine Instance beenden, stellen Sie sicher, dass Sie alle Daten, die Sie nach der Beendigung behalten müssen, im persistenten Speicher gesichert haben.

Nachdem Sie das Tutorial abgeschlossen haben, empfiehlt es sich, alle Ressourcen zu bereinigen (zu löschen), die Sie nicht mehr verwenden möchten. Das Bereinigen von AWS-Ressourcen verhindert, dass weitere Gebühren für Ihr Konto anfallen.

Wenn Sie eine EC2-Instance speziell für dieses Tutorial gestartet haben, können Sie sie beenden, damit keine damit verbundenen Gebühren anfallen.

Um eine Instance mithilfe der Konsole zu beenden

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus, die Sie für dieses Tutorial erstellt haben, und wählen Sie Instance state (Instance-Status), Terminate instance (Instance beenden) aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Beenden aus.

Wenn Sie eine RDS-Datenbank speziell für dieses Tutorial erstellt haben, können Sie sie löschen, damit keine damit verbundenen Gebühren anfallen.

Löschen einer RDS-Datenbank mithilfe der Konsole

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie die RDS-Datenbank aus, die Sie für dieses Tutorial erstellt haben, und wählen Sie Actions (Aktionen), Delete (Löschen) aus.
4. Geben Sie **`delete me`** in das Feld ein und wählen Sie dann Delete (Löschen).

EC2 Flotte und Spot-Flotte

EC2 Fleet und Spot Fleet sind als nützliche Methode konzipiert, um eine Flotte von Dutzenden, Hunderten oder Tausenden von EC2 Amazon-Instances in einem einzigen Vorgang zu starten. Jede Instance in einer Flotte wird entweder durch eine Startvorlage oder durch eine Reihe von Startparametern konfiguriert, die Sie beim Start manuell konfigurieren.

Themen

- Features und Vorteile
- Was ist die beste Flottenmethode?
- Konfigurationsoptionen für Ihre EC2-Flotte oder Spot-Flotte
- Arbeiten Sie mit EC2 Fleet
- Mit Spot-Flotten arbeiten
- Überwachen Sie Ihre EC2 Flotte oder Spot-Flotte
- Tutorials für EC2-Flotte
- CLI-Beispielkonfigurationen für EC2 Fleet
- Beispiel für CLI-Konfigurationen der Spot-Flotte
- Kontingente für EC2 Fleet und Spot-Flotte

Features und Vorteile

Flotten bieten die folgenden Funktionen und Vorteile, sodass Sie bei der Ausführung von Anwendungen auf mehreren EC2 Instances maximale Kosteneinsparungen erzielen und Verfügbarkeit und Leistung optimieren können.

Mehrere Instance-Typen

Eine Flotte kann mehrere Instance-Typen starten, wodurch sichergestellt wird, dass sie nicht von der Verfügbarkeit eines einzelnen Instance-Typs abhängig ist. Dies erhöht die Gesamtverfügbarkeit der Instances in Ihrer Flotte.

Aufteilen von Instances in mehrere Availability Zones

Eine Flotte kann in mehrere Availability Zones starten, sodass Sie Kosten senken und die Verfügbarkeit verbessern können. Wenn Ihre Flotte Spot Instances umfasst, wählt die Flotte

automatisch Availability Zones auf der Grundlage Ihrer Präferenzen in Bezug auf Preis und Unterbrechungen aus.

Vielfältige Kaufoptionen

Eine Flotte kann mehrere Kaufoptionen (Spot- und On-Demand-Instances) starten, so dass Sie die Kosten durch die Nutzung von Spot-Instances optimieren können. Sie können auch Rabatte für Reserved Instances und Savings Plan nutzen, indem Sie sie in Verbindung mit On-Demand-Instances in der Flotte verwenden.

Automatischer Ersatz von Spot Instances

Wenn Ihre Flotte Spot Instances umfasst, kann sie automatisch Ersatz-Spot-Kapazität anfordern, falls Ihre Spot Instances unterbrochen werden. Durch den Kapazitätsausgleich kann eine Flotte auch Ihre Spot Instances überwachen und proaktiv ersetzen, die einem erhöhten Risiko einer Unterbrechung ausgesetzt sind.

On-Demand-Kapazität reservieren

Eine Flotte kann eine On-Demand-Kapazitätsreservierung verwenden, um On-Demand-Kapazität zu reservieren. Eine Flotte kann auch Kapazitätsblöcke für ML enthalten, die es Ihnen ermöglichen, GPU-Instances für einen späteren Zeitpunkt zu reservieren, um Ihre kurzzeitigen Machine Learning (ML)-Workloads zu unterstützen.

Was ist die beste Flottenmethode?

Als allgemeine bewährte Methode empfehlen wir, Flotten von Spot- und On-Demand-Instances mit Amazon EC2 Auto Scaling zu starten, da es zusätzliche Funktionen bietet, mit denen Sie Ihre Flotte verwalten können. Die Liste der zusätzlichen Funktionen umfasst den automatischen Ersatz von Integritätsprüfungen für Spot- und On-Demand-Instances, anwendungsbasierte Zustandsprüfungen und eine Integration mit ELB, um eine gleichmäßige Verteilung des Anwendungsverkehrs auf Ihre fehlerfreien Instances sicherzustellen. Sie können Amazon EC2 Auto Scaling Scaling-Gruppen auch verwenden, wenn Sie AWS Services wie Amazon ECS, Amazon EKS (selbstverwaltete Knotengruppen) und Amazon VPC Lattice verwenden. Weitere Informationen finden Sie im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Wenn Sie Amazon EC2 Auto Scaling nicht verwenden können, sollten Sie die Verwendung von EC2 Fleet oder Spot Fleet in Betracht ziehen. EC2 Fleet und Spot Fleet bieten dieselbe Kernfunktionalität. EC2 Fleet ist jedoch nur über eine Befehlszeile verfügbar und bietet keine Konsolenunterstützung.

Spot-Flotte bietet Konsolenunterstützung, basiert jedoch auf einer Legacy-API ohne geplante Investition.

Bestimmen Sie anhand der folgenden Tabelle, welche Flottenmethode verwendet werden soll.

FlottenmethodeFlotteFlotte	Wann sollte dies verwendet werden?	Anwendungsfall
Amazon EC2 Auto Scaling	• Sie benötigen mehrere Instances mit einer einzigen Konfiguration oder einer gemischten Konfiguration. • Sie möchten das Lebenszyklusmanagement Ihrer Instances automatisieren.	Erstellen Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe, die den Lebenszyklus Ihrer Instances verwaltet und gleichzeitig die gewünschte Anzahl von Instances beibehält. Unterstützt die horizontale Skalierung (Hinzufügen weiterer Instances) zwischen festgelegten Mindest- und Maximalgrenzen.
EC2 Flotte	• Sie benötigen mehrere Instances mit einer einzigen Konfiguration oder einer gemischten Konfiguration. • Sie möchten Ihren Instance-Lebenszyklus selbst verwalten. • Wenn Sie kein Auto Scaling benötigen, empfehlen wir Ihnen, einen `instant` Typ EC2 Fleet zu verwenden.	Erstellen Sie eine `instant`-Flotte von On-Demand-Instances und Spot Instances in einem einzigen Vorgang mit mehreren Startspezifikationen, die sich nach Instance-Typ, AMI, Availability Zone oder Subnetz unterscheiden. Die Spot-Instance-Allokationsstrategie ist standardmäßig auf `lowest-price` pro Einheit eingestellt, aber Sie können die Einstellung auf `price-capacity-optimized` ändern.
Spot-Flotte	• Wir raten dringend davon ab, die Spot-Flotte zu verwenden, da es sich	Verwenden Sie Spot Fleet nur, wenn Sie Konsolenunterstützung für einen Anwendungsfall

FlottenmethodeFlotteFlotte	Wann sollte dies verwendet werden?	Anwendungsfall
	um eine Legacy-API ohne geplante Investition handelt. • Wenn Sie Ihren Instance-Lebenszyklus verwalten möchten, verwenden Sie lieber EC2 Fleet. • Wenn Sie Ihren Instance-Lebenszyklus nicht verwalten möchten, verwenden Sie lieber eine Amazon EC2 Auto Scaling Scaling-Gruppe.	benötigen, in dem Sie EC2 Fleet verwenden würden.

Konfigurationsoptionen für Ihre EC2-Flotte oder Spot-Flotte

Bei der Planung Ihrer EC2-Flotte oder Spot-Flotte empfehlen wir Ihnen, die folgenden Optionen in Betracht zu ziehen, wenn Sie entscheiden, wie Sie Ihre Flotte konfigurieren.

Konfigurationsoption	Frage	Dokumentation
Art der Flottanforderung	Möchten Sie eine Flotte, die eine einmalige Anfrage für die gewünschte Zielkapazität stellt, oder eine Flotte, die die Zielkapazität im Laufe der Zeit beibehält?	EC2-Flotten- und Spot-Flotten-Anforderungstypen
Spot-Instances	Planen Sie, Spot Instances in Ihre Flotte aufzunehmen? Nutzen Sie diese bewährten Methoden für Spot bei der Planung Ihrer Flotte, damit Sie die Instances zum niedrigstmöglichen Preis bereitstellen können.	Bewährte Methoden für Amazon EC2 Spot

Konfigurationsoption	Frage	Dokumentation
Ausgabenlimit für Ihre Flotte	Möchten Sie einschränken, wie viel Sie pro Stunde für Ihre Flotte zahlen werden?	Ausgabenlimit für Ihre EC2-Flotte oder Spot-Flotte festlegen
Instance-Typen und attributbasierte Auswahl von Instance-Typen	Möchten Sie die Instance-Typen in Ihrer Flotte angeben oder Amazon EC2 die Instance-Typen auswählen lassen, die Ihren Anwendungsanforderungen entsprechen?	Geben Sie Attribute für die Auswahl von Instance-Typen für EC2-Flotte oder Spot-Flotte an
Instance-Gewichtung	Möchten Sie jedem Instance-Typ Gewichtungen zuweisen, um deren Rechenkapazität und Leistung darzustellen, sodass Amazon EC2 eine beliebige Kombination verfügbarer Instance-Typen auswählen kann, um Ihre gewünschte Zielkapazität zu erreichen?	Instance-Gewichtung verwenden, um die Kosten und die Leistung Ihrer EC2-Flotte oder Spot-Flotte zu verwalten
Zuweisungsstrategien	Möchten Sie entscheiden, ob Sie die verfügbare Kapazität, den Preis oder die Instance-Typen für die Spot Instances und On-Demand-Instances in Ihrer Flotte optimieren möchten?	Verwenden Sie Zuweisungsstrategien, um festzustellen, wie die EC2-Flotte oder Spot-Flotte die Spot- und On-Demand-Kapazitäten ausfüllt
Kapazitätsausgleich	Möchten Sie, dass Ihre Flotte gefährdete Spot Instances automatisch ersetzt?	Den Kapazitätsausgleich in der EC2-Flotte und der Spot-Flotte verwenden, um gefährdete Spot Instances zu ersetzen

Konfigurationsoption	Frage	Dokumentation
On-Demand-Kapazitätsreservierung	Möchten Sie Kapazität für die On-Demand-Instances in Ihrer Flotte reservieren?	Kapazitätsreservierungen verwenden, um On-Demand-Kapazitäten in der EC2-Flotte zu reservieren

EC2-Flotten- und Spot-Flotten-Anforderungstypen

Der Anforderungstyp für eine EC2-Flotte oder Spot-Flotte bestimmt, ob die Anforderung synchron oder asynchron ist und ob es sich um eine einmalige Anforderung für die gewünschte Zielkapazität oder um einen kontinuierlichen Versuch handelt, die Kapazität dauerhaft aufrechtzuerhalten. Bei der Konfiguration Ihrer Flotte müssen Sie den Anforderungstyp angeben.

Sowohl EC2-Flotte als auch Spot-Flotte bieten zwei Anforderungstypen: `request` und`maintain`. Darüber hinaus bietet EC2-Flotte einen dritten Anfragetyp namens `instant`.

Flotten-Anforderungstypen

`instant` (Nur EC2-Flotte)

Wenn Sie den Anforderungstyp als `instant` konfigurieren, erstellt EC2-Flotte eine einmalige, synchrone Anforderung für Ihre gewünschte Kapazität. In der API-Antwort gibt er die gestarteten Instances zurück sowie die Fehler für Instances, die nicht gestartet werden konnten. Weitere Informationen finden Sie unter EC2-Flotte des Typs instant konfigurieren.

`request`

Wenn Sie den Anforderungstyp als `request` konfigurieren, erstellt die Flotte eine einmalige, asynchrone Anforderung für Ihre gewünschte Kapazität. Wenn die Kapazität aufgrund von Spot-Unterbrechungen abnimmt, versucht die Flotte weder, Spot Instances aufzufüllen, noch stellt sie Anfragen in alternativen Spot-Kapazitätspools, wenn die Kapazität nicht verfügbar ist. Um eine Spot-Flotte des Typs `request` mit der Konsole zu erstellen, wählen Sie das Kontrollkästchen Erhalten der Zielkapazität ab.

`maintain` (Standard)

Wenn Sie den Anforderungstyp als `maintain` konfigurieren, erstellt Spot-Flotte eine asynchrone Anforderung für Ihre gewünschte Kapazität und erhält die Kapazität aufrecht, indem sie alle unterbrochenen Spot Instances automatisch auffüllt. Um eine Spot-Flotte des Typs `maintain` mit der Konsole zu erstellen, wählen Sie das Kontrollkästchen Erhalten der Zielkapazität aus

EC2-Flotte des Typs instant konfigurieren

Die EC2-Flotte des Typs Instant ist eine einmalige, synchrone Anforderung, die nur einen Versuch macht, die gewünschte Kapazität zu starten. Die API-Antwort gibt die gestarteten Instances zurück sowie die Fehler für Instances, die nicht gestartet werden konnten. Die Verwendung einer EC2-Flotte des Typs Instant, die in diesem Artikel beschrieben werden, hat mehrere Vorzüge. Beispielkonfigurationen finden Sie am Ende des Artikels.

Für Workloads, die eine Nur-Start-API zum Starten von EC2-Instances benötigen, können Sie die RunInstances API verwenden. Mit RunInstances können Sie jedoch nur On-Demand-Instances oder Spot-Instances starten, aber nicht beide in derselben Anforderung. Wenn Sie RunInstances zum Starten von Spot-Instances verwenden, ist Ihre Spot-Instance-Anforderung außerdem auf einen Instance-Typ und eine Availability Zone beschränkt. Dies zielt auf einen Spot-Kapazitätspool ab (eine Reihe von unbenutzten Instances mit gleichem Instance-Typ und gleicher Availability Zone). Wenn der Spot-Kapazitätspool nicht über ausreichende Spot-Instance-Kapazität für Ihre Anforderung verfügt, schlägt der RunInstances-Aufruf fehl.

Anstatt RunInstances zum Starten von Spot-Instances zu verwenden, empfehlen wir, die CreateFleet-API für folgende Vorteile lieber mit dem `type`-Parameterwert auf `instant` zu setzen:

- Launchen von On-Demand-Instances und Spot Instances in einer Anforderung. Eine EC2-Flotte kann On-Demand-Instances, Spot-Instances oder beides starten. Die Anforderung für Spot-Instances ist erfüllt, wenn ausreichend Kapazität verfügbar ist und der maximale Preis pro Stunde für Ihre Anforderung den Spot-Preis überschreitet.
- Erhöhen Sie die Verfügbarkeit von Spot Instances. Durch die Verwendung einer EC2-Flotte des Typs `instant` können Sie Spot-Instances nach den Bewährte Methoden für Spot mit den daraus resultierenden Vorteilen starten:
  - Bewährte Methoden für Spot: Flexibel sein bei Instance-Typen und Availability Zones.

    Vorteil: Durch die Angabe mehrerer Instance-Typen und Availability Zones erhöhen Sie die Anzahl der Spot-Kapazitätspools. Dies gibt dem Spot-Dienst eine bessere Chance, die

gewünschte Spot-Rechenkapazität zu finden und zuzuweisen. Eine gute Faustregel besteht darin, für jeden Workload über mindestens 10 Instance-Typen hinweg flexibel zu sein und sicherzustellen, dass alle Availability Zones für die Verwendung in Ihrer VPC konfiguriert sind.

- Bewährte Methoden für Spot: Nutzung der price-capacity-optimized Zuweisungsstrategie.

  Vorteil: Die Zuweisungsstrategie `price-capacity-optimized` identifiziert Instances aus den am meisten verfügbaren Spot-Kapazitätspools und stellt dann automatisch Instances aus dem preisgünstigsten dieser Pools bereit. Da Ihre Spot-Instance-Kapazität aus Pools mit optimaler Kapazität bezogen wird, verringert dies die Möglichkeit, dass Ihre Spot-Instances unterbrochen werden, wenn Amazon EC2 die Kapazität zurück braucht.

- Erhalten Sie Zugriff auf eine breitere Palette von Funktionen. Für Workloads, die eine Nur-Start-API benötigen und bei denen Sie den Lebenszyklus Ihrer Instance lieber verwalten möchten, anstatt der EC2-Flotte diese für Sie verwalten zu lassen, verwenden Sie die EC2-Flotte vom Typ `instant` anstelle der RunInstances-API. Die EC2-Flotte bietet eine breitere Palette von Funktionen als RunInstances, wie in den folgenden Beispielen gezeigt. Für alle anderen Workloads sollten Sie Amazon EC2 Auto Scaling verwenden, da es ein umfassenderes Feature-Umfang für eine Vielzahl von Workloads bietet, wie beispielsweise ELB-unterstützte Anwendungen, containerisierte Workloads und Warteschlangenverarbeitungsaufträge.

Sie können eine EC2-Flotte vom Typ instant verwenden, um Instances in Kapazitätsblöcken zu starten. Weitere Informationen finden Sie unter Tutorial: Ihre EC2-Flotte konfigurieren, um Instances in Kapazitätsblöcken zu starten.

AWS-Services wie Amazon EC2 Auto Scaling und Amazon EMR verwenden EC2-Flotte vom Typ Instant, um EC2-Instances zu starten.

Voraussetzungen für EC2-Flotte des Typs Instant

Informationen zu den Voraussetzungen für das Erstellen einer EC2-Flotte finden Sie unter EC2 Voraussetzungen für die Flotte.

So funktioniert die Instant-EC2-Flotte

Bei der Arbeit mit einer EC2-Flotte des Typs `instant` lautet die Ereignisabfolge wie folgt:

1. Konfigurieren: Konfigurieren Sie den Anforerungstyp CreateFleet als `instant`. Weitere Informationen finden Sie unter Erstellen Sie eine EC2 Flotte. Beachten Sie, dass Sie den API-Aufruf nicht ändern können, nachdem Sie ihn machen.

2. Anforderung: Wenn Sie den API-Aufruf durchführen, erstellt Amazon EC2 eine einmalige, synchrone Anforderung für Ihre gewünschte Kapazität.
3. Antwort: Die API-Antwort gibt die gestarteten Instances zurück sowie die Fehler für Instances, die nicht gestartet werden konnten.
4. Beschreiben: Sie können Ihre EC2-Flotte beschreiben, die Instances auflisten, die der EC2-Flotte zudeordnet sind, und den Verlauf Ihrer EC2-Flotte anzeigen.
5. Instances beenden: Sie können die Instances jederzeit beenden.
6. Flottenanforderung löschen: Die Flottenanforderung kann entweder manuell oder automatisch gelöscht werden:
   - Manuell: Sie können die Flottenanforderung löschen, nachdem Sie die Instances gestartet haben.

     Beachten Sie, dass eine gelöschte `instant`-Flotte mit laufenden Instances nicht unterstützt wird. Wenn Sie eine `instant`-Flotte löschen, beendet Amazon EC2 automatisch alle zugehörigen Instances. Bei Flotten mit mehr als 1 000 Instances schlägt die Löschanforderung möglicherweise fehl. Wenn Ihre Flotte über mehr als 1 000 Instances verfügt, beenden Sie die meisten Instances zunächst manuell, sodass 1 000 oder weniger übrig bleiben. Löschen Sie dann die Flotte, und die verbleibenden Instances werden automatisch beendet.
   - Automatisch: Amazon EC2 löscht die Flottenanforderung einige Zeit nach einem der folgenden Ereignissen:
     - Alle Instances werden beendet.
     - Die Flotte kann keine Instances starten.

Beispiele

In den folgenden Beispielen wird gezeigt, wie Sie eine EC2-Flotte des Typs `instant` für verschiedene Anwendungsfälle nutzen. Weitere Informationen zur Verwendung der EC2-CreateFleet-API-Parameter finden Sie unter CreateFleet in der Amazon EC2 API-Referenz.

Beispiele

- Beispiel 1: Starten von Spot-Instances mit der kapazitätsoptimierten Zuweisungsstrategie
- Beispiel 2: Starten einer einzelnen Spot-Instance mit der kapazitätsoptimierten Zuweisungsstrategie
- Beispiel 3: Starten einer Spot-Instance mit Instance-Gewichtung
- Beispiel 4: Spot Instances innerhalb einer einzelnen Availability Zone starten

- Beispiel 5: Starten von Spot-Instances eines einzelnen Instance-Typs innerhalb einer Availability Zone
- Beispiel 6: Spot-Instances nur starten, wenn minimale Zielkapazität gestartet werden kann
- Beispiel 7: Starten Sie Spot-Instances nur, wenn die minimale Zielkapazität desselben Instance-Typs in einer einzigen Availability Zone gestartet werden kann
- Beispiel 8: Starten von Instances mit mehreren Startvorlagen
- Beispiel 9: Starten von Spot-Instance mit einer Basis von On-Demand-Instances
- Beispiel 10: Starten von Spot-Instances mit kapazitätsoptimierter Zuweisungsstrategie mit einer Basis von On-Demand-Instances unter Verwendung von Kapazitätsreservierungen und der priorisierten Zuweisungsstrategie
- Beispiel 11: Starten von Spot-Instances mit kapazitätsoptimierter priorisierter Zuweisungsstrategie
- Beispiel 12: Einen Systems-Manager-Parameters anstelle einer AMI-ID angeben

Beispiel 1: Starten von Spot-Instances mit der kapazitätsoptimierten Zuweisungsstrategie

Das folgende Beispiel gibt die Parameter an, die in einer EC2-Flotte des Typs `instant` benötigt werden: eine Startvorlage, eine Zielkapazität, eine Standard-Kaufoption und Startvorlagenüberschreibungen.

- Die Startvorlage wird durch ihren Startvorlagennamen und die Versionsnummer identifiziert.
- In den 12 Startvorlagenüberschreibungen werden 4 verschiedene Instance-Typen und 3 verschiedene Subnetze angegeben, die sich jeweils in einer separaten Availability Zone befinden. Jeder Instance-Typ und jede Subnetzkombination definiert einen Spot-Kapazitätspool, der zu 12 Spot-Kapazitätspools führt.
- Die Mindest-Zielkapazität für die Flotte ist 20 Instances.
- Die standardmäßige Kaufoption ist `spot`, wodurch die Flotte versucht, 20 Spot-Instances in dem Spot-Kapazitätspool zu starten, der über die optimale Kapazität für die Anzahl der zu startenden Instances verfügt.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
```

```
        "LaunchTemplateSpecification":{
           "LaunchTemplateName":"ec2-fleet-lt1",
           "Version":"$Latest"
        },
        "Overrides":[
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"m5.large",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"m5.large",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"m5.large",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"m5d.large",
              "SubnetId":"subnet-fae8c380"
```

```
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Beispiel 2: Starten einer einzelnen Spot-Instance mit der kapazitätsoptimierten Zuweisungsstrategie

Sie können eine Spot-Instance gleichzeitig optimal starten, indem Sie mehrere EC2-Flotten-API-Aufrufe vom Typ `instant` durchführen, indem Sie die TotalTargetCapacity auf 1 setzen.

Das folgende Beispiel gibt die Parameter an, die in einer EC2-Flotte des Typs Instant benötigt werden: eine Startvorlage, eine Zielkapazität, eine Standard-Kaufoption und Startvorlagenüberschreibungen. Die Startvorlage wird durch ihren Startvorlagennamen und die Versionsnummer identifiziert. Die 12 Startvorlagenüberschreibungen haben 4 verschiedene Instance-Typen und 3 verschiedene Subnetze, die sich jeweils in einer separaten Availability Zone befinden. Die Zielkapazität für die Flotte beträgt 1 Instance und die Standardeinkaufoption ist Spot, was dazu führt, dass die Flotte versucht, eine Spot-Instance aus einem der 12 Spot-Kapazitätspools basierend auf der kapazitätsoptimierten Zuweisungsstrategie zu starten, um eine Spot-Instance aus dem am meisten verfügbaren Kapazitätspool zu starten.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
```

```
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
```

```
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Beispiel 3: Starten einer Spot-Instance mit Instance-Gewichtung

Die folgenden Beispiele verwenden die Instance-Gewichtung, d. h. der Preis versteht sich pro Einheitsstunde anstatt pro Instance-Stunde. Jede Startkonfiguration listet einen anderen Instance-Typ und eine andere Gewichtung auf, je nachdem, wie viele Einheiten des Workloads auf der Instance ausgeführt werden können, sofern eine Einheit der Workload 15 GB Arbeitsspeicher und 4 vCPUs benötigt. Zum Beispiel kann ein m5.xlarge (4 vCPUs und 16 GB Speicher) eine Einheit ausführen und ist gewichtet 1, m5.2xlarge (8 vCPUs und 32 GB Speicher) kann 2 Einheiten ausführen und ist gewichtet 2 usw. Die gesamte Zielkapazität wird auf 40 Einheiten eingestellt. Die Standardeinkaufoption ist vor Ort, und die Allokationsstrategie ist kapazitätsoptimiert, was entweder 40 m5.xlarge (40 geteilt durch 1), 20 m5.2xlarge (40 geteilt durch 2), 10 m5.4xlarge (40 geteilt durch 4), 5 m5.8xlarge (40 geteilt durch 8) oder eine Mischung der Instance-Typen mit Gewichtungen, die zu den gewünschten Kapazität basierend auf der kapazitätsoptimierten Zuweisungsstrategie.

Weitere Informationen finden Sie unter Instance-Gewichtung verwenden, um die Kosten und die Leistung Ihrer EC2-Flotte oder Spot-Flotte zu verwalten.

```
{
   "SpotOptions":{
      "AllocationStrategy":"capacity-optimized"
   },
   "LaunchTemplateConfigs":[
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
```

```
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":2
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":2
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":2
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":4
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":4
            },
            {
```

```
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":4
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":8
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":8
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":8
            }
         ]
      }
   ],
   "TargetCapacitySpecification":{
      "TotalTargetCapacity":40,
      "DefaultTargetCapacityType":"spot"
   },
   "Type":"instant"
}
```

Beispiel 4: Spot Instances innerhalb einer einzelnen Availability Zone starten

Sie können eine Flotte so konfigurieren, dass alle Instances in einer einzigen Availability Zone gestartet werden, indem Sie die Spot-Optionen SingleAvailabilityZone auf true festlegen.

Die 12 Startvorlagenüberschreibungen haben unterschiedliche Instance-Typen und Subnetze (jeweils in einer separaten Availability Zone), aber die gleiche gewichtete Kapazität. Die Gesamtzielkapazität beträgt 20 Instances, die voreingestellte Kaufoption ist spot und die Spot-Zuweisungsstrategie ist kapazitätsoptimiert. Die EC2-Flotte startet 20 Spot-Instances in einem einzigen AZ, aus dem Spot-Kapazitätspool (s) mit optimaler Kapazität unter Verwendung der Launch-Spezifikationen.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
```

```
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
```

```
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Beispiel 5: Starten von Spot-Instances eines einzelnen Instance-Typs innerhalb einer Availability Zone

Sie können eine Flotte so konfigurieren, dass alle Instances desselben Instance-Typs und in einer einzelnen Availability Zone gestartet werden, indem Sie SpotOptions SingleInstanceType auf true und SingleAvailabilityZone auf true festlegen.

Die 12 Startvorlagenüberschreibungen haben unterschiedliche Instance-Typen und Subnetze (jeweils in einer separaten Availability Zone), aber die gleiche gewichtete Kapazität. Die Gesamtzielkapazität beträgt 20 Instances, die voreingestellte Kaufoption ist spot, die Spot-Zuweisungsstrategie ist kapazitätsoptimiert. Die EC2-Flotte startet 20 Spot-Instances desselben Instance-Typs in einem einzigen AZ aus dem Spot-Instance-Pool mit optimaler Kapazität unter Verwendung der Startspezifikationen.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true
```

```
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
```

```
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Beispiel 6: Spot-Instances nur starten, wenn minimale Zielkapazität gestartet werden kann

Sie können eine Flotte so konfigurieren, dass Instances nur gestartet werden können, wenn die minimale Zielkapazität gestartet werden kann, indem Sie die Spot-Optionen MinTargetCapacity auf die minimale Zielkapazität festlegen, die Sie gemeinsam starten möchten.

Wenn Sie MinTargetCapacity angeben, müssen Sie mindestens einen der folgenden Parameter angeben: SingleInstanceType oder SingleAvailabilityZone. In diesem Beispiel wird SingleInstanceType angegeben, sodass alle 20 Instances den gleichen Instance-Typ verwenden müssen.

Die 12 Startvorlagenüberschreibungen haben unterschiedliche Instance-Typen und Subnetze (jeweils in einer separaten Availability Zone), aber die gleiche gewichtete Kapazität. Die Gesamtzielkapazität und die minimale Zielkapazität sind beide auf 20 Instances festgelegt, die Standard-Kaufoption ist Spot, die Spot-Zuweisungsstrategie ist kapazitätsoptimiert. Die EC2-Flotte startet 20 Spot-Instances aus dem Spot-Kapazitätspool mit optimaler Kapazität unter Verwendung der Startvorlagenüberschreibungen nur, wenn alle 20 Instances gleichzeitig gestartet werden können.

```
{
    "SpotOptions": {
```

```
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
```

```
                "InstanceType":"m5.4xlarge",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Beispiel 7: Starten Sie Spot-Instances nur, wenn die minimale Zielkapazität desselben Instance-Typs in einer einzigen Availability Zone gestartet werden kann

Sie können eine Flotte so konfigurieren, dass Instances nur gestartet werden können, wenn die minimale Zielkapazität mit einem einzelnen Instance-Typ in einer einzigen Availability Zone gestartet werden kann, indem Sie die Spot-Optionen MinTargetCapacity auf die minimale Zielkapazität festlegen, die Sie zusammen mit SingleInstanceType und SingleAvailabilityZone Optionen starten möchten.

Die 12 Startspezifikationen, die die Startvorlage überschreiben, haben unterschiedliche Instance-Typen und Subnetze (jede in einer separaten Availability Zone), aber die gleiche gewichtete Kapazität. Die gesamte Zielkapazität und die minimale Zielkapazität sind beide auf 20 Instances festgelegt, die Standardeinkaufoption ist Spot, die Spot-Allokationsstrategie ist kapazitätsoptimiert, der SingleInstanceType ist true und SingleAvailabilityZone ist true. Die EC2-Flotte startet 20 Spot-Instances desselben Instance-Typs in einem einzigen AZ aus dem Spot-Kapazitätspool mit optimaler

Kapazität unter Verwendung der Startspezifikationen nur, wenn alle 20 Instances gleichzeitig gestartet werden können.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
```

```
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5.4xlarge",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5.4xlarge",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-49e41922"
            }
        ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Beispiel 8: Starten von Instances mit mehreren Startvorlagen

Sie können eine Flotte so konfigurieren, dass Instances mit unterschiedlichen Startspezifikationen für verschiedene Instance-Typen oder eine Gruppe von Instance-Typen gestartet werden, indem Sie mehrere Startvorlagen angeben. In diesem Beispiel wollen wir verschiedene EBS-Volume-Größen für verschiedene Instance-Typen haben und wir haben das in den Launch-Vorlagen ec2-fleet-lt-4xl, ec2-fleet-lt-9xl und ec2-fleet-lt-18xl konfiguriert.

In diesem Beispiel verwenden wir 3 verschiedene Startvorlagen für die 3 Instance-Typen, die auf ihrer Größe basieren. Die Startspezifikations-Überschreibungen für alle Startvorlagen verwenden Instance-Gewichtungen basierend auf den vCPUs des Instance-Typs. Die Gesamtzielkapazität

beträgt 144 Einheiten, die voreingestellte Kaufoption ist Spot und die Spot-Zuweisungsstrategie ist kapazitätsoptimiert. Die EC2-Flotte kann entweder 9 c5n.4xlarge (144 geteilt durch 16) mit der Startvorlage ec2-fleet-4xl oder 4 c5n.9xlarge (144 geteilt durch 36) mit der Startvorlage ec2-fleet-9xl oder 2 c5n.18xlarge (144 geteilt durch 72) mit der Startvorlage ec2-fleet-18xl oder eine Mischung der Instance-Typen mit Gewichtungen bis zur gewünschten Kapazität basierend auf der kapazitätsoptimierten Allokationsstrategie starten.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-18xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":72
            },
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":72
            },
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":72
            }
         ]
      },
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-9xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.9xlarge",
```

```
            "SubnetId":"subnet-fae8c380",
            "WeightedCapacity":36
         },
         {
            "InstanceType":"c5n.9xlarge",
            "SubnetId":"subnet-e7188bab",
            "WeightedCapacity":36
         },
         {
            "InstanceType":"c5n.9xlarge",
            "SubnetId":"subnet-49e41922",
            "WeightedCapacity":36
         }
      ]
   },
   {
      "LaunchTemplateSpecification":{
         "LaunchTemplateName":"ec2-fleet-lt-4xl",
         "Version":"$Latest"
      },
      "Overrides":[
         {
            "InstanceType":"c5n.4xlarge",
            "SubnetId":"subnet-fae8c380",
            "WeightedCapacity":16
         },
         {
            "InstanceType":"c5n.4xlarge",
            "SubnetId":"subnet-e7188bab",
            "WeightedCapacity":16
         },
         {
            "InstanceType":"c5n.4xlarge",
            "SubnetId":"subnet-49e41922",
            "WeightedCapacity":16
         }
      ]
   }
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 144,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
```

```
}
```

Beispiel 9: Starten von Spot-Instance mit einer Basis von On-Demand-Instances

Das folgende Beispiel gibt die Gesamtzielkapazität von 20 Instances für die Flotte und eine Zielkapazität von 5 On-Demand-Instances an. Die Standard-Kaufoption ist Spot. Die Flotte startet 5 On-Demand-Instances wie angegeben, muss aber noch 15 weitere Instance starten, um die gesamte Zielkapazität zu erreichen. Die Kaufoption für die Differenz wird berechnet als TotalTargetCapacity — OnDemandTargetCapacity = DefaultTargetCapacityType, was dazu führt, dass die Flotte 15 Spot-Instances von einer der 12 Spot-Kapazitätspools startet, die auf der kapazitätsoptimierten Zuweisungsstrategie basieren.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab"
```

```
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Beispiel 10: Starten von Spot-Instances mit kapazitätsoptimierter Zuweisungsstrategie mit einer Basis von On-Demand-Instances unter Verwendung von Kapazitätsreservierungen und der priorisierten Zuweisungsstrategie

Sie können eine Flotte so konfigurieren, dass sie On-Demand-Kapazitätsreservierungen zuerst beim Start einer Basis von On-Demand-Instances mit dem standardmäßigen Zielkapazitätstyp wie Spot verwendet, indem Sie die Nutzungsstrategie für Kapazitätsreservierungen auf use-capacity-reservations-first festlegt. Und wenn mehrere Instance-Pools nicht verwendete Kapazitätsreservierungen haben, wird die gewählte On-Demand-Zuordnungsstrategie angewendet. In diesem Beispiel ist die On-Demand-Zuordnungsstrategie prioritisiert.

In diesem Beispiel sind 6 nicht verwendete Kapazitätsreservierungen verfügbar. Dies ist geringer als die On-Demand-Zielkapazität der Flotte von 10 On-Demand-Instances.

Das Konto hat die folgenden 6 nicht verwendeten Kapazitätsreservierungen in 2 Pools. Die Anzahl der Kapazitätsreservierungen in jedem Pool wird durch AvailableInstanceCount angezeigt.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Die folgende Flottenkonfiguration zeigt nur die relevanten Konfigurationen für dieses Beispiel. Die On-Demand-Zuordnungsstrategie ist priorisiert und die Nutzungsstrategie für Kapazitätsreservierungen ist use-capacity-reservations-first. Die Spot-Zuweisungsstrategie ist kapazitätsoptimiert. Die

Gesamtzielkapazität beträgt 20, die On-Demand-Zielkapazität beträgt 10 und der voreingestellte Zielkapazitätstyp ist Spot.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "OnDemandOptions":{
       "CapacityReservationOptions": {
         "UsageStrategy": "use-capacity-reservations-first"
       },
       "AllocationStrategy":"prioritized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 3.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 4.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab",
```

```
            "Priority": 5.0
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-49e41922",
            "Priority": 6.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-fae8c380",
            "Priority": 7.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-e7188bab",
            "Priority": 8.0
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-49e41922",
            "Priority": 9.0
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-fae8c380",
            "Priority": 10.0
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-e7188bab",
            "Priority": 11.0
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-49e41922",
            "Priority": 12.0
         }
      ]
   }
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "OnDemandTargetCapacity": 10,
    "DefaultTargetCapacityType": "spot"
```

```
    },
    "Type": "instant"
}
```

Nachdem Sie die Instant-Flotte mit der vorherigen Konfiguration erstellt haben, werden die folgenden 20 Instances gestartet, um die Zielkapazität zu erreichen:

- 7 c5.large On-Demand-Instances in us-east-1a – c5.large in us-east-1a wird zuerst priorisiert und es gibt drei verfügbare, nicht verwendete c5.large-Kapazitätsreservierungen. Die Kapazitätsreservierungen werden zuerst verwendet, um 3 On-Demand-Instances zu starten; dazu werden vier zusätzliche On-Demand-Instances gemäß der On-Demand-Zuordnungsstrategie gestartet, die in diesem Beispiel priorisiert sind.
- 3 m5.large On-Demand-Instances in us-east-1a – m5.large in us-east-1a wird zweitrangig priorisiert und es gibt drei verfügbare, nicht verwendete c3.large-Kapazitätsreservierungen.
- 10 Spot-Instances aus einem der 12 Spot-Kapazitätspools mit der optimalen Kapazität gemäß der kapazitätsoptimierten Zuweisungsstrategie.

Nachdem die Flotte gestartet wurde, können Sie describe-capacity-reservations ausführen, um zu sehen, wie viele nicht verwendete Kapazitätsreservierungen noch übrig sind. In diesem Beispiel sollten Sie die folgende Antwort sehen, die zeigt, dass alle c5.large- und m5.large-Kapazitätsreservierungen verwendet wurden.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "AvailableInstanceCount": 0
}
```

Beispiel 11: Starten von Spot-Instances mit kapazitätsoptimierter priorisierter Zuweisungsstrategie

Das folgende Beispiel gibt die Parameter an, die in einer EC2-Flotte des Typs Instant benötigt werden: eine Startvorlage, eine Zielkapazität, eine Standard-Kaufoption und Startvorlagenüberschreibungen. Die Startvorlage wird durch ihren Startvorlagennamen und die

Versionsnummer identifiziert. Die 12 Startspezifikationen, die die Startvorlage außer Kraft setzen, haben 4 verschiedene Instance-Typen mit einer zugeordneten Priorität und 3 verschiedene Subnetze je in einer separaten Availability Zone. Die Zielkapazität für die Flotte beträgt 20 Instances, und die Standardeinkaufoption ist Spot-Option, was dazu führt, dass die Flotte versucht, 20 Spot-Instances aus einem der 12 Spot-Kapazitätspools basierend auf der kapazitätsoptimierten Allokationsstrategie zu starten, die Prioritäten nach bestem Bemühen umsetzt, optimiert aber zuerst für die Kapazität.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 2.0
            },
```

```
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 2.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 3.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 3.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 3.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 4.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 4.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 4.0
            }
         ]
      }
   ],
   "TargetCapacitySpecification": {
       "TotalTargetCapacity": 20,
       "DefaultTargetCapacityType": "spot"
   },
   "Type": "instant"
```

```
}
```

Beispiel 12: Einen Systems-Manager-Parameters anstelle einer AMI-ID angeben

Im folgenden Beispiel wird eine Startvorlage verwendet, um die Konfiguration für die Instances in der Flotte anzugeben. In diesem Beispiel wird für `ImageId` anstelle der Angabe einer AMI-ID mit einem Systemmanager-Parameter auf das AMI verwiesen. Beim Start der Instance wird der Systems-Manager-Parameter in eine AMI-ID aufgelöst.

In diesem Beispiel wird der Systems-Manager-Parameter in einem gültigen Format angegeben: `resolve:ssm:golden-ami`. Es gibt andere gültige Formate für den Systems-Manager-Parameter. Weitere Informationen finden Sie unter Verwenden eines Systems-Manager-Parameters anstelle einer AMI-ID.

> **Note**
>
> Der Flottentyp muss vom Typ sein `instant`. Bei anderen Flotten-Typen wird die Angabe eines Systems-Manager-Parameters anstelle einer AMI-ID nicht unterstützt.

```
{
    "LaunchTemplateData": {
        "ImageId": "resolve:ssm:golden-ami",
        "InstanceType": "m5.4xlarge",
        "TagSpecifications": [{
            "ResourceType": "instance",
            "Tags": [{
                "Key": "Name",
                "Value": "webserver"
            }]
        }]
    }
}
```

Ausgabenlimit für Ihre EC2-Flotte oder Spot-Flotte festlegen

Sie können ein Limit festlegen, wie viel Sie bereit sind, pro Stunde für Ihre EC2-Flotte oder Spot-Flotte auszugeben. Wenn Ihr Ausgabenlimit erreicht ist, startet die Flotte keine Instances mehr, auch wenn die Zielkapazität noch nicht erreicht ist.

Es gibt separate Ausgabenlimits für On-Demand-Instances und Spot Instances.

Ein Ausgabenlimit für On-Demand-Instances und Spot Instances in Ihrer EC2-Flotte konfigurieren

Verwenden Sie den Befehl create-fleet und die folgenden Parameter:

- Für On-Demand-Instances: Geben Sie in der `OnDemandOptions`-Struktur Ihr Ausgabenlimit in das `MaxTotalPrice`-Feld ein.
- Für Spot Instances: Geben Sie in der `SpotOptions`-Struktur Ihr Ausgabenlimit im `MaxTotalPrice`-Feld an.

Ein Ausgabenlimit für On-Demand-Instances und Spot Instances in Ihrer Spot-Flotte konfigurieren

Sie können die Amazon-EC2-Konsole oder die AWS CLI verwenden, um Ihr Ausgabenlimit zu konfigurieren.

(Konsole) Aktivieren Sie bei der Erstellung der Spot-Flotte das Kontrollkästchen Höchstkosten für Spot Instances festlegen und geben Sie dann einen Wert für Maximale Kosten festlegen (pro Stunde) ein. Weitere Informationen finden Sie in Schritt 6.e unter Eine Spot-Flottenanforderung mit definierten Parametern erstellen.

(AWS CLI) Verwenden Sie den Befehl request-spot-fleet und die folgenden Parameter:

- Für On-Demand-Instances: Geben Sie im Feld `OnDemandMaxTotalPrice` Ihr Ausgabenlimit an.
- Für Spot Instances: Geben Sie Ihr Ausgabenlimit in das `SpotMaxTotalPrice`-Feld ein.

Beispiele

Im folgenden Beispiel werden zwei verschiedene Szenarien gezeigt. Im ersten Beispiel beendet die Flotte den Start von On-Demand-Instances, wenn sie die für On-Demand-Instances festgelegte Zielkapazität (`OnDemandTargetCapacity`) erreicht hat. Im zweiten Beispiel stoppt die Flotte das Starten von On-Demand-Instances, wenn die maximale Summe erreicht ist, die Sie bereit sind für On-Demand-Instances zu zahlen (`MaxTotalPrice`).

Beispiel: Kein Starten mehr von On-Demand-Instances, wenn die Zielkapazität erreicht ist

Bei einer Anforderung für `m4.large` On-Demand-Instances mit:

- On-Demand-Preis: 0,10 USD pro Stunde

- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 1,50 USD

Die Flotte startet 10 On-Demand-Instances, da der Gesamtpreis von 1,00 USD (10 Instances x 0,10 USD) den `MaxTotalPrice` von 1,50 USD für On-Demand-Instances nicht überschreitet.

Beispiel: Kein Starten mehr von Instances, wenn der Höchstpreis erreicht ist

Bei einer Anforderung für `m4.large` On-Demand-Instances mit:

- On-Demand-Preis: 0,10 USD pro Stunde
- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 0,80 USD

Wenn die Flotte die On-Demand-Zielkapazität (10 On-Demand-Instances) startet, betragen die Gesamtkosten pro Stunde 1,00 USD. Dies überschreitet die Summe (0,80 USD), die als `MaxTotalPrice` für On-Demand-Instances festgelegt ist. Damit Sie nicht mehr ausgeben, als Sie möchten, startet die Flotte nur 8 On-Demand-Instances (weniger als die On-Demand-Zielkapazität), da sonst der `MaxTotalPrice` für On-Demand-Instances überschritten werden würde.

Instances mit Spitzenlastleistung

Wenn Sie Ihre Spot-Instances mit einem Typ von Burstable Performance Instance starten, und wenn Sie planen, Ihre Spot-Instances mit Spitzenlastleistung sofort und für eine kurze Dauer zu verwenden, ohne Leerlaufzeit für die Anrechnung von CPU-Guthaben, empfiehlt sich, diese im Standard mode (Standardmodus) zu starten, um höhere Kosten zu vermeiden. Wenn Sie die Spot Instances mit Spitzenlastleistung im Unlimited mode (Unbegrenzten Modus) starten und die Spitzenlastleistung der CPU sofort nutzen, geben Sie überschüssiges Guthaben für Spitzen aus. Wenn Sie die Instance für eine kurze Zeit nutzen, hat die Instance keine Zeit, CPU-Guthaben zu sammeln, um das überschüssige Guthaben zu bezahlen. Das überschüssige Guthaben wir beim Beenden der Instance abgerechnet.

Der unbegrenzte Modus für Spot Instances mit Spitzenlastleistung ist nur dann geeignet, wenn die Instance lange genug läuft, um CPU-Guthaben für Spitzen zu erhalten. Andernfalls macht das Bezahlen für überzähliges Guthaben die Spot Instances mit Spitzenlastleistung teurer als die Verwendung anderer Instances. Weitere Informationen finden Sie unter Verwendung des unbegrenzten Modus im Vergleich zu einer festen CPU.

Startguthaben sollen eine produktive erste Starterfahrung für T2-Instances bieten, indem sie ausreichende Rechenressourcen zur Verfügung gestellt werden, um die Instance zu konfigurieren. Wiederholte Starts von T2-Instances, um neue Startguthaben zu erhalten, sind nicht zulässig. Wenn Sie dauerhaft eine CPU benötigen, können Sie Guthaben verdienen (durch Leerlauf über einen gewissen Zeitraum), Unbegrenzten Modus für T2 Spot Instances verwenden oder einen Instance-Typ mit dedizierter CPU verwenden.

Geben Sie Attribute für die Auswahl von Instance-Typen für EC2-Flotte oder Spot-Flotte an

Wenn Sie eine EC2-Flotte oder Spot-Flotte erstellen, müssen Sie mindestens einen Instance-Typ für die Konfiguration der On-Demand-Instances und Spot Instances in der Flotte angeben. Alternativ zur manuellen Angabe der Instance-Typen können Sie die Attribute angeben, die eine Instance haben muss, und Amazon EC2 identifiziert alle Instance-Typen mit diesen Attributen. Dies ist bekannt als attributbasierte Instance-Typauswahl. Sie können beispielsweise die minimale und maximale Anzahl von vCPUs angeben, die für Ihre Instances erforderlich sind, und die Flotte startet die Instances mit allen verfügbaren Instance-Typen, die diese vCPU-Anforderungen erfüllen.

Die attributbasierte Auswahl von Instance-Typen ist ideal für Workloads und Frameworks, die hinsichtlich der verwendeten Instance-Typen flexibel sein können, etwa beim Ausführen von Containern oder Web-Flotten, beim Verarbeiten von Big Data und der Implementierung von Tools zur fortlaufenden Integration und Bereitstellung (CI/CD).

Vorteile

Die Auswahl des attributbasierten Instance-Typs bietet folgende Vorteile:

- Einfacher Einsatz der richtigen Instance-Typen – Da so viele Instance-Typen verfügbar sind, kann es zeitaufwendig sein, die richtigen Instance-Typen für Ihre Workload zu finden. Wenn Sie Instance-Attribute angeben, haben die Instance-Typen automatisch die erforderlichen Attribute für Ihre Workload.
- Vereinfachte Konfiguration – Um mehrere Instance-Typen für eine Flotte manuell anzugeben, müssen Sie für jeden Instance-Typ eine separate Überschreibung der Startvorlagen erstellen. Bei der attributbasierten Auswahl von Instance-Typen müssen Sie jedoch nur die Instance-Attribute in der Startvorlage oder in einer Startvorlagen-Überschreibung angeben, um mehrere Instance-Typen bereitzustellen.

- Automatische Verwendung neuer Instance-Typen – Wenn Sie Instance-Attribute anstelle von Instance-Typen angeben, kann Ihre Flotte bei der Freigabe Instance-Typen einer neueren Generation verwenden, um die Zukunftsfähigkeit der Flottenkonfiguration zu gewährleisten.
- Flexible Instance-Typen – Wenn Sie Instance-Attribute anstelle von Instance-Typen angeben, kann die Spot-Flotte aus einer Vielzahl von Instance-Typen zum Starten von Spot Instances auswählen, was der bewährten Spot-Methode der Flexibilität von Instance-Typen entspricht.

Themen

- Attributbasierte Auswahl von Instance-Typen
- Preisschutz
- Leistungsschutz
- Überlegungen
- Erstellen einer EC2-Flotte mit attributbasierter Auswahl von Instance-Typen
- Erstellen einer Spot-Flotte mit attributbasierter Auswahl von Instance-Typen
- Beispiele für EC2-Flotte-Konfigurationen, die gültig und ungültig sind
- Beispiele für Spot-Flotte-Konfigurationen, die gültig und ungültig sind
- Vorschau von Instance-Typen mit bestimmten Attributen

Attributbasierte Auswahl von Instance-Typen

Um die attributbasierte Auswahl von Instance-Typen in Ihrer Flottenkonfiguration zu verwenden, ersetzen Sie die Liste der Instance-Typen durch eine Liste von Instance-Attributen, die Ihre Instances erfordern. Die EC2-Flotte oder Spot-Flotte startet Instances für alle verfügbaren Instance-Typen mit den angegebenen Instance-Attributen.

Themen

- Arten von Instance-Attributen
- Wo wird die attributbasierte Auswahl von Instance-Typen konfiguriert?
- Wie die EC2-Flotte oder Spot-Flotte bei der Bereitstellung einer Flotte die attributbasierte Auswahl von Instance-Typen verwendet

Arten von Instance-Attributen

Es gibt mehrere Instance-Attribute, die Sie angeben können, um Ihre Datenverarbeitungsanforderungen auszudrücken, wie:

- vCPU-Anzahl – Die minimale und maximale Anzahl von vCPUs pro Instance.
- Arbeitsspeicher – Die minimalen und maximalen GiBs Arbeitsspeicher pro Instance.
- Lokaler Speicher – Ob EBS- oder Instance-Speicher-Volumes für den lokalen Speicher verwendet werden sollen.
- Burstable Performance – Gibt an, ob die T-Instance-Familie verwendet werden soll, einschließlich der Typen T4g, T3a, T3 und T2.

Eine Beschreibung der einzelnen Attribute und der Standardwerte finden Sie unter InstanceRequirements in der Amazon-EC2-API-Referenz.

Wo wird die attributbasierte Auswahl von Instance-Typen konfiguriert?

Je nachdem, ob Sie die Konsole oder die AWS CLI verwenden, können Sie die Instance-Attribute für die attributbasierte Auswahl von Instance-Typen wie folgt angeben:

In der Konsole können Sie die Instance-Attribute in einer oder beiden der folgenden Flottenkonfigurationskomponenten angeben:

- In einer Startvorlage. Verweisen Sie dann in der Flottenanforderung auf die Startvorlage
- (Nur Spot-Flotte) In der Flottenanfrage

In der AWS CLI können Sie die Instance-Attribute in einer oder allen der folgenden Flottenkonfigurationskomponenten angeben:

- In einer Startvorlage. Verweisen Sie dann in der Flottenanforderung auf die Startvorlage
- In einer Startvorlagen-Überschreibung

  Wenn Sie eine Mischung aus Instances wünschen, die verschiedene AMIs verwenden, können Sie Instance-Attribute in mehreren Startvorlagen-Überschreibungen angeben. Zum Beispiel können verschiedene Instance-Typen x86- und ARM-basierte Prozessoren verwenden.
- (Nur Spot-Flotte) In einer Startspezifikation

Wie die EC2-Flotte oder Spot-Flotte bei der Bereitstellung einer Flotte die attributbasierte Auswahl von Instance-Typen verwendet

Die EC2-Flotte oder Spot-Flotte stellt eine Flotte auf folgende Weise bereit:

- Sie identifiziert die Instance-Typen mit den angegebenen Attributen.
- Sie bestimmt anhand des Preisschutzes, welche Instance-Typen ausgeschlossen werden sollen.
- Sie bestimmt die Kapazitätspools, aus denen die Instances gestartet werden sollen, basierend auf den AWS-Regionen oder Availability Zones mit übereinstimmenden Instance-Typen.
- Sie wendet die angegebene Zuweisungsstrategie an, um zu bestimmen, aus welchen Kapazitätspools die Instances gestartet werden sollen.

  Beachten Sie, dass die attributbasierte Auswahl von Instance-Typen nicht die Kapazitätspools auswählt, aus denen die Flotte bereitgestellt werden soll. Dies ist die Aufgabe der Zuweisungsstrategien.

  Wenn Sie eine Zuweisungsstrategie angeben, startet die Flotte Instances gemäß der angegebenen Zuweisungsstrategie.

  - Bei Spot Instances unterstützt die attributbasierte Auswahl von Instance-Typen die Preis-Kapazitätsoptimierte, kapazitätsoptimierte und niedrigstpreisige Zuweisungsstrategien. Beachten Sie, dass wir nicht die Spot-Allokationsstrategie mit dem niedrigsten Preis empfehlen, da sie das höchste Unterbrechungsrisiko für Ihre Spot Instances birgt.
  - Für On-Demand-Instances unterstützt die attributbasierte Auswahl von Instance-Typen die niedrigstpreisige Zuweisungsstrategie.
- Wenn es keine Kapazität für die Instance-Typen mit den angegebenen Instance-Attributen gibt, können keine Instances gestartet werden und die Flotte gibt einen Fehler zurück.

Preisschutz

Der Preisschutz ist ein Feature, das verhindert, dass IhreEC2-Flotte oder Spot-Flotte Instance-Typen verwendet, die Sie für zu teuer halten würden, selbst wenn sie den von Ihnen angegebenen Attributen entsprechen. Um den Preisschutz zu nutzen, legen Sie einen Preisgrenzwert fest. Wenn Amazon EC2 Instance-Typen mit Ihren Attributen auswählt, werden Instance-Typen ausgeschlossen, die über Ihrem Schwellenwert liegen.

Amazon EC2 berechnet den Preisschwellenwert wie folgt:

- Amazon EC2 identifiziert zunächst den Instance-Typ mit dem niedrigsten Preis aus den Instance-Typen, die Ihren Attributen entsprechen.
- Amazon EC2 nimmt dann den Wert (ausgedrückt als Prozentsatz), den Sie für den Preisschutzparameter angegeben haben, und multipliziert ihn mit dem Preis des identifizierten Instance-Typs. Das Ergebnis ist der Preis, der als Preisschwellenwert verwendet wird.

Es gibt separate Preisschwellenwert für On-Demand-Instances und Spot Instances.

Wenn Sie eine Flotte mit attributbasierter Auswahl von Instance-Typen erstellen, ist der Preisschutz standardmäßig aktiviert. Sie können die Standardwerte beibehalten oder Ihre eigenen angeben.

Sie können den Preisschutz auch deaktivieren. Um anzugeben, dass es keinen Preisschutzschwellenwert gibt, geben Sie einen hohen Prozentsatz an, z. B. 999999.

Themen

- Wie der Instance-Typ mit dem niedrigsten Preis identifiziert wird
- On-Demand-Instance-Preisschutz
- Spot-Instance-Preisschutz
- Schwellenwert für Preisschutz angeben

Wie der Instance-Typ mit dem niedrigsten Preis identifiziert wird

Amazon EC2 bestimmt den Preis, auf dem der Preisschwellenwert basieren soll, indem es den Instance-Typ mit dem niedrigsten Preis aus den Instance-Typen identifiziert, die Ihren angegebenen Attributen entsprechen. Das macht es auf folgende Weise:

- Zunächst werden die Instance-Typen C, M oder R der aktuellen Generation betrachtet, die Ihren Attributen entsprechen. Wenn es Übereinstimmungen findet, wird der Instance-Typ mit dem niedrigsten Preis identifiziert.
- Wenn es keine Übereinstimmung gibt, sucht es nach allen Instance-Typen der aktuellen Generation, die Ihren Attributen entsprechen. Wenn es Übereinstimmungen findet, wird der Instance-Typ mit dem niedrigsten Preis identifiziert.
- Wenn es keine Übereinstimmung gibt, sucht es nach allen Instance-Typen der vorherigen Generation, die Ihren Attributen entsprechen, und identifiziert den Instance-Typ mit dem niedrigsten Preis.

On-Demand-Instance-Preisschutz

Der Schwellenwert für den Preisschutz für On-Demand-Instance-Typen wird als Prozentsatz berechnet, der über dem identifizierten On-Demand-Instance-Typ mit dem niedrigsten Preis liegt (`OnDemandMaxPricePercentageOverLowestPrice`). Sie geben den höheren Prozentsatz an, den Sie zu zahlen bereit sind. Wenn Sie diesen Parameter nicht angeben, wird ein Standardwert von `20` verwendet, um einen Preisschutzschwellenwert zu berechnen, der 20 % über dem identifizierten Preis liegt.

Wenn der identifizierte On-Demand-Instance-Preis beispielsweise `0.4271` ist, und Sie `25` angeben, liegt der Preisschwellenwert 25 % über `0.4271`. Die Berechnung ist wie folgt: `0.4271 * 1.25 = 0.533875`. Der berechnete Preis ist der Höchstbetrag, den Sie bereit sind, für On-Demand-Instances zu zahlen. In diesem Beispiel schließt Amazon EC2 alle On-Demand-Instance-Typen aus, die mehr als `0.533875` kosten.

Spot-Instance-Preisschutz

Standardmäßig wendet Amazon EC2 automatisch einen optimalen Spot-Instance-Preisschutz an, sodass konsistent aus einer breiten Palette von Instance-Typen ausgewählt werden kann. Sie können den Preisschutz auch manuell selbst festlegen. Wenn Sie dies jedoch Amazon EC2 für Sie erledigen lassen, können Sie die Wahrscheinlichkeit erhöhen, dass Ihre Spot-Kapazität erfüllt ist.

Sie können den Preisschutz mit einer der folgenden Optionen manuell angeben. Wenn Sie den Preisschutz manuell festlegen, empfehlen wir, die erste Option zu verwenden.

- Ein Prozentsatz des identifizierten On-Demand-Instance-Typs mit dem niedrigsten Preis [`MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`]

  Wenn der angegebene Preis für den On-Demand-Instance-Typ beispielsweise `0.4271` ist und Sie `60` angeben, liegt der Preisgrenzwert bei 60 % von `0.4271`. Die Berechnung ist wie folgt: `0.4271 * 0.60 = 0.25626`. Der berechnete Preis ist der Höchstbetrag, den Sie bereit sind, für Spot Instances zu zahlen. In diesem Beispiel schließt Amazon EC2 alle Spot-Instance-Typen aus, die mehr als `0.25626` kosten.
- Ein Prozentsatz, der höher ist als der identifizierte Spot-Instance-Typ mit dem niedrigsten Preis [`SpotMaxPricePercentageOverLowestPrice`]

  Wenn der Preis für den identifizierten Spot-Instance-Typ beispielsweise `0.1808` ist und Sie `25` angeben, liegt der Preisschwellenwert 25 % über `0.1808`. Die Berechnung ist wie folgt: `0.1808 * 1.25 = 0.226`. Der berechnete Preis ist der Höchstbetrag, den Sie bereit sind, für Spot Instances

zu zahlen. In diesem Beispiel schließt Amazon EC2 alle Spot-Instance-Typen aus, die mehr als `0.266` kosten. Wir empfehlen die Verwendung dieses Parameters nicht, da die Spot-Preise schwanken können und daher auch Ihr Preisschutzschwellenwert schwanken kann.

Schwellenwert für Preisschutz angeben

Schwellenwert für Preisschutz mit der AWS CLI angeben

Konfigurieren Sie beim Erstellen der EC2-Flotte oder Spot-Flotte mit der AWS CLI die Flotte für eine attributbasierte Auswahl des Instance-Typs und gehen Sie dann folgendermaßen vor:

- Zum Angeben des Schwellenwerts zum Preisschutz für On-Demand-Instances geben Sie in der JSON-Konfigurationsdatei in der `InstanceRequirements`-Struktur für `OnDemandMaxPricePercentageOverLowestPrice` den Preisschutzschwellenwert als Prozentsatz ein.
- Zum Angeben des Schwellenwerts zum Preisschutz für Spot-Instances geben Sie in der JSON-Konfigurationsdatei in der `InstanceRequirements`-Struktur einen der folgenden Parameter an:
  - Geben Sie bei `MaxSpotPriceAsPercentageOfOptimalOnDemandPrice` den Preisschutzschwellenwert als Prozentsatz ein.
  - Geben Sie bei `SpotMaxPricePercentageOverLowestPrice` den Preisschutzschwellenwert als Prozentsatz ein.

Weitere Informationen finden Sie unter Erstellen einer EC2-Flotte mit attributbasierter Auswahl von Instance-Typen oder Erstellen einer Spot-Flotte mit attributbasierter Auswahl von Instance-Typen.

(Nur Spot-Flotte) Schwellenwert für Preisschutz mit der Konsole angeben

Konfigurieren Sie beim Erstellen der Spot-Flotte in der Konsole die Flotte für eine attributbasierte Auswahl des Instance-Typs und gehen Sie dann folgendermaßen vor:

- Zur Eingabe des Schwellenwerts für On-Demand-Instance-Preisschutz wählen Sie unter Zusätzliches Instance-Attribut die Option On-Demand-Preisschutz aus. Wählen Sie dann Attribut hinzufügen aus.
- Um den Schwellenwert für die Preisgarantie einer Spot Instance festzulegen, wählen Sie Zusätzliches Instance-Attribut, wählen Sie Spot-Preisschutz, wählen Sie Attribut hinzufügen, wählen Sie einen Basiswert, auf dem Ihr Preis basieren soll, und geben Sie dann den Schwellenwert für die Preisgarantie als Prozentsatz ein.

> **Note**
>
> Wenn Sie beim Erstellen der Flotte `TargetCapacityUnitType` auf `vcpu` oder `memory-mib` festlegen, wird der Schwellenwert für den Preisschutz anhand des Preises pro vCPU oder pro Arbeitsspeicher anstelle des Preises pro Instance angewendet.

Leistungsschutz

Der Leistungsschutz ist eine Funktion, die sicherstellt, dass Ihre EC2-Flotte oder Spot-Flotte Instance-Typen verwendet, die einer bestimmten Leistungsbasislinie ähnlich sind oder diese übertreffen. Um den Leistungsschutz zu nutzen, geben Sie eine Instance-Familie als Basisreferenz an. Die Funktionen der angegebenen Instance-Familie stellen das niedrigste akzeptable Leistungsniveau dar. Bei der Auswahl von Instance-Typen für Ihre Flotte berücksichtigt Amazon EC2 Ihre angegebenen Attribute und die Leistungsbasis. Instance-Typen, die unter die Leistungsbasis fallen, werden automatisch von der Auswahl ausgeschlossen, auch wenn sie Ihren anderen angegebenen Attributen entsprechen. Dadurch wird sichergestellt, dass alle ausgewählten Instance-Typen eine ähnliche oder bessere Leistung als die von der angegebenen Instance-Familie festgelegte Leistungsbasis bieten. Amazon EC2 verwendet diese Baseline als Leitfaden für die Auswahl des Instance-Typs, es gibt jedoch keine Garantie dafür, dass die ausgewählten Instance-Typen immer die Basis für jede Anwendung überschreiten.

Derzeit unterstützt dieses Feature nur die CPU-Leistung als Basisleistungsfaktor. Die CPU-Leistung des CPU-Prozessors der angegebenen Instance-Familie dient als Leistungsbasis und stellt sicher, dass die ausgewählten Instance-Typen dieser Basislinie ähnlich sind oder diese übertreffen. Instance-Familien mit denselben CPU-Prozessoren führen zu denselben Filterergebnissen, auch wenn sich ihre Netzwerk- oder Festplattenleistung unterscheidet. Wenn Sie beispielsweise entweder `c6in` oder `c6i` als Basisreferenz angeben, würde dies zu identischen leistungsbasierten Filterergebnissen führen, da beide Instance-Familien denselben CPU-Prozessor verwenden.

Nicht unterstützte Instance-Familien

Die folgenden Instance-Familien werden aus Gründen des Leistungsschutzes nicht unterstützt:

- `c1`
- `g3 | g3s`
- `hpc7g`
- `m1 | m2`

- `mac1` | `mac2` | `mac2-m1ultra` | `mac2-m2` | `mac2-m2pro`
- `p3dn` | `p4d` | `p5`
- `t1`
- `u-12tb1` | `u-18tb1` | `u-24tb1` | `u-3tb1` | `u-6tb1` | `u-9tb1` | `u7i-12tb` | `u7in-16tb` | `u7in-24tb` | `u7in-32tb`

Wenn Sie den Leistungsschutz aktivieren, indem Sie eine unterstützte Instance-Familie angeben, schließen die zurückgegebenen Instance-Typen die oben genannten nicht unterstützten Instance-Familien aus.

Wenn Sie eine nicht unterstützte Instance-Familie als Wert für die Basisleistung angeben, gibt die API eine leere Antwort für GetInstance-TypesFromInstanceRequirements und eine Ausnahme für CreateFleet, RequestSpotFleet, ModifyFleet und ModifySpotFleetRequest zurück.

Beispiel: Einen Basiswert für die CPU-Leistung festlegen

Im folgenden Beispiel besteht die Instance-Anforderung darin, mit Instance-Typen zu starten, deren CPU-Kerne genauso leistungsfähig sind wie die `c6i`-Instance-Familie. Dadurch werden Instance-Typen mit weniger leistungsstarken CPU-Prozessoren herausgefiltert, auch wenn sie Ihre anderen angegebenen Instance-Anforderungen erfüllen, z. B. die Anzahl der vCPUs. Wenn Ihre angegebenen Instance-Attribute beispielsweise 4 vCPUs und 16 GB Arbeitsspeicher umfassen, wird ein Instance-Typ mit diesen Attributen, aber mit einer geringeren CPU-Leistung als `c6i`, von der Auswahl ausgeschlossen.

```
"BaselinePerformanceFactors": {
        "Cpu": {
            "References": [
                {
                    "InstanceFamily": "c6i"
                }
            ]
        }
```

Überlegungen

- Sie können entweder Instance-Typen oder Instance-Attribute in einer EC2-Flotte oder Spot-Flotte angeben, aber nicht beides gleichzeitig.

Wenn Sie die CLI verwenden, überschreiben die Startvorlagen-Überschreibungen die Startvorlage. Wenn die Startvorlage beispielsweise einen Instance-Typ enthält und die Startvorlagen-Überschreibung Instance-Attribute enthält, überschreiben die Instances, die durch die Instance-Attribute identifiziert werden, den Instance-Typ in der Startvorlage.

- Wenn Sie die CLI verwenden und Instance-Attribute als Überschreibungen angeben, können Sie nicht auch Gewichtungen oder Prioritäten angeben.
- Sie können maximal vier `InstanceRequirements`-Strukturen in einer Anforderungskonfiguration angeben.

Erstellen einer EC2-Flotte mit attributbasierter Auswahl von Instance-Typen

Sie können eine EC2-Flotte so konfigurieren, dass sie die attributbasierte Auswahl von Instance-Typen verwendet. Es ist nicht möglich, eine EC2-Flotte mit der Amazon-EC2-Konsole zu erstellen.

Die Attribute für die attributbasierte Auswahl von Instance-Typen werden in der `InstanceRequirements`-Struktur angegeben. Wenn `InstanceRequirements` in der Flottenkonfiguration enthalten ist, müssen `InstanceType` und `WeightedCapacity` ausgeschlossen werden. Sie können die Flottenkonfiguration nicht gleichzeitig mit den Instance-Attributen bestimmen.

In den Beispielen für AWS CLI und PowerShell werden die folgenden Attribute angegeben:

- `VCpuCount` – Mindestens 2 vCPUs und maximal 4 vCPUs. Wenn Sie kein Höchstlimit benötigen, können Sie den Höchstwert weglassen.
- `MemoryMiB` – Mindestens 8 GiB Arbeitsspeicher und maximal 16 GiB. Wenn Sie kein Höchstlimit benötigen, können Sie den Höchstwert weglassen.

Diese Konfiguration identifiziert alle Instance-Typen mit 2 bis 4 vCPUs und 8 bis 16 GiB Arbeitsspeicher. Der Preisschutz und die Zuweisungsstrategie könnten jedoch einige Instance-Typen ausschließen, wenn die EC2-Flotte die Flotte bereitstellt.

AWS CLI

So erstellen Sie eine EC2-Flotte mit attributbasierter Auswahl von Instance-Typen

Verwenden Sie den Befehl create-fleet, um eine EC2-Flotte zu erstellen. Geben Sie die Flottenkonfiguration in einer JSON-Datei an.

```
aws ec2 create-fleet \
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

Die folgende Beispielsdatei *file_name*.json enthält die Parameter, mit denen eine EC2-Flotte für attributbasierte Auswahl von Instance-Typen konfiguriert wird.

```
{
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized"
    },
    "LaunchTemplateConfigs": [{
        "LaunchTemplateSpecification": {
            "LaunchTemplateName": "my-launch-template",
            "Version": "1"
        },
        "Overrides": [{
            "InstanceRequirements": {
                "VCpuCount": {
                    "Min": 2,
                    "Max": 4
                },
                "MemoryMiB": {
                    "Min": 8192,
                    "Max": 16384
                }
            }
        }]
    }],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

PowerShell

So erstellen Sie eine EC2-Flotte mit attributbasierter Auswahl von Instance-Typen

Verwenden Sie das cmdlet New-EC2Fleet.

```
$vcpuCount = New-Object Amazon.EC2.Model.VCpuCountRangeRequest
```

```
$vcpuCount.Min = 2
$vcpuCount.Max = 4
$memoryMiB = New-Object Amazon.EC2.Model.MemoryMiBRequest
$memoryMiB.Min = 8192
$memoryMiB.Max = 16384
$instanceRequirements = New-Object Amazon.EC2.Model.InstanceRequirementsRequest
$instanceRequirements.VCpuCount = $vcpuCount
$instanceRequirements.MemoryMiB = $memoryMiB

$launchTemplateSpec = New-Object
 Amazon.EC2.Model.FleetLaunchTemplateSpecificationRequest
$launchTemplateSpec.LaunchTemplateName = "my-launch-template"
$launchTemplateSpec.Version = "1"
$override = New-Object Amazon.EC2.Model.FleetLaunchTemplateOverridesRequest
$override.InstanceRequirements = $instanceRequirements
$launchTemplateConfig = New-Object Amazon.EC2.Model.FleetLaunchTemplateConfigRequest
$launchTemplateConfig.LaunchTemplateSpecification = $launchTemplateSpec
$launchTemplateConfig.Overrides = @($override)

New-EC2Fleet `
    -SpotOptions_AllocationStrategy "price-capacity-optimized" `
    -LaunchTemplateConfig @($launchTemplateConfig) `
    -TargetCapacitySpecification_DefaultTargetCapacityType "spot" `
    -TargetCapacitySpecification_TotalTargetCapacity 20 `
    -Type "instant"
```

Erstellen einer Spot-Flotte mit attributbasierter Auswahl von Instance-Typen

Sie können eine Flotte so konfigurieren, dass sie die attributbasierte Auswahl von Instance-Typen verwendet.

Die Attribute für die attributbasierte Auswahl von Instance-Typen werden in der `InstanceRequirements`-Struktur angegeben. Wenn `InstanceRequirements` in der Flottenkonfiguration enthalten ist, müssen `InstanceType` und `WeightedCapacity` ausgeschlossen werden. Sie können die Flottenkonfiguration nicht gleichzeitig mit den Instance-Attributen bestimmen.

In den Beispielen für AWS CLI und PowerShell werden die folgenden Attribute angegeben:

- `VCpuCount` – Mindestens 2 vCPUs und maximal 4 vCPUs. Wenn Sie kein Höchstlimit benötigen, können Sie den Höchstwert weglassen.

- `MemoryMiB` – Mindestens 8 GiB Arbeitsspeicher und maximal 16 GiB. Wenn Sie kein Höchstlimit benötigen, können Sie den Höchstwert weglassen.

Diese Konfiguration identifiziert alle Instance-Typen mit 2 bis 4 vCPUs und 8 bis 16 GiB Arbeitsspeicher. Der Preisschutz und die Zuweisungsstrategie könnten jedoch einige Instance-Typen ausschließen, wenn die Spot-Flotte die Flotte bereitstellt.

Console

So konfigurieren Sie eine Spot-Flotte für die attributbasierte Auswahl von Instance-Typen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Spot-Anforderungen und wählen Sie die Spot-Instances anfordern aus.
3. Befolgen Sie die Schritte zum Erstellen einer Spot-Flotte. Weitere Informationen finden Sie unter Eine Spot-Flottenanforderung mit definierten Parametern erstellen.

   Konfigurieren Sie beim Erstellen der Spot-Flotte wie folgt die Flotte für die attributbasierte Auswahl von Instance-Typen:

   a. Wählen Sie für Instance type requirements (Anforderungen hinsichtlich des Instance-Typs) die Option Specify instance attributes that match your compute requirements (Instance-Attribute angeben, die Ihren Computinganforderungen entsprechen) aus.
   b. Geben Sie für vCPUs die gewünschte minimale und maximale Anzahl der vCPUs ein. Um kein Limit anzugeben, wählen Sie Kein Minimum, Kein Maximum oder beides.
   c. Geben Sie für Arbeitsspeicher (GiB) den gewünschten Mindest- und Höchstwert ein. Um kein Limit anzugeben, wählen Sie Kein Minimum, Kein Maximum oder beide Optionen aus.
   d. (Optional) Für Zusätzliche Instance-Attribute können Sie optional ein oder mehrere Attribute angeben, um Ihre Computinganforderungen genauer auszudrücken. Jedes zusätzliche Attribut fügt Ihrer Anfrage weitere Einschränkungen hinzu.
   e. (Optional) Um die Instance-Typen mit Ihren angegebenen Attributen anzuzeigen, erweitern Sie Vorschau der übereinstimmenden Instance-Typen.

AWS CLI

So konfigurieren Sie eine Spot-Flotte für die attributbasierte Auswahl von Instance-Typen

Verwenden Sie den Befehl request-spot-fleet, um eine Spot-Flotte zu erstellen. Geben Sie die Flottenkonfiguration in einer JSON-Datei an.

```
aws ec2 request-spot-fleet \
    --region us-east-1 \
    --spot-fleet-request-config file://file_name.json
```

Die folgende Beispielsdatei *file_name*.json enthält die Parameter, mit denen eine Spot-Flotte für attributbasierte Auswahl von Instance-Typen konfiguriert wird.

```
{
    "AllocationStrategy": "priceCapacityOptimized",
    "TargetCapacity": 20,
    "Type": "request",
    "LaunchTemplateConfigs": [{
        "LaunchTemplateSpecification": {
            "LaunchTemplateName": "my-launch-template",
            "Version": "1"
        },
        "Overrides": [{
            "InstanceRequirements": {
                "VCpuCount": {
                    "Min": 2,
                    "Max": 4
                },
                "MemoryMiB": {
                    "Min": 8192,
                    "Max": 16384
                }
            }
        }]
    }]
}
```

PowerShell

So konfigurieren Sie eine Spot-Flotte für die attributbasierte Auswahl von Instance-Typen

Verwenden Sie das cmdlet Request-EC2SpotFleet.

```
$vcpuCount = New-Object Amazon.EC2.Model.VCpuCountRange
$vcpuCount.Min = 2
$vcpuCount.Max = 4
```

```
$memoryMiB = New-Object Amazon.EC2.Model.MemoryMiB
$memoryMiB.Min = 8192
$memoryMiB.Max = 16384
$instanceRequirements = New-Object Amazon.EC2.Model.InstanceRequirements
$instanceRequirements.VCpuCount = $vcpuCount
$instanceRequirements.MemoryMiB = $memoryMiB

$launchTemplateSpec = New-Object Amazon.EC2.Model.FleetLaunchTemplateSpecification
$launchTemplateSpec.LaunchTemplateName = "my-launch-template"
$launchTemplateSpec.Version = "1"
$override = New-Object Amazon.EC2.Model.LaunchTemplateOverrides
$override.InstanceRequirements = $instanceRequirements
$launchTemplateConfig = New-Object Amazon.EC2.Model.LaunchTemplateConfig
$launchTemplateConfig.LaunchTemplateSpecification = $launchTemplateSpec
$launchTemplateConfig.Overrides = @($override)

Request-EC2SpotFleet `
    -SpotFleetRequestConfig_AllocationStrategy "PriceCapacityOptimized" `
    -SpotFleetRequestConfig_TargetCapacity 20 `
    -SpotFleetRequestConfig_Type "Request" `
    -SpotFleetRequestConfig_LaunchTemplateConfig $launchTemplateConfig
```

Beispiele für EC2-Flotte-Konfigurationen, die gültig und ungültig sind

Wenn Sie die AWS CLI verwenden, um eine EC2-Flotte zu erstellen, müssen Sie sicherstellen, dass Ihre Flottenkonfiguration gültig ist. Die folgenden Beispiele zeigen gültige und ungültige Konfigurationen.

Konfigurationen gelten als ungültig, wenn sie Folgendes enthalten:

- Eine einzelne `Overrides`-Struktur mit `InstanceRequirements` und `InstanceType`
- Zwei `Overrides`-Strukturen, eine mit `InstanceRequirements` und die andere mit `InstanceType`
- Zwei `InstanceRequirements`-Strukturen mit sich überlappenden Attributwerten innerhalb derselben `LaunchTemplateSpecification`

Beispielkonfigurationen

- Gültige Konfiguration: Einzelstartvorlage mit Überschreibungen
- Gültige Konfiguration: Einzelne Startvorlage mit mehreren InstanceRequirements

- Gültige Konfiguration: Zwei Startvorlagen, jede mit Überschreibungen
- Gültige Konfiguration: Nur InstanceRequirements angegeben, keine überlappenden Attributwerte
- Die Konfiguration ist nicht gültig: Overrides enthalten InstanceRequirements und InstanceType.
- Konfiguration ungültig: Zwei Overrides enthalten InstanceRequirements und InstanceType
- Konfiguration ungültig: Überlappende Attributwerte

Gültige Konfiguration: Einzelstartvorlage mit Überschreibungen

Die folgende Konfiguration ist gültig. Sie enthält eine Startvorlage und eine `Overrides`-Struktur mit einer `InstanceRequirements`-Struktur. Eine Texterklärung der Beispielkonfiguration folgt.

```
{
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5000,
        "DefaultTargetCapacityType": "spot",
```

```
        "TargetCapacityUnitType": "vcpu"
        }
    }
}
```

`InstanceRequirements`

Um die attributbasierte Instance-Auswahl zu verwenden, müssen Sie die `InstanceRequirements`-Struktur in Ihre Flottenkonfiguration aufnehmen und die gewünschten Attribute für die Instances in der Flotte angeben.

Im vorhergehenden Beispiel werden die folgenden Instance-Attribute angegeben:

- `VCpuCount` – Die Instance-Typen müssen mindestens 2 und höchstens 8 vCPUs aufweisen.
- `MemoryMiB` – Die Instance-Typen müssen maximal 10240 MiB Speicher haben. Ein Minimum von 0 bedeutet, dass kein Mindestwert vorhanden ist.
- `MemoryGiBPerVCpu` – Die Instance-Typen müssen maximal 10 000 GiB Speicher pro vCPU haben. Der Parameter `Min` ist optional. Indem Sie ihn weglassen, geben Sie kein Mindestlimit an.

`TargetCapacityUnitType`

Der `TargetCapacityUnitType`-Parameter gibt die Einheit für die Zielkapazität an. Im Beispiel ist die Zielkapazität `5000` und der Typ der Zielkapazitätseinheit `vcpu`. Zusammen geben Sie eine gewünschte Zielkapazität von 5 000 vCPUs an. Die EC2-Flotte wird genügend Instances starten, damit die Gesamtzahl der vCPUs in der Flotte 5 000 vCPUs beträgt.

Gültige Konfiguration: Einzelne Startvorlage mit mehreren InstanceRequirements

Die folgende Konfiguration ist gültig. Sie enthält eine Startvorlage und eine `0verrides`-Struktur mit zwei `InstanceRequirements`-Strukturen. Die in `InstanceRequirements` angegebenen Attribute sind gültig, da sich die Werte nicht überschneiden – die erste `InstanceRequirements`-Struktur gibt eine `VCpuCount` von 0-2 vCPUs an, während die zweite `InstanceRequirements`-Struktur 4-8 vCPUs angibt.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
```

```
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Gültige Konfiguration: Zwei Startvorlagen, jede mit Überschreibungen

Die folgende Konfiguration ist gültig. Sie enthält zwei Startvorlagen mit jeweils einer `Overrides`-Struktur, die eine `InstanceRequirements`-Struktur enthält. Diese Konfiguration ist nützlich für `arm`- und `x86`-Architekturunterstützung in derselben Flotte.

```
{
        "LaunchTemplateConfigs": [
            {
```

```
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
           }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Gültige Konfiguration: Nur **`InstanceRequirements`** angegeben, keine überlappenden Attributwerte

Die folgende Konfiguration ist gültig. Sie enthält zwei `LaunchTemplateSpecification`-Strukturen, jeweils mit einer Startvorlage und einer `Overrides`-Struktur, die eine `InstanceRequirements`-Struktur enthält. Die in `InstanceRequirements` angegebenen Attribute sind gültig, da sich die Werte nicht überschneiden – die erste `InstanceRequirements`-Struktur gibt eine `VCpuCount` von 0-2 vCPUs an, während die zweite `InstanceRequirements`-Struktur 4-8 vCPUs angibt.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
```

```
                        }
                    }
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    }
  }
}
```

Die Konfiguration ist nicht gültig: **`Overrides`** enthalten **`InstanceRequirements`** und **`InstanceType`**.

Die folgende Konfiguration ist ungültig. Die `Overrides`-Struktur enthält `InstanceRequirements` und `InstanceType`. Sie können für `Overrides` `InstanceRequirements` oder `InstanceType` angeben, aber nicht beides.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "MyLaunchTemplate",
                "Version": "1"
            },
            "Overrides": [
            {
                "InstanceRequirements": {
                    "VCpuCount": {
                        "Min": 0,
                        "Max": 2
                    },
                    "MemoryMiB": {
                        "Min": 0
                    }
                }
            },
            {
                "InstanceType": "m5.large"
            }
        ]
```

```
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Konfiguration ungültig: Zwei **`Overrides`** enthalten **`InstanceRequirements`** und **`InstanceType`**

Die folgende Konfiguration ist ungültig. Die `Overrides`-Strukturen enthalten `InstanceRequirements` und `InstanceType`. Sie können entweder `InstanceRequirements` oder `InstanceType` angeben, aber nicht beides, auch wenn sie sich in unterschiedlichen `Overrides`-Strukturen befinden.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
```

```
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Konfiguration ungültig: Überlappende Attributwerte

Die folgende Konfiguration ist ungültig. Die beiden `InstanceRequirements`-Strukturen enthalten jeweils `"VCpuCount": {"Min": 0, "Max": 2}`. Die Werte für diese Attribute überschneiden sich, was zu doppelten Kapazitätspools führt.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
                              "Max": 2
                          },
```

```
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
            }
        ]
    }
  ],
   "TargetCapacitySpecification": {
      "TotalTargetCapacity": 1,
      "DefaultTargetCapacityType": "spot"
  }
 }
}
```

Beispiele für Spot-Flotte-Konfigurationen, die gültig und ungültig sind

Wenn Sie die AWS CLI verwenden, um eine Spot-Flotte zu erstellen, müssen Sie sicherstellen, dass Ihre Flottenkonfiguration gültig ist. Die folgenden Beispiele zeigen gültige und ungültige Konfigurationen.

Konfigurationen gelten als ungültig, wenn sie Folgendes enthalten:

- Eine einzelne `Overrides`-Struktur mit `InstanceRequirements` und `InstanceType`
- Zwei `Overrides`-Strukturen, eine mit `InstanceRequirements` und die andere mit `InstanceType`
- Zwei `InstanceRequirements`-Strukturen mit sich überlappenden Attributwerten innerhalb derselben `LaunchTemplateSpecification`

Beispielkonfigurationen

- Gültige Konfiguration: Einzelstartvorlage mit Überschreibungen
- Gültige Konfiguration: Einzelne Startvorlage mit mehreren InstanceRequirements
- Gültige Konfiguration: Zwei Startvorlagen, jede mit Überschreibungen
- Gültige Konfiguration: Nur InstanceRequirements angegeben, keine überlappenden Attributwerte
- Die Konfiguration ist nicht gültig: Overrides enthalten InstanceRequirements und InstanceType.
- Konfiguration ungültig: Zwei Overrides enthalten InstanceRequirements und InstanceType

- Konfiguration ungültig: Überlappende Attributwerte

Gültige Konfiguration: Einzelstartvorlage mit Überschreibungen

Die folgende Konfiguration ist gültig. Sie enthält eine Startvorlage und eine `Overrides`-Struktur mit einer `InstanceRequirements`-Struktur. Eine Texterklärung der Beispielkonfiguration folgt.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
            ]
        }
    ],
        "TargetCapacity": 5000,
            "OnDemandTargetCapacity": 0,
            "TargetCapacityUnitType": "vcpu"
    }
```

```
}
```

`InstanceRequirements`

Um die attributbasierte Instance-Auswahl zu verwenden, müssen Sie die `InstanceRequirements`-Struktur in Ihre Flottenkonfiguration aufnehmen und die gewünschten Attribute für die Instances in der Flotte angeben.

Im vorhergehenden Beispiel werden die folgenden Instance-Attribute angegeben:

- `VCpuCount` – Die Instance-Typen müssen mindestens 2 und höchstens 8 vCPUs aufweisen.
- `MemoryMiB` – Die Instance-Typen müssen maximal 10240 MiB Speicher haben. Ein Minimum von 0 bedeutet, dass kein Mindestwert vorhanden ist.
- `MemoryGiBPerVCpu` – Die Instance-Typen müssen maximal 10 000 GiB Speicher pro vCPU haben. Der Parameter `Min` ist optional. Indem Sie ihn weglassen, geben Sie kein Mindestlimit an.

`TargetCapacityUnitType`

Der `TargetCapacityUnitType`-Parameter gibt die Einheit für die Zielkapazität an. Im Beispiel ist die Zielkapazität `5000` und der Typ der Zielkapazitätseinheit `vcpu`. Zusammen geben Sie eine gewünschte Zielkapazität von 5 000 vCPUs an. Die Spot-Flotte wird genügend Instances starten, damit die Gesamtzahl der vCPUs in der Flotte 5 000 vCPUs beträgt.

Gültige Konfiguration: Einzelne Startvorlage mit mehreren InstanceRequirements

Die folgende Konfiguration ist gültig. Sie enthält eine Startvorlage und eine `0verrides`-Struktur mit zwei `InstanceRequirements`-Strukturen. Die in `InstanceRequirements` angegebenen Attribute sind gültig, da sich die Werte nicht überschneiden – die erste `InstanceRequirements`-Struktur gibt eine `VCpuCount` von 0-2 vCPUs an, während die zweite `InstanceRequirements`-Struktur 4-8 vCPUs angibt.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
```

```
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Gültige Konfiguration: Zwei Startvorlagen, jede mit Überschreibungen

Die folgende Konfiguration ist gültig. Sie enthält zwei Startvorlagen mit jeweils einer `Overrides`-Struktur, die eine `InstanceRequirements`-Struktur enthält. Diese Konfiguration ist nützlich für `arm`- und `x86`-Architekturunterstützung in derselben Flotte.

```
{
    "SpotFleetRequestConfig": {
```

```
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
```

```
        "Type": "maintain"
    }
}
```

Gültige Konfiguration: Nur **`InstanceRequirements`** angegeben, keine überlappenden Attributwerte

Die folgende Konfiguration ist gültig. Sie enthält zwei `LaunchTemplateSpecification`-Strukturen, jeweils mit einer Startvorlage und einer `Overrides`-Struktur, die eine `InstanceRequirements`-Struktur enthält. Die in `InstanceRequirements` angegebenen Attribute sind gültig, da sich die Werte nicht überschneiden – die erste `InstanceRequirements`-Struktur gibt eine `VCpuCount` von 0-2 vCPUs an, während die zweite `InstanceRequirements`-Struktur 4-8 vCPUs angibt.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
```

```
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Die Konfiguration ist nicht gültig: **`Overrides`** enthalten **`InstanceRequirements`** und **`InstanceType`**.

Die folgende Konfiguration ist ungültig. Die `Overrides`-Struktur enthält `InstanceRequirements` und `InstanceType`. Sie können für `Overrides` `InstanceRequirements` oder `InstanceType` angeben, aber nicht beides.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
```

```
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Konfiguration ungültig: Zwei **`Overrides`** enthalten **`InstanceRequirements`** und **`InstanceType`**

Die folgende Konfiguration ist ungültig. Die `Overrides`-Strukturen enthalten `InstanceRequirements` und `InstanceType`. Sie können entweder `InstanceRequirements` oder `InstanceType` angeben, aber nicht beides, auch wenn sie sich in unterschiedlichen `Overrides`-Strukturen befinden.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
```

```
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Konfiguration ungültig: Überlappende Attributwerte

Die folgende Konfiguration ist ungültig. Die beiden `InstanceRequirements`-Strukturen enthalten jeweils `"VCpuCount": {"Min": 0, "Max": 2}`. Die Werte für diese Attribute überschneiden sich, was zu doppelten Kapazitätspools führt.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
```

```
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
                              "Max": 2
                          },
                          "MemoryMiB": {
                              "Min": 0
                          }
                      }
                  }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Vorschau von Instance-Typen mit bestimmten Attributen

Sie können den Befehl get-instance-types-from-instance-requirements verwenden, um eine Vorschau der Instance-Typen anzuzeigen, die den von Ihnen angegebenen Attributen entsprechen. Dies ist besonders nützlich, um herauszufinden, welche Attribute in Ihrer Anforderungskonfiguration angegeben werden sollen, ohne Instances zu starten. Beachten Sie, dass der Befehl die verfügbare Kapazität nicht berücksichtigt.

So zeigen Sie eine Vorschau einer Liste von Instance-Typen an, indem Sie Attribute mit der angeben AWS CLI

1. (Optional) Um alle möglichen Attribute zu generieren, die angegeben werden können, verwenden Sie den Befehl get-instance-types-from-instance-requirements und den `--generate-cli-skeleton`-Parameter. Sie können die Ausgabe optional in eine Datei umleiten, um sie mit mit zu speichern `input > attributes.json`.

```
aws ec2 get-instance-types-from-instance-requirements \
    --region us-east-1 \
    --generate-cli-skeleton input > attributes.json
```

Erwartete Ausgabe

```
{
    "DryRun": true,
    "ArchitectureTypes": [
        "i386"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 0,
            "Max": 0
        },
        "MemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "CpuManufacturers": [
            "intel"
        ],
        "MemoryGiBPerVCpu": {
            "Min": 0.0,
            "Max": 0.0
        },
        "ExcludedInstanceTypes": [
            ""
        ],
        "InstanceGenerations": [
```

```
            "current"
        ],
        "SpotMaxPricePercentageOverLowestPrice": 0,
        "OnDemandMaxPricePercentageOverLowestPrice": 0,
        "BareMetal": "included",
        "BurstablePerformance": "included",
        "RequireHibernateSupport": true,
        "NetworkInterfaceCount": {
            "Min": 0,
            "Max": 0
        },
        "LocalStorage": "included",
        "LocalStorageTypes": [
            "hdd"
        ],
        "TotalLocalStorageGB": {
            "Min": 0.0,
            "Max": 0.0
        },
        "BaselineEbsBandwidthMbps": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorTypes": [
            "gpu"
        ],
        "AcceleratorCount": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorManufacturers": [
            "nvidia"
        ],
        "AcceleratorNames": [
            "a100"
        ],
        "AcceleratorTotalMemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "NetworkBandwidthGbps": {
            "Min": 0.0,
            "Max": 0.0
        },
```

```
        "AllowedInstanceTypes": [
            ""
        ]
    },
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Erstellen Sie eine JSON-Konfigurationsdatei mit der Ausgabe des vorherigen Schritts und konfigurieren Sie sie wie folgt:

> **Note**
>
> Sie müssen Werte für `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` und `MemoryMiB` angeben. Sie können die anderen Attribute weglassen. In diesem Fall werden die Standardwerte verwendet.
> Eine Beschreibung der einzelnen Attribute und ihrer Standardwerte finden Sie unter get-instance-types-from-instance-requirements.

   a. Geben Sie für `ArchitectureTypes` mindestes einen Prozessorarchitekturtyp an.
   b. Geben Sie für `VirtualizationTypes` mindestens eine Art von Virtualisierung an.
   c. Geben Sie für `VCpuCount` die minimale und maximale Anzahl von vCPUs an. Wenn Sie keine Mindestgrenze angeben möchten, geben Sie `0` für `Min` an. Wenn Sie keine Maximalgrenze angeben möchten, lassen Sie den `Max`-Parameter weg.
   d. Geben Sie für `MemoryMiB` den Mindest- und Höchstwert für Speicher in MiB an. Wenn Sie keine Mindestgrenze angeben möchten, geben Sie `0` für `Min` an. Wenn Sie keine Maximalgrenze angeben möchten, lassen Sie den `Max`-Parameter weg.
   e. Sie können optional eines oder mehrere der anderen Attribute angeben, um die Liste der zurückgegebenen Instance-Typen weiter einzuschränken.

3. Um eine Vorschau der Instance-Typen anzuzeigen, die die von Ihnen in der JSON-Datei angegebenen Attribute aufweisen, verwenden Sie den Befehl get-instance-types-from-instance-requirements und geben Sie mithilfe des `--cli-input-json`-Parameters den Namen und Pfad zu Ihrer JSON-Datei an. Sie können die Ausgabe optional so formatieren, dass sie in einem Tabellenformat angezeigt wird.

```
aws ec2 get-instance-types-from-instance-requirements \
    --cli-input-json file://attributes.json \
```

```
    --output table
```

Beispiel-Datei *Attribute.json*

In diesem Beispiel sind die erforderlichen Attribute in der JSON-Datei enthalten. Sie lauten `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount`, und `MemoryMiB`. Darüber hinaus ist das optionale `InstanceGenerations`-Attribut ebenfalls enthalten. Beachten Sie, dass für `MemoryMiB` der `Max`-Wert weggelassen werden kann, um anzuzeigen, dass kein Grenzwert vorhanden ist.

```
{

    "ArchitectureTypes": [
        "x86_64"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 4,
            "Max": 6
        },
        "MemoryMiB": {
            "Min": 2048
        },
        "InstanceGenerations": [
            "current"
        ]
    }
}
```

Beispielausgabe

```
-----------------------------------------
|GetInstanceTypesFromInstanceRequirements|
+---------------------------------------+
||             InstanceTypes             ||
|+-------------------------------------+|
||             InstanceType              ||
|+-------------------------------------+|
```

```
||  c4.xlarge                           ||
||  c5.xlarge                           ||
||  c5a.xlarge                          ||
||  c5ad.xlarge                         ||
||  c5d.xlarge                          ||
||  c5n.xlarge                          ||
||  d2.xlarge                           ||
...
```

4. Nachdem Sie Instance-Typen identifiziert haben, die Ihren Anforderungen entsprechen, notieren Sie die Instance-Attribute, die Sie verwendet haben, damit Sie sie beim Konfigurieren Ihrer Flottenanforderung verwenden können.

Instance-Gewichtung verwenden, um die Kosten und die Leistung Ihrer EC2-Flotte oder Spot-Flotte zu verwalten

Bei der Instance-Gewichtung weisen Sie jedem Instance-Typ in Ihrer EC2-Flotte oder Spot-Flotte eine Gewichtung zu, um deren Rechenkapazität und Leistung im Verhältnis zueinander darzustellen. Basierend auf der Gewichtung kann die Flotte eine beliebige Kombination der angegebenen Instance-Typen verwenden, sofern sie die gewünschte Zielkapazität erfüllen kann. Dies kann Ihnen helfen, die Kosten und die Leistung Ihrer Flotte zu verwalten.

Die Gewichtung stellt die Kapazitätseinheiten dar, die ein Instance-Typ zur gesamten Zielkapazität beiträgt.

Beispiel: Verwenden Sie die Gewichtung von Instances für das Leistungsmanagement

Angenommen, Ihre Flotte hat zwei Instance-Typen, und Sie weisen jedem Instance-Typ eine unterschiedliche Gewichtung zu, um widerzuspiegeln, wie viele Sie jeweils benötigen, um dieselbe Performance zu erzielen. Gehen Sie wie folgt vor:

- `m5.large` – Gewicht: 1
- `m5.2xlarge` – Gewicht: 4

Wenn Sie diese Gewichtung zuweisen, sagen Sie, dass Sie 4 `m5.large`-Instances benötigen, um dieselbe Leistung wie 1 `m5.2xlarge` zu erzielen.

Verwenden Sie die folgende Formel, um zu berechnen, wie viele Instances jedes Instance-Typs für eine bestimmte Zielkapazität benötigt werden:

```
target capacity / weight = number of instances
```

Wenn Ihre Zielkapazität 8 Einheiten beträgt, könnte die Flotte die Zielkapazität entweder mit einem `m5.large` oder `m5.2xlarge`, einer Kombination aus beidem, wie folgt erreichen:

- 8 `m5.large` Instances (Kapazität von 8 / Gewicht von 1 = 8 Instances)
- 2 `m5.2xlarge` Instances (Kapazität von 8 / Gewicht von 4 = 2 Instances)
- 4 `m5.large` und 1 `m5.2xlarge`

Beispiel: Verwenden Sie die Gewichtung von Instances für das Kostenmanagement

Standardmäßig gilt der von Ihnen angegebene Preis pro Instance-Stunde. Wenn Sie das Feature der Instance-Gewichtung verwenden, gilt der von Ihnen angegebene Preis pro Einheitsstunde. Der Preis pro Einheitsstunde lässt sich errechnen, indem Sie Ihren Preis für einen Instance-Typ durch die Anzahl der Einheiten dividieren, die er darstellt. Die Flotte berechnet die Anzahl der zu startenden Instances, indem die Zielkapazität durch die Instance-Gewichtung geteilt wird. Wenn es sich bei dem Ergebnis nicht um eine Ganzzahl handelt, rundet die Flotte dieses auf die nächste Ganzzahl auf, sodass die Größe Ihrer Flotte nicht unter der Zielkapazität liegt. Die Flotte kann alle Pools auswählen, die Sie in Ihrer Startspezifikation angeben, selbst wenn die Kapazität der gestarteten Instances die angeforderte Zielkapazität übersteigt.

Die folgende Tabelle enthält Beispiele für die Berechnung des Preises pro Einheit für eine Flotte mit einer Zielkapazität von 10.

Instance-Typ	Instance-Gewichtung	Zielkapazität	Anzahl an gestarteten Instances	Preis pro Instance-Stunde	Preis pro Einheitsstunde
`r3.xlarge`	2	10	5 (10 geteilt durch 2)	$0.05	0,025 USD (0,05 geteilt durch 2)
`r3.8xlarge`	8	10	2 (10 geteilt durch 8, Ergebnis	$0.10	0,0125 USD (0,10 geteilt durch 8)

Instance-Typ	Instance-Gewichtung	Zielkapazität	Anzahl an gestarteten Instances	Preis pro Instance-Stunde	Preis pro Einheitsstunde
			aufgerundet)		

Verwenden Sie Flotte Instance-Gewichtung wie folgt, um die gewünschte Zielkapazität in den Pools mit dem niedrigsten Preis pro Einheit zum Zeitpunkt der Erfüllung bereitzustellen:

1. Geben Sie die Zielkapazität für Ihre Flotte entweder in Instances (Standard) oder in den Einheiten Ihrer Wahl an, z. B. virtuelle CPUs, Arbeitsspeicher, Speicher oder Durchsatz.
2. Legen Sie den Preis pro Einheit fest.
3. Geben Sie für jede Startspezifikation die Gewichtung an, d. h. die Anzahl der Einheiten, die der Instance-Typ für die Zielkapazität darstellt.

Beispiel für die Instance-Gewichtung

Überlegen Sie sich eine Spot-Flotten-Anforderung mit der folgenden Konfiguration:

- Eine Zielkapazität von 24
- Eine Startspezifikation mit dem Instance-Typ `r3.2xlarge` und der Gewichtung 6
- Eine Startspezifikation mit dem Instance-Typ `c3.xlarge` und der Gewichtung 5

Die Gewichtung stellt die Anzahl an Einheiten dar, die der Instance-Typ hinsichtlich der Zielkapazität darstellt. Wenn die erste Startspezifikation den niedrigsten Preis pro Einheit (Preis für `r3.2xlarge` pro Instance-Stunde geteilt durch 6) bereitstellt, würde die Flotte vier dieser Instances starten (24 geteilt durch 6).

Wenn die zweite Startspezifikation den niedrigsten Preis pro Einheit (Preis für `c3.xlarge` pro Instance-Stunde geteilt durch 5) bereitstellt, würde die Flotte fünf dieser Instances starten (24 geteilt durch 5, Ergebnis aufgerundet).

Instance-Gewichtung und Zuweisungsstrategie

Überlegen Sie sich eine Spot-Flotten-Anforderung mit der folgenden Konfiguration:

- Eine Zielkapazität von 30 Spot-Instances
- Eine Startspezifikation mit dem Instance-Typ `c3.2xlarge` und der Gewichtung 8
- Eine Startspezifikation mit dem Instance-Typ `m3.xlarge` und der Gewichtung 8
- Eine Startspezifikation mit dem Instance-Typ `r3.xlarge` und der Gewichtung 8

Die Flotte würde vier Instances starten (30 geteilt durch 8, Ergebnis aufgerundet). Bei der `diversified`-Strategie startet die Flotte eine Instance in jedem der drei Pools und die vierte Instance in dem Pool, für den der niedrigste Preis pro Einheit anfällt.

Verwenden Sie Zuweisungsstrategien, um festzustellen, wie die EC2-Flotte oder Spot-Flotte die Spot- und On-Demand-Kapazitäten ausfüllt

Wenn Sie mehrere Kapazitätspools (die jeweils einen Instance-Typ und eine Availability Zone umfassen) in einer EC2-Flotte oder Spot-Flotte verwenden, können Sie mithilfe einer Zuweisungsstrategie steuern, wie Amazon EC2 Ihre Spot- und On-Demand-Kapazitäten aus diesen Pools ausfüllt. Die Zuweisungsstrategien können für die verfügbare Kapazität, den Preis und die zu verwendenden Instance-Typen optimiert werden. Es gibt unterschiedliche Zuweisungsstrategien für Spot Instances und On-Demand-Instances.

Themen

- Zuweisungsstrategien für Spot-Instances
- Zuweisungsstrategie für On-Demand-Instances
- Die geeignete Zuweisungsstrategie auswählen
- Zielkapazität für Spot Instances erhalten
- Priorisieren von Instance-Typen für On-Demand-Kapazität

Zuweisungsstrategien für Spot-Instances

Ihre Startkonfiguration bestimmt alle möglichen Spot-Kapazitätspools (Instance-Typen und Availability Zones), aus denen EC2-Flotte oder Spot-Flotte Spot Instances starten kann. Beim Starten von Instances nutzt Flotte jedoch die von Ihnen angegebene Zuweisungsstrategie, um die jeweiligen Pools aus allen möglichen Pools auszuwählen.

> **Note**
>
> (Nur Linux-Instances) Wenn Sie eine Spot Instance mit aktiviertem AMD SEV-SNP starten, wird Ihnen eine zusätzliche stündliche Nutzungsgebühr in Höhe von 10 % des On-Demand-Stundensatzes für den ausgewählten Instance-Typ berechnet. Wenn die Zuweisungsstrategie den Preis als Eingabe verwendet, berücksichtigt die Flotte diese zusätzliche Gebühr nicht. Es wird nur der Spot-Preis verwendet.

Sie können eine der folgenden Zuweisungsstrategien für Spot Instances angeben:

Preis-/kapazitätsoptimiert (empfohlen)

Die Flotte identifiziert die Pools mit der höchsten Kapazitätsverfügbarkeit für die Anzahl der Instances, die gestartet werden. Das bedeutet, dass wir Spot Instances aus den Pools anfordern werden, von denen wir glauben, dass die Wahrscheinlichkeit einer kurzfristigen Unterbrechung am geringsten ist. Die Flotte fordert dann Spot Instances aus dem günstigsten dieser Pools an.

Die Preis-/kapazitätsoptimierte Zuweisungsstrategie ist die beste Wahl für die meisten Spot-Workloads, z. B. statuslose containerisierte Anwendungen, Microservices, Webanwendungen, Daten- und Analytikaufträge sowie Batchverarbeitung.

Wenn Sie den verwendenAWS CLI, lautet der Parametername `price-capacity-optimized` für EC2 Fleet und `priceCapacity0ptimized` für Spot Fleet.

Kapazitätsoptimiert

Die Flotte identifiziert die Pools mit der höchsten Kapazitätsverfügbarkeit für die Anzahl der Instances, die gestartet werden. Das bedeutet, dass wir Spot Instances aus den Pools anfordern werden, von denen wir glauben, dass die Wahrscheinlichkeit einer kurzfristigen Unterbrechung am geringsten ist. Sie können optional eine Priorität für jeden Instance-Typ in Ihrer Flotte festlegen, wobei die Flotte zuerst die Kapazität optimiert, die Instance-Typprioritäten jedoch so gut wie möglich beachtet.

Im Fall von Spot-Instances ändern sich die Preise allmählich im Lauf der Zeit, basierend auf langfristigen Trends bei Angebot und Nachfrage. Die Kapazität fluktuiert jedoch in Echtzeit. Bei Anwendung der Strategie Kapazitätsoptimiert wird Spot Instances automatisch zu den am besten verfügbaren Pools gestartet, indem Echtzeitdaten zur Kapazität analysiert werden und prognostiziert wird, welche Pools am besten verfügbar sind. Diese Strategie ist gut für Workloads, bei denen Unterbrechungen aufgrund von Neustarts von Aufgaben höhere Kosten

verursachen, wie Continuous Integration (CI), Image- und Medien-Rendering, Deep Learning und High Performance Compute (HPC)-Workloads, bei denen Unterbrechungen höhere Kosten verursachen, da Aufgaben neu gestartet werden müssen. Da die Kapazitätsoptimiert-Strategie die Zahl der Unterbrechungen reduzieren kann, trägt sie zur Senkung der Gesamtkosten Ihrer Workload bei.

Alternativ können Sie die Kapazitätsoptimiertpriorisierte Zuweisungsstrategie mit einem Prioritätsparameter verwenden, um die Instance-Typen von der höchsten zur niedrigsten Priorität zu ordnen. Sie können die gleiche Priorität für verschiedene Instance-Typen festlegen. Die Flotte wird zuerst für die Kapazität optimiert, berücksichtigt jedoch so gut wie möglich die Prioritäten der Instance-Typen (wenn z. B. die Berücksichtigung der Prioritäten keinen wesentlichen Einfluss auf die Fähigkeit der Flotte zur Bereitstellung optimaler Kapazität hat). Dies ist eine gute Option für Workloads, bei denen die Möglichkeit von Unterbrechungen minimiert werden muss und die Präferenz für bestimmte Instance-Typen wichtig ist. Beachten Sie, dass, wenn Sie die Priorität für Instance-Typen für Ihre Spot-Kapazität festlegen, dieselbe Priorität auch auf Ihre On-Demand-Instances angewendet wird, wenn die On-Demand-Zuweisungsstrategie auf priorisiert eingestellt ist. Die Verwendung von Prioritäten wird für Spot-Flotte nur unterstützt, wenn Ihre Flotte eine Startvorlage verwendet.

Wenn Sie die AWS CLI verwenden, lauten die Parameternamen `capacity-optimized` und `capacity-optimized-prioritized` für EC2 Fleet und `capacityOptimized` und `capacityOptimizedPrioritized` für Spot-Flotte.

Diversifiert

Spot-Instances werden auf alle Spot-Kapazitätspools verteilt. Wenn Sie die AWS CLI verwenden, gilt der Parametername sowohl `diversified` für EC2-Flotte als auch für Spot-Flotte.

Niedrigster Preis (nicht empfohlen)

> **Warning**
>
> Wir empfehlen nicht, die Strategie für die Zuteilung des niedrigsten Preises zu wählen, da sie das größte Risiko einer Unterbrechung Ihrer Spot Instances birgt.

Die Spot-Instances kommen aus dem preisgünstigsten Pool mit verfügbarer Kapazität. Bei der Verwendung der AWS CLI ist dies die Standardstrategie. Es wird jedoch empfohlen, die Standardeinstellung zu überschreiben, indem Sie die Preis–Kapazitätsoptimierte Zuweisungsstrategie angeben.

Bei der Niedrigstpreisstrategie werden die Spot Instances aus dem nächstgünstigeren Pool mit freien Kapazitäten bezogen, wenn der Pool mit dem niedrigsten Preis keine freien Kapazitäten hat. Wenn in einem Pool die Kapazität zu Neige geht, bevor Ihre gewünschte Kapazität erreicht ist, wird Ihre Anforderung von der Flotte über den nächstgünstigsten Pool erfüllt. Damit die gewünschte Kapazität auf jeden Fall erreicht wird, erhalten Sie möglicherweise Spot-Instances aus mehreren Pools.

Da bei dieser Strategie nur der Instance-Preis und nicht die Kapazitätsverfügbarkeit berücksichtigt wird, kann es zu hohen Unterbrechungsraten kommen.

Die Niedrigstpreisstrategie ist nur verfügbar, wenn Sie die AWS CLI verwenden. Der Parametername ist `lowest-price` für EC2 Fleet und `lowestPrice` für Spot Fleet.

Anzahl der zu verwendenden Pools

Die Anzahl der Spot-Pools, über die Ihre Spot-Zielkapazität zugewiesen werden soll. Ist nur gültig, wenn die Zuweisungsstrategie auf Niedrigster Preis eingestellt ist. Die Flotte wählt die günstigsten Spot-Pools aus und weist Ihre Spot-Zielkapazität gleichmäßig über die von Ihnen angegebene Anzahl von Spot-Pools zu.

Beachten Sie, dass die Flotte versucht, Spot Instances aus der Anzahl der Pools zu ziehen, die Sie nach bestem Aufwand angeben. Wenn einem Pool die Spot-Kapazität ausgeht, bevor Ihre Zielkapazität erreicht ist, wird die Flotte Ihre Anfrage weiterhin erfüllen, indem sie sie aus dem nächsten preisgünstigsten Pool zieht. Um sicherzustellen, dass Ihre Zielkapazität erreicht wird, erhalten Sie möglicherweise Spot-Instances von mehr als der von Ihnen angegebenen Anzahl von Pools. Wenn die meisten Pools keine Spot-Kapazität haben, erhalten Sie Ihre volle Zielkapazität möglicherweise von weniger als der von Ihnen angegebenen Anzahl von Pools.

Dieser Parameter ist nur verfügbar, wenn die Strategie für die Zuteilung mit dem niedrigsten Preis angegeben wird, und nur bei Verwendung von AWS CLI. Der Parametername ist `InstancePoolsToUseCount` sowohl für EC2-Flotte als auch Spot-Flotte.

Zuweisungsstrategie für On-Demand-Instances

Ihre Startkonfiguration bestimmt alle möglichen Spot-Kapazitätspools (Instance-Typen und Availability Zones), aus denen EC2-Flotte oder Spot-Flotte On-Demand-Instances starten kann. Beim Starten von Instances nutzt Flotte jedoch die von Ihnen angegebene Zuweisungsstrategie, um die jeweiligen Pools aus allen möglichen Pools auszuwählen.

Sie können eine der folgenden Zuweisungsstrategien für On-Demand-Instances angeben:

niedrigster Preis

Die On-Demand-Instances kommen aus dem preisgünstigsten Pool mit verfügbarer Kapazität. Dies ist die Standardstrategie.

Wenn der günstigste Pool keine verfügbare Kapazität aufweist, kommen die On-Demand-Instances aus dem nächstgünstigsten Pool mit verfügbarer Kapazität.

Wenn in einem Pool die Kapazität zu Neige geht, bevor Ihre gewünschte Kapazität erreicht ist, wird Ihre Anforderung von der Flotte über den nächstgünstigsten Pool erfüllt. Damit die gewünschte Kapazität auf jeden Fall erreicht wird, erhalten Sie möglicherweise On-Demand-Instances aus mehreren Pools.

Priorisiert

Die Flotte verwendet die Priorität, die Sie jeder Einführungsvorlagen-Überschreibung zugewiesen haben, und launcht Instance-Typen mit der höchsten Priorität zuerst. Diese Strategie kann nicht mit attributbasierter Auswahl von Instance-Typen verwendet werden. Ein Beispiel für die Verwendung dieser Zuweisungsstrategie finden Sie unter Priorisieren von Instance-Typen für On-Demand-Kapazität.

Die geeignete Zuweisungsstrategie auswählen

Sie können Ihre Flotte für Ihren Anwendungsfall optimieren, indem Sie die entsprechende Spot-Zuweisungsstrategie wählen.

Gleichgewicht zwischen niedrigstem Preis und Kapazitätsverfügbarkeit

Um die Kompromisse zwischen den Spot-Kapazitätspools mit dem niedrigsten Preis und den Spot-Kapazitätspools mit der höchsten Kapazitätsverfügbarkeit auszugleichen, empfehlen wir, die Preis-Kapazitätsoptimierte Zuweisungsstrategie zu verwenden. Bei dieser Strategie werden Entscheidungen darüber getroffen, von welchen Pools Spot Instances angefordert werden sollen, sowohl auf der Grundlage des Preises der Pools als auch der Kapazitätsverfügbarkeit der Spot Instances in diesen Pools. Das bedeutet, dass wir Spot Instances aus den Pools anfordern werden, von denen wir glauben, dass die Wahrscheinlichkeit einer kurzfristigen Unterbrechung am geringsten ist, wobei der Preis weiterhin berücksichtigt wird.

Wenn Ihre Flotte belastbare und statuslose Workloads ausführt, einschließlich containerisierter Anwendungen, Microservices, Webanwendungen, Daten- und Analytikaufträge sowie

Stapelverarbeitung, dann sollten Sie die Preis-Kapazitätsoptimierte Zuweisungsstrategie verwenden, um optimale Kosteneinsparungen und Kapazitätsverfügbarkeit zu erzielen.

Wenn Ihre Flotte Workloads ausführt, bei denen Unterbrechungen aufgrund von Neustarts von Aufgaben höhere Kosten verursachen, sollten Sie Checkpointing implementieren, damit die Anwendungen von dem Punkt aus neu gestartet werden können, an dem sie unterbrochen wurden. Durch die Verwendung von Checkpointing passen Sie die Preis-Kapazitätsoptimierte Zuweisungsstrategie an diese Workloads an, da sie Kapazität aus den Pools mit dem niedrigsten Preis zuweist, die auch eine niedrige Spot-Instance-Unterbrechungsrate bieten.

Ein Beispiel für JSON-Konfigurationen, die die Preis-Kapazitätsoptimierte Zuweisungsstrategie verwenden, finden Sie im Folgenden:

- EC2-Flotte – Beispiel 10: Starten Sie Spot-Instances in einer Flotte price-capacity-optimized
- Spot-Flotte – Beispiel 11: Spot Instances in einer priceCapacityOptimized-Flotte starten

Wenn Workloads mit hohen Unterbrechungskosten verbunden sind

Sie können die kapazitätsoptimierte Strategie optional verwenden, wenn Sie Workloads ausführen, die entweder Instance-Typen mit ähnlichen Preisen verwenden oder bei denen die Kosten einer Unterbrechung so hoch sind, dass jegliche Kostenersparnis im Vergleich zu einer geringfügigen Zunahme der Unterbrechungen nicht ausreicht. Bei dieser Strategie wird die Kapazität aus den am besten verfügbaren Spot-Kapazitätspools zugewiesen, die die Möglichkeit von weniger Unterbrechungen bieten, was die Gesamtkosten Ihres Workloads senken kann.

Wenn die Möglichkeit von Unterbrechungen minimiert werden muss, aber die Präferenz für bestimmte Instance-Typen wichtig ist, können Sie Ihre Pool-Prioritäten ausdrücken, indem Sie die kapazitätsoptimiert-priorisierte Zuweisungsstrategie verwenden und dann die Reihenfolge der zu verwendenden Instance-Typen von der höchsten zur niedrigsten Priorität festlegen.

Beachten Sie Folgendes: Wenn Sie Prioritäten auf kapazitätsoptimiert-priorisiert festlegen, werden die gleichen Prioritäten auch auf Ihre On-Demand-Instances angewendet, wenn die On-Demand-Zuweisungsstrategie auf priorisiert eingestellt ist. Beachten Sie, dass für Spot-Flotte die Verwendung von Prioritäten nur unterstützt wird, wenn Ihre Flotte eine Startvorlage verwendet.

Beispiele für JSON-Konfigurationen, die die kapazitätsoptimierte Zuweisungsstrategie verwenden, finden Sie im Folgenden:

- EC2-Flotte – Beispiel 8: Starten von Spot Instances in einer kapazitätsoptimierten Flotte

- Spot-Flotte – Beispiel 9: Starten von Spot-Instances in einer kapazitätsoptimierten Flotte

Beispiele für JSON-Konfigurationen, die die kapazitätsoptimierte priorisierte Zuweisungsstrategie verwenden, finden Sie im Folgenden:

- EC2-Flotte – Beispiel 9: Starten von Spot Instances in einer kapazitätsoptimierten Flotte mit Prioritäten
- Spot-Flotte – Beispiel 10: Starten von Spot-Instances in einer kapazitätsoptimierten Flotte mit Prioritäten

Wenn Ihr Workload zeitlich flexibel ist und die Kapazitätsverfügbarkeit kein Faktor ist

Wenn Ihre Flotte klein ist oder nur für einen kurzen Zeitraum ausgeführt wird, können Sie Preis-Kapazitätsoptimiert nutzen, um die Kosteneinsparungen zu maximieren und dabei die Kapazitätsverfügbarkeit zu berücksichtigen.

Wenn Ihre Flotte groß ist oder lange läuft

Wenn Ihre Flotte groß ist oder für einen langen Zeitraum ausgeführt wird, können Sie die Verfügbarkeit Ihrer Flotte verbessern, indem Sie die Spot Instances mit der Strategie diversifiziert über mehrere Pools verteilen. Wenn Ihre Spot-Flotten-Anforderung beispielsweise 10 Pools und eine Zielkapazität von 100 Instances angibt, startet die Flotte 10 Spot Instances in jedem Pool. Wenn der Spot-Preis für einen Pool Ihren Höchstpreis für diesen Pool übersteigt, sind nur 10 % Ihrer Flotte betroffen. Bei dieser Strategie reagiert Ihre Flotte außerdem weniger empfindlich auf Steigerungen des Spot-Preises für die verschiedenen Pools im Laufe der Zeit. Bei der diversifizierten Strategie setzt die Flotte keine Spot Instances in Pools mit einem Spot-Preis ein, der gleich oder höher ist als der On-Demand-Preis.https://aws.amazon.com/ec2/pricing/

Zielkapazität für Spot Instances erhalten

Wenn Spot Instances aufgrund einer Änderung in Bezug auf den Spot-Preis oder die verfügbare Kapazität eines Spot-Kapazitätspools beendet werden, startet eine Flotte vom Typ `maintain` Ersatz-Spot-Instances. Die Zuweisungsstrategie bestimmt die Pools, von denen aus die Ersatz-Instances gestartet werden, wie folgt:

- Wenn die Zuweisungsstrategie Preis-Kapazitätsoptimiert ist, startet die Flotte Ersatz-Instances in den Pools mit der größten Spot-Instance-Kapazitätsverfügbarkeit. Dabei wird auch der Preis berücksichtigt und die günstigsten Pools mit hoher Kapazitätsverfügbarkeit identifiziert.

- Wenn die Zuweisungsstrategie Kapazitätsoptimiert ist, startet die Flotte Ersatz-Instances in den Pools mit der größten verfügbaren Spot Instance-Kapazität.
- Wenn die Zuweisungsstrategie Diversifiziert lautet, verteilt die Flotte die Ersatz-Spot-Instances über die verbleibenden Pools.

Priorisieren von Instance-Typen für On-Demand-Kapazität

Wenn dieEC2-Flotte oder Spot-Flotte versucht, Ihre On-Demand-Kapazität zu erfüllen, startet sie standardmäßig zuerst den kostengünstigsten Instance-Typ. Wenn die On-Demand-Zuweisungsstrategie auf Priorisiert eingestellt ist, verwendet die Flotte die Priorität, um zu bestimmen, welcher Instance-Typ bei der Erfüllung der On-Demand-Kapazität zuerst verwendet werden soll. Die Priorität wird der Startvorlagen-Überschreibung zugewiesen, und die höchste Priorität wird zuerst gestartet.

Beispiel: Priorisieren von Instance-Typen

In diesem Bespiel konfigurieren Sie drei Startvorlagen-Überschreibungen, jede mit einem anderen Instance-Typ.

Der On-Demand-Preis für die Instance-Typen variiert. Im Folgenden sind die in diesem Beispiel verwendeten Instance-Typen nach Preisen aufgeführt, beginnend mit dem günstigsten Instance-Typ:

- `m4.large` – am günstigsten
- `m5.large`
- `m5a.large`

Wenn Sie die Reihenfolge nicht anhand der Priorität bestimmen, startet die Flotte zur Erfüllung der On-Demand-Kapazität mit dem günstigsten Instance-Typ.

Nehmen wir jedoch an, Sie hätten ungenutzte `m5.large` Reserved Instances, die Sie zuerst verwenden möchten. Sie können die Startvorlagen-Überschreibungspriorität so einstellen, dass die Instance-Typen wie folgt in der Reihenfolge ihrer Priorität verwendet werden:

- `m5.large` – Priorität 1
- `m4.large` – Priorität 2
- `m5a.large` – Priorität 3

Den Kapazitätsausgleich in der EC2-Flotte und der Spot-Flotte verwenden, um gefährdete Spot Instances zu ersetzen

Mit Kapazitätsneuausgleich kann Ihre EC2-Flotte oder Spot-Flotte die gewünschte Spot-Kapazität aufrechterhalten, indem Spot Instances, bei denen das Risiko einer Unterbrechung besteht, proaktiv ersetzt werden. Wenn eine Spot-Instance ein erhöhtes Unterbrechungsrisiko hat, sendet Amazon EC2 eine Neuausgleichsempfehlung. Wenn Kapazitätsneuausgleich aktiviert ist, löst die Empfehlung zur Neuverteilung den Start einer neuen Spot-Instance aus, bevor die gefährdete Instance unterbrochen wird.

Der Kapazitätsneuausgleich hilft Ihnen, die Verfügbarkeit von Workloads aufrechtzuerhalten, indem Sie Ihre Flotte proaktiv um eine neue Spot Instance erweitern, bevor eine ausgeführte Instance durch Amazon EC2 unterbrochen wird.

EC2-Flotte konfigurieren, Kapazitätsneuausgleich zu verwenden, um eine Ersatz-Spot-Instance zu starten

Verwenden Sie den Befehl create-fleet und die relevanten Parameter in der `MaintenanceStrategies`-Struktur. Eine JSON-Beispielkonfiguration finden Sie unter Beispiel 7: Konfigurieren des Kapazitätsneuausgleichs, um Ersatz-Spot-Instances zu starten.

Spot-Flotte so konfigurieren, dass der Kapazitätsneuausgleich zum Starten einer neuen Spot Instance verwendet wird

Sie können die Amazon-EC2-Konsole oder die AWS CLI verwenden, um Kapazitätsneuausgleich zu konfigurieren.

(Konsole) Aktivieren Sie bei der Erstellung der Spot-Flotte das Kontrollkästchen Kapazitätsneuausgleich. Weitere Informationen finden Sie in Schritt 6.d unter Eine Spot-Flottenanforderung mit definierten Parametern erstellen.

(AWS CLI) Verwenden Sie den Befehl request-spot-fleet und die relevanten Parameter in der `SpotMaintenanceStrategies`-Struktur. Eine JSON-Beispielkonfiguration finden Sie unter Beispiel 8: Konfigurieren des Kapazitätsneuausgleichs, um den Ersatz Spot-Instances zu starten.

Themen

- Einschränkungen
- Konfigurationsoptionen

- Überlegungen

Einschränkungen

- Die Kapazitätsanpassung ist nur für Flotten des Typs verfügbar `maintain`.
- Wenn die Flotte läuft, können Sie die Kapazitätsausgleichs-Einstellung nicht ändern. Um die Einstellung Kapazitätsausgleich zu ändern, müssen Sie die Flotte löschen und eine neue Flotte erstellen.

Konfigurationsoptionen

`ReplacementStrategy` für die EC2-Flotte und Spot-Flotte unterstützt die folgenden beiden Werte:

`launch-before-terminate`

Amazon EC2 kann die Spot Instances beenden, die eine Neuausgleichsbenachrichtigung erhalten, nachdem neue Ersatz-Spot-Instances gestartet wurden. Wenn Sie `launch-before-terminate` angeben, müssen Sie auch einen Wert für `termination-delay` angeben. Nachdem die neuen Ersatz-Instances gestartet wurden, wartet Amazon EC2 während der Dauer des `termination-delay` und beendet dann die alten Instances. Für `termination-delay` beträgt das Minimum 120 Sekunden (2 Minuten) und das Maximum 7 200 Sekunden (2 Stunden).

Wir empfehlen die Verwendung von `launch-before-terminate` nur, wenn Sie vorhersagen können, wie lange Ihre Verfahren zum Herunterfahren der Instances dauern werden. Dadurch wird sichergestellt, dass die alten Instances erst beendet werden, wenn die Verfahren zum Herunterfahren abgeschlossen sind. Beachten Sie, dass Amazon EC2 die alten Instances mit einer zweiminütigen Warnung vor der unterbrechen kann `termination-delay`.

Wir raten dringend davon ab, die Zuweisungsstrategie `lowest-price` (EC2-Flotte) oder `lowestPrice` (Spot-Flotte) in Kombination mit `launch-before-terminate` zu verwenden, um zu vermeiden, dass Ersatz-Spot-Instances vorhanden sind, die ebenfalls ein erhöhtes Risiko einer Unterbrechung aufweisen.

`launch`

Amazon EC2 startet Ersatz-Spot-Instances, wenn eine Neuausgleichsbenachrichtigung für bestehende Spot-Instances ausgegeben wird. Amazon EC2 beendet nicht die Instances, die eine Neuausgleichsbenachrichtigung erhalten. Sie können die alten Instances beenden oder laufen lassen. Ihnen werden alle Instances in Rechnung gestellt, während sie ausgeführt werden.

Überlegungen

Wenn Sie eine EC2-Flotte oder Spot-Flotte für Kapazitätsausgleich konfigurieren, sollten Sie Folgendes berücksichtigen:

Stellen Sie so viele Spot-Kapazitätspools wie möglich in der Anfrage bereit

Konfigurieren Sie Ihre Flotte für die Verwendung mehrerer Instance-Typen und Availability Zones. Dies bietet die Flexibilität, Spot-Instances in verschiedenen Spot-Kapazitätspools zu starten. Weitere Informationen finden Sie unter Flexibel sein bei Instance-Typen und Availability Zones.

Vermeiden Sie ein erhöhtes Risiko einer Unterbrechung von Ersatz-Spot-Instances

Um ein erhöhtes Unterbrechungsrisiko zu vermeiden, empfehlen wir die `capacity-optimized`- oder `capacity-optimized-prioritized`-Zuweisungsstrategie. Diese Strategien stellen sicher, dass Ersatz-Spot-Instances in den optimalen Spot-Kapazitätspools gestartet werden und ihre Unterbrechung in naher Zukunft daher weniger wahrscheinlich ist. Weitere Informationen finden Sie unter Nutzen der preis- und kapazitätsoptimierten Zuweisungsstrategie.

Ihre Ersatz-Spot-Instances haben möglicherweise ein erhöhtes Risiko einer Unterbrechung, wenn Sie die `lowest-price`-Zuweisungsstrategie verwenden. Dies liegt daran, dass Amazon EC2 immer Instances im preisgünstigsten Pool startet, der zu diesem Zeitpunkt verfügbare Kapazität hat, auch wenn Ihre Ersatz-Spot-Instances wahrscheinlich kurz nach dem Start unterbrochen werden.

Amazon EC2 startet eine neue Instance nur dann, wenn die Verfügbarkeit gleich oder besser ist

Eines der Ziele des Kapazitätsausgleichs ist die Verbesserung der Verfügbarkeit einer Spot Instance. Wenn eine vorhandene Spot Instance eine Neuausgleichsempfehlung erhält, startet Amazon EC2 nur dann eine neue Instance, wenn die neue Instance dieselbe oder eine bessere Verfügbarkeit als die vorhandene Instance bietet. Wenn das Risiko einer Unterbrechung einer neuen Instance größer ist als das der vorhandenen Instance, startet Amazon EC2 keine neue Instance. Amazon EC2 wird die Spot-Kapazitätspools jedoch weiterhin bewerten und eine neue Instance starten, falls sich die Verfügbarkeit verbessert.

Es besteht die Möglichkeit, dass Ihre vorhandene Instance unterbrochen wird, ohne dass Amazon EC2 pro-aktiv eine neue Instance startet. In diesem Fall versucht Amazon EC2, eine neue Instance zu starten, sobald die Unterbrechungsmeldung für eine Spot Instance eingeht, unabhängig davon, ob bei der neuen Instance ein hohes Unterbrechungsrisiko besteht.

Capacity Rebalancing erhöht nicht die Unterbrechungsrate Ihrer Spot-Instance

Wenn Sie Capacity Rebalancing aktivieren, wird Ihre Spot-Instance-Unterbrechungsrate (die Anzahl der Spot-Instances, die zurückgefordert werden, wenn Amazon EC2 die Kapazität zurück benötigt) nicht erhöht. Wenn der Kapazitätsausgleich jedoch feststellt, dass bei einer Instance das Risiko einer Unterbrechung besteht, versucht Amazon EC2 sofort, eine neue Instance zu starten. Das Ergebnis ist, dass möglicherweise mehr Instances ersetzt werden, als wenn Sie darauf gewartet hätten, dass Amazon EC2 eine neue Instance startet, nachdem die gefährdete Instance unterbrochen wurde.

Sie können zwar mehr Instances mit aktiviertem Capacity Rebalancing ersetzen, jedoch Sie profitieren davon, dass Sie eher proaktiv als reaktiv sind, indem Sie mehr Zeit haben, Maßnahmen zu ergreifen, bevor Ihre Instances unterbrochen werden. Mit einer Spot-Instance-Unterbrechungsbenachrichtigung haben Sie normalerweise nur bis zu zwei Minuten Zeit, um Ihre Instance ordnungsgemäß herunterzufahren. Wenn Capacity Rebalancing eine neue Instance im Voraus startet, geben Sie bestehenden Prozessen eine bessere Chance, sie auf Ihrer gefährdeten Instance abzuschließen. Sie können mit dem Herunterfahren Ihrer Instance beginnen und verhindern, dass neue Arbeiten für Ihre gefährdete Instance geplant werden. Sie können auch damit beginnen, die neu gestartete Instance für die Übernahme der Anwendung vorzubereiten. Mit dem proaktiven Ersetzen durch Capacity Rebalancing profitieren Sie von einer reibungslosen Kontinuität.

Betrachten Sie als theoretisches Beispiel zur Demonstration der Risiken und Vorteile des Einsatzes von Capacity Rebalancing das folgende Szenario:

- 14:00 Uhr – Für Instance-A wird eine Empfehlung zum erneuten Ausgleich empfangen und Amazon EC2 versucht sofort, eine Ersatz-Instance-B zu starten, sodass Sie Zeit haben, Ihre Shutdown-Verfahren zu starten.*
- 14:30 Uhr — Für Instance-B wird eine Empfehlung zum erneuten Ausgleich empfangen, die durch Instance-C ersetzt wird, sodass Sie Zeit haben, Ihre Shutdown-Verfahren zu starten.*
- 14:32 Uhr — Wenn Capacity Rebalancing nicht aktiviert wäre und um 14:32 Uhr eine Benachrichtigung über eine Unterbrechung der Spot-Instance für Instance-A eingegangen wäre, hätten Sie nur bis zu zwei Minuten Zeit gehabt, um Maßnahmen zu ergreifen, währenddessen Instance-A allerdings bis zu diesem Zeitpunkt hochgefahren wäre.

* Wenn `launch-before-terminate` angegeben ist, beendet Amazon EC2 die gefährdete Instance, nachdem die Ersatz-Instance online geschaltet wurde.

Amazon EC2 kann einen neuen Ersatz Spot-Instances starten, bis die erfüllte Kapazität die doppelte Zielkapazität hat

Wenn eine Flotte für den Kapazitätsneuausgleich konfiguriert ist, versucht die Flotte, eine neue Ersatz-Spot-Instance für jede Spot-Instance zu starten, die eine Ausgleichsempfehlung erhält. Nachdem eine Spot-Instance eine Neuausgleichsempfehlung erhalten hat, wird sie nicht mehr als Teil der erfüllten Kapazität gezählt. Je nach Ersetzungsstrategie beendet Amazon EC2 die Instance entweder nach einer vorkonfigurierten Beendigungsverzögerung oder lässt sie laufen. Dies gibt Ihnen die Möglichkeit, Neuausgleichsaktionen für die Instance durchzuführen.

Wenn Ihre Flotte die doppelte Zielkapazität erreicht, wird sie keine neuen Ersatz-Instances mehr starten, selbst wenn die Ersatz-Instances selbst eine Empfehlung zum Neuausgleich erhalten.

Angenommen, Sie erstellen Sie eine Spot-Flotte mit einer Zielkapazität von 100 Spot Instances. Alle Spot Instances erhalten eine Neuausgleichsempfehlung, die dazu führt, dass Amazon EC2 100 Ersatz-Spot-Instances startet. Dadurch wird die Anzahl der erfüllten Spot-Instances auf 200 erhöht, was der doppelten Zielkapazität entspricht. Einige der Ersatz-Instances erhalten eine Neuausgleichsempfehlung, es werden jedoch keine Ersatz-Instances mehr gestartet, da die Flotte die doppelte Zielkapazität nicht überschreiten kann.

Beachten Sie, dass Ihnen alle Instances in Rechnung gestellt werden, während sie ausgeführt werden.

Wir empfehlen Ihnen, die Flotte so zu konfigurieren, dass Spot Instances beendet werden, die eine Neuausgleichsempfehlung erhalten.

Wenn Sie Ihre Flotte für den Kapazitätsneuausgleich konfigurieren, empfehlen wir Ihnen, `launch-before-terminate` mit einer angemessenen Beendigungsverzögerung nur dann auszuwählen, wenn Sie vorhersagen können, wie lange die Verfahren zum Herunterfahren der Instances dauern werden. Dadurch wird sichergestellt, dass die alten Instances erst beendet werden, wenn die Verfahren zum Herunterfahren abgeschlossen sind.

Wenn Sie die für die Neuausgleichsempfehlung empfohlenen Instances selbst beenden möchten, empfehlen wir Ihnen, das Signal für die Neuausgleichsempfehlung zu überwachen, das von den Spot-Instances in der Flotte empfangen wird. Durch die Überwachung des Signals können Sie schnell Neuausgleichsaktionen für die betroffenen Instances durchführen, bevor Amazon EC2 sie unterbricht, und dann können Sie sie manuell beenden. Wenn Sie die Instances nicht beenden, bezahlen Sie weiterhin für sie, während sie ausgeführt werden. Amazon EC2 beendet die Instances, die eine Neuausgleichsempfehlung erhalten, nicht automatisch.

Sie können Benachrichtigungen mit Amazon EventBridge oder Instance-Metadaten einrichten. Weitere Informationen finden Sie unter Überwachen von Signalen für Neuausgleichsempfehlungen.

Die Flotte zählt keine Instances, die bei der Berechnung der erfüllten Kapazität bei einer Verringerung oder Vergrößerung eine Neuausgleichsempfehlung während der Skalierung erhalten

Wenn Ihre Flottett für den Kapazitätsneuausgleich konfiguriert ist und Sie die Zielkapazität so ändern, dass sie entweder abskaliert oder aufskaliert wird, zählt die Flotte die Instances nicht, die für den Ausgleich markiert sind, wie folgt:

- Abskalieren – Wenn Sie die gewünschte Zielkapazität verringern, beendet Amazon EC2 Instances, die nicht für eine Neuverteilung markiert sind, bis die gewünschte Kapazität erreicht ist. Die Instances, die für einen Neuausgleich markiert sind, werden nicht auf die erfüllte Kapazität angerechnet.

  Ein Beispiel: Angenommen, Sie erstellen eine Spot-Flotte mit einer Zielkapazität von 100 Spot Instances. 10 Instances erhalten eine Neuausgleichsempfehlung. Amazon EC2 startet also 10 neue Ersatz-Instances, was zu einer erfüllten Kapazität von 110 Instances führt. Sie reduzieren dann die Zielkapazität auf 50 (abskalieren), aber die erfüllte Kapazität beträgt tatsächlich 60 Instances, da die 10 Instances, die für einen Neuausgleich markiert sind, nicht von Amazon EC2 beendet werden. Sie müssen diese Instances manuell beenden oder Sie können sie laufen lassen.

- Aufskalieren – Wenn Sie Ihre gewünschte Zielkapazität erhöhen, startet Amazon EC2 neue Instances, bis die gewünschte Kapazität erreicht ist. Die Instances, die für einen Neuausgleich markiert sind, werden nicht auf die erfüllte Kapazität angerechnet.

  Ein Beispiel: Angenommen, Sie erstellen eine Spot-Flotte mit einer Zielkapazität von 100 Spot Instances. 10 Instances erhalten eine Neuausgleichsempfehlung. Die Flotte startet also 10 neue Ersatz-Instances, was zu einer erfüllten Kapazität von 110 Instances führt. Sie erhöhen dann die Zielkapazität auf 200 (Erweiterung), aber die erfüllte Kapazität beträgt tatsächlich 210 Instances, da die 10 Instances, die für einen Neuausgleich markiert sind, nicht von der Flotte als Teil der Zielkapazität gezählt werden. Sie müssen diese Instances manuell beenden, oder Sie können sie laufen lassen.

Kapazitätsreservierungen verwenden, um On-Demand-Kapazitäten in der EC2-Flotte zu reservieren

Mit On-Demand-Kapazitätsreservierungen können Sie Rechenkapazität für Ihre On-Demand-Instances in einer bestimmten Availability Zone für eine beliebige Dauer reservieren. Sie können eine EC2-Flotte so konfigurieren, dass sie die Kapazitätsreservierungen beim Starten von On-Demand-Instances zuerst verwendet.

Kapazitätsreservierungen auf Abruf sind nur für EC2-Flotten verfügbar, bei denen der Anfragetyp auf `instant` eingestellt ist.

Kapazitätsreservierungen werden entweder als `open` oder `targeted` konfiguriert. EC2-Flotte kann On-Demand-Instances entweder in `open`- oder `targeted`-Kapazitätsreservierungen wie folgt starten:

- Wenn eine Kapazitätsreservierung `open` ist, werden On-Demand-Instances mit übereinstimmenden Attributen automatisch in der reservierten Kapazität ausgeführt.
- Wenn die Kapazitätsreservierung `targeted` ist, müssen die On-Demand-Instances speziell für die Ausführung in der reservierten Kapazität ausgerichtet sein. Dies ist nützlich, um bestimmte Kapazitätsreservierungen zu verwenden oder um zu kontrollieren, wann bestimmte Kapazitätsreservierungen verwendet werden sollen.

Wenn Sie `targeted`-Kapazitätsreservierungen in Ihrer EC2-Flotte verwenden, müssen genügend Kapazitätsreservierungen vorhanden sein, um die angeforderte On-Demand-Kapazität zu erfüllen, andernfalls schlägt der Start fehl. Um zu vermeiden, dass ein Start fehlschlägt, fügen Sie stattdessen die `targeted`-Kapazitätsreservierungen einer Ressourcengruppe hinzu, und richten Sie dann die Ressourcengruppe an. Die Ressourcengruppe muss nicht über ausreichende Kapazitätsreservierungen verfügen. Wenn die Kapazitätsreservierungen ausgehen, bevor die Ziel-On-Demand-Kapazität erfüllt ist, kann die Flotte die verbleibende Zielkapazität in reguläre On-Demand-Kapazität starten.

So verwenden Sie Kapazitätsreservierungen mit EC2-Flotte

1. Konfigurieren Sie die Flotte als Typ `instant`. Sie können Kapazitätsreservierungen für Flotten anderer Art nicht verwenden.
2. Konfigurieren Sie die Nutzungsstrategie für Kapazitätsreservierungen als `use-capacity-reservations-first`.

3. Wählen Sie in der Startvorlage für Kapazitätsreservierung entweder Öffnen oder Ziel nach Gruppe aus. Wenn Sie Ziel nach Gruppe wählen, geben Sie die Ressourcengruppen-ID für Kapazitätsreservierungen an.

Wenn die Flotte versucht, die On-Demand-Kapazität zu erfüllen, und wenn sie feststellt, dass mehrere Instance-Pools über ungenutzte übereinstimmende Kapazitätsreservierungen verfügen, bestimmt sie die Pools, in denen die On-Demand-Instances gestartet werden sollen, basierend auf der On-Demand-Zuordnungsstrategie (`lowest-price` oder `prioritized`).

Zugehörige Ressourcen

- CLI-Beispiele für die Konfiguration einer Flotte für die Verwendung von Kapazitätsreservierungen zur Erfüllung von On-Demand-Kapazitäten finden Sie unter CLI-Beispielkonfigurationen für EC2 Fleet, insbesondere Beispiele 5 bis 7.
- Ein Tutorial, das Sie Schritt für Schritt durch die Erstellung von Kapazitätsreservierungen, deren Verwendung in Ihrer Flotte und die Anzeige der verbleibenden Kapazitätsreservierungen führt, finden Sie unter Tutorial: EC2 Fleet so konfigurieren, dass On-Demand Instances mit gezielten Kapazitätsreservierungen gestartet werden
- Weitere Informationen zum Konfigurieren von Kapazitätsreservierungen finden Sie unter Reservieren Sie Rechenkapazität mit Kapazitätsreservierungen EC2 auf Abruf und Häufig gestellte Fragen zur On-Demand-Kapazitätsreservierung.

Arbeiten Sie mit EC2 Fleet

Um mit der Nutzung einer EC2 Flotte zu beginnen, erstellen Sie eine Anfrage, die die gesamte Zielkapazität, die On-Demand-Kapazität, die Spot-Kapazität und eine Startvorlage enthält, in der die Konfiguration für die Instances in der Flotte angegeben ist. Sie können optional zusätzliche Parameter angeben oder die Flotte Standardwerte verwenden lassen. Sie können die Flottenanforderung sowie ihre Instances und Volumes auch taggen, wenn Sie die Flotte erstellen.

Die Flotte startet On-Demand-Instances, wenn freie Kapazität vorhanden ist, und startet Spot Instances, wenn Ihr Höchstpreis den Spot-Preis übersteigt und Kapazität verfügbar ist.

Sobald Ihre Flotte gestartet ist, können Sie die Flottenanforderung, die Instances in der Flotte und alle Flottenereignisse beschreiben. Sie können bei Bedarf auch zusätzliche Tags zuweisen.

Wenn Sie Flottenparameter ändern müssen, z. B. die Gesamtzielkapazität, können Sie die Flotte ändern, vorausgesetzt, sie wurde so konfiguriert, dass sie die Kapazität beibehält. Sie können die Zielkapazität einer einmaligen Anfrage nach der Übermittlung nicht mehr ändern.

Eine Flottenanforderung bleibt solange aktiv, bis sie abläuft oder Sie sie löschen. Wenn Sie die Flottenanforderung löschen, können Sie die zugeordneten Instances beenden oder laufen lassen. Wenn Sie sich dafür entscheiden, sie laufen zu lassen, werden die On-Demand Instances ausgeführt, bis Sie sie beenden, und die Spot Instances laufen, bis sie unterbrochen werden oder Sie sie beenden.

Themen

- EC2 Status der Flottenanfrage
- EC2 Voraussetzungen für die Flotte
- Erstellen Sie eine EC2 Flotte
- Kennzeichnen Sie eine neue oder bestehende EC2 Fleet-Anfrage sowie die Instances und Volumes, die sie startet
- Beschreiben Sie eine EC2 Flotte, ihre Instanzen und ihre Ereignisse
- Modifizieren Sie eine EC2 Flotte
- Löschen Sie eine EC2 Flottenanfrage und die Instances in der Flotte

EC2 Status der Flottenanfrage

Eine EC2 Flottenanfrage kann aus verschiedenen Zuständen bestehen, wobei jeder Status auf eine andere Phase des Lebenszyklus der Anfrage und der Verwaltung der Instanzen hinweist.

Eine EC2 Flottenanforderung kann sich in einem der folgenden Zustände befinden:

`submitted`

Die EC2 Flottenanfrage wird geprüft und Amazon bereitet EC2 sich darauf vor, die angestrebte Anzahl von Instances zu starten. Wenn eine Anforderung Ihre Flottenlimits überschreiten würde, wird sie sofort gelöscht.

`active`

Die EC2 Flottenanfrage wurde validiert und Amazon EC2 versucht, die angestrebte Anzahl laufender Instances beizubehalten. Die Anforderung bleibt so lange in diesem Zustand, bis sie geändert oder gelöscht wird.

`modifying`

Die EC2 Flottenanfrage wird geändert. Die Anforderung bleibt in diesem Zustand, bis die Änderung vollständig bearbeitet oder die Anforderung gelöscht wird. Nur ein `maintain`-Flottentyp kann geändert werden. Dieser Status gilt nicht für die anderen Anforderungstypen.

`deleted_running`

Die EC2 Flottenanfrage wird gelöscht und startet keine weiteren Spot-Instances. Die bestehenden Instances laufen weiter, bis sie unterbrochen oder manuell beendet werden. Die Anforderung bleibt so lange in diesem Zustand, bis alle Instances unterbrochen oder beendet wurden. Nach dem Löschen der EC2 Flottenanforderung `request` kann es nur eine EC2 Flotte des Typs `maintain` oder aktive Instances geben. Eine gelöschte `instant`-Flotte mit laufenden Instances wird nicht unterstützt. Dieser Status gilt nicht für `instant`-Flotten.

`deleted_terminating`

Die EC2 Flottenanfrage wird gelöscht und die zugehörigen Instanzen werden beendet. Die Anforderung bleibt so lange in diesem Zustand, bis alle Instances beendet wurden.

`deleted`

Die EC2 Flottenanfrage wurde gelöscht und hat keine laufenden Instances. Die Anforderung wird zwei Tage nach Beendigung der zugehörigen Instances gelöscht.

EC2 Voraussetzungen für die Flotte

Um eine EC2 Flotte zu erstellen, müssen die folgenden Voraussetzungen erfüllt sein:

- Startvorlage
- Servicebezogene Rolle für Fleet EC2
- Gewähren Sie Zugriff auf vom Kunden verwaltete Schlüssel zur Verwendung mit verschlüsselten AMIs und EBS-Snapshots
- Berechtigungen für EC2 Flottenbenutzer

Startvorlage

Eine Startvorlage gibt die Konfigurationsinformationen über die zu startenden Instances an, wie beispielsweise den Instance-Typ und die Availability Zone. Weitere Informationen über Startvorlagen finden Sie unter Instance-Startparameter in EC2 Amazon-Startvorlagen speichern.

Servicebezogene Rolle für Fleet EC2

Die `AWSServiceRoleForEC2Fleet` Rolle gewährt der EC2 Flotte die Berechtigung, Instances in Ihrem Namen anzufordern, zu starten, zu beenden und zu taggen. Amazon EC2 verwendet diese servicebezogene Rolle, um die folgenden Aktionen durchzuführen:

- `ec2:RunInstances` – Instances starten.
- `ec2:RequestSpotInstances` – Spot-Instances anfragen.
- `ec2:TerminateInstances` – Instances beenden.
- `ec2:DescribeImages`— Beschreiben Sie Amazon Machine Images (AMIs) für die Instances.
- `ec2:DescribeInstanceStatus` – Beschreiben des Status der Instances.
- `ec2:DescribeSubnets` – Beschreiben der Subnetze für Instances.
- `ec2:CreateTags`— Fügen Sie der EC2 Flotte, den Instances und den Volumes Tags hinzu.

Stellen Sie sicher, dass diese Rolle existiert, bevor Sie die AWS CLI oder eine API verwenden, um eine EC2 Flotte zu erstellen.

> **Note**
>
> Eine `instant` EC2 Flotte benötigt diese Rolle nicht.

Um die Rolle anzulegen, verwenden Sie die IAM-Konsole wie folgt.

Um die AWSService RoleFor EC2 Flottenrolle für EC2 Fleet zu erstellen

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Rollen aus.
3. Wählen Sie Create role (Rolle erstellen) aus.
4. Gehen Sie auf der Seite Select trusted entity (Vertrauenswürdige Entität auswählen) wie folgt vor:
   a. Wählen Sie unter Vertrauenswürdiger Entitätstyp die Option AWS -Service aus.
   b. Wählen Sie unter Anwendungsfall für Service oder Anwendungsfall die Option EC2 - Flotte aus.

> **Tip**
>
> Achten Sie darauf, dass Sie EC2 — Flotte wählen. Wenn Sie wählen EC2, wird der Anwendungsfall EC2 — Fleet nicht in der Liste der Anwendungsfälle angezeigt. Der Anwendungsfall EC2 - Fleet erstellt automatisch eine Richtlinie mit den erforderlichen IAM-Berechtigungen und schlägt AWSServiceRoleForEC2Fleet als Rollennamen vor.

c. Wählen Sie Weiter aus.

5. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next (Weiter) aus.
6. Wählen Sie auf der Seite Benennen, Überprüfen und Erstellen die Option Rolle erstellen aus.

Wenn Sie EC2 Fleet nicht mehr verwenden müssen, empfehlen wir Ihnen, die AWSServiceRoleForEC2Fleet-Rolle zu löschen. Nachdem diese Rolle aus Ihrem Konto gelöscht wurde, können Sie die Rolle erneut anlegen, wenn Sie eine andere Flotte anlegen.

Weitere Informationen finden Sie unter Serviceverknüpfte Rollen im IAM-Benutzerhandbuch.

Gewähren Sie Zugriff auf vom Kunden verwaltete Schlüssel zur Verwendung mit verschlüsselten AMIs und EBS-Snapshots

Wenn Sie in Ihrer EC2 Flotte ein verschlüsseltes AMI oder einen verschlüsselten Amazon EBS-Snapshot angeben und einen AWS KMS Schlüssel für die Verschlüsselung verwenden, müssen Sie der AWSServiceRoleForEC2Flottenrolle die Erlaubnis erteilen, den vom Kunden verwalteten Schlüssel zu verwenden, damit Amazon Instances in Ihrem Namen starten EC2 kann. Dazu müssen Sie dem vom Kunden verwalteten Schlüssel eine Erteilung hinzufügen, wie im Folgenden gezeigt:

Bei der Einrichtung von Berechtigungen ist die Erteilung von Berechtigung eine Alternative zu Schüsselrichtlinien. Weitere Informationen finden Sie unter Verwenden von Erteilungen und Verwenden von Schlüsselrichtlinien in AWS KMS im Entwicklerhandbuch für AWS Key Management Service .

Um der AWSService RoleFor EC2 Flottenrolle Berechtigungen zur Verwendung des vom Kunden verwalteten Schlüssels zu erteilen

- Verwenden Sie den Befehl create-grant, um dem vom Kunden verwalteten Schlüssel einen Grant hinzuzufügen und den Principal (die dienstbezogene AWSServiceRoleForEC2Flottenrolle) anzugeben, der die Berechtigung zur Ausführung der durch die Gewährung erlaubten Operationen erhält. Der vom Kunden verwaltete Schlüssel wird durch den `key-id`-Parameter und den ARN des vom Kunden verwalteten Schlüssels angegeben. Der Principal wird durch den `grantee-principal` Parameter und den ARN der mit dem AWSServiceRoleForEC2Fleet-Service verknüpften Rolle angegeben.

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2Fleet \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Berechtigungen für EC2 Flottenbenutzer

Wenn Ihre Benutzer eine EC2 Flotte erstellen oder verwalten, stellen Sie sicher, dass Sie ihnen die erforderlichen Berechtigungen gewähren.

Um eine Richtlinie für EC2 Fleet zu erstellen

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Richtlinien.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie auf der Seite Create policy (Richtlinie erstellen) die Registerkarte JSON, ersetzen Sie den Text durch den im Folgenden gezeigten Text, und wählen Sie Review policy (Richtlinie überprüfen).

   JSON

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
              "iam:ListRoles",
              "iam:PassRole",
              "iam:ListInstanceProfiles"
            ],
            "Resource":"arn:aws:iam::123456789012:role/DevTeam*"
        }
    ]
}
```

Das `ec2:*` gewährt einem Benutzer die Erlaubnis, alle EC2 Amazon-API-Aktionen aufzurufen. Um den Benutzer auf bestimmte EC2 Amazon-API-Aktionen zu beschränken, geben Sie stattdessen diese Aktionen an.

Der Benutzer muss berechtigt sein, die `iam:ListRoles` Aktion zum Auflisten vorhandener IAM-Rollen, die `iam:PassRole` Aktion zum Angeben der EC2 Flottenrolle und die `iam:ListInstanceProfiles` Aktion zum Auflisten vorhandener Instance-Profile aufzurufen.

(Optional) Um einem Benutzer das Erstellen von Rollen oder Instance-Profilen mithilfe der IAM-Konsole zu ermöglichen, müssen Sie der Richtlinie auch die folgenden Aktionen hinzufügen:

- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

5. Geben Sie auf der Seite Review policy (Richtlinie überprüfen) einen Richtlinienamen und eine Beschreibung ein und wählen Sie anschließend Create policy (Richtlinie erstellen) aus.

6. Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

   - Benutzer und Gruppen in: AWS IAM Identity Center

     Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

   - Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

     Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.

   - IAM-Benutzer:
     - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
     - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie eine EC2 Flotte

Um eine EC2 Flotte zu erstellen, definieren Sie die Flottenkonfiguration in einer JSON-Datei und verweisen Sie mit dem Befehl create-fleet auf die Datei. In der JSON-Datei müssen Sie die Gesamtzielkapazität für die Flotte angeben, separate Zielkapazitäten für Spot Instances und On-Demand-Instances sowie eine Startvorlage angeben, die Konfiguration für die Instances in der Flotte definiert, z. B. eine AMI, einen Instance-Typ, ein Subnetz oder eine Availability Zone, und eine oder mehrere Sicherheitsgruppen. Sie können optional zusätzliche Konfigurationen angeben, z. B. Parameter zum Überschreiben der Konfiguration der Startvorlage, Zuweisungsstrategien für die Auswahl von Spot-Instances und On-Demand-Instances aus den EC2 Kapazitätspools und den Höchstbetrag, den Sie bereit sind, für die Flotte zu zahlen. Weitere Informationen finden Sie unter Konfigurationsoptionen für Ihre EC2-Flotte oder Spot-Flotte.

Die EC2 Flotte startet On-Demand-Instances, wenn Kapazität verfügbar ist, und Spot-Instances, wenn Ihr Höchstpreis den Spot-Preis übersteigt und Kapazität verfügbar ist.

Wenn Ihre Flotte Spot-Instances umfasst und dem Typ entspricht`maintain`, versucht Amazon, EC2 die Zielkapazität Ihrer Flotte aufrechtzuerhalten, wenn Ihre Spot-Instances unterbrochen werden.

EC2 Einschränkungen bei der Flotte

Für EC2 Fleet gelten die folgenden Einschränkungen:

- Das Erstellen einer EC2 Flotte ist nur über die EC2 Amazon-API, AWS CLIAWS SDKs, und verfügbar CloudFormation.
- Eine EC2 Flottenanfrage kann sich nicht über mehrere AWS Regionen erstrecken. Sie müssen für jede Region eine separate EC2 Flotte erstellen.
- Eine EC2 Flottenanfrage kann sich nicht über verschiedene Subnetze derselben Availability Zone erstrecken.

Erstellen Sie eine Flotte EC2

Um eine Flotte von Instances mit EC2 Fleet zu starten, müssen Sie in Ihrer Flottenanforderung nur die folgenden Parameter angeben, und die Flotte verwendet die Standardwerte für die anderen Parameter:

- `LaunchTemplateId` oder `LaunchTemplateName` – Gibt die zu verwendende Startvorlage an (die die Parameter für die zu startenden Instances enthält, wie beispielsweise den Instance-Typ, die Availability Zone)
- `TotalTargetCapacity` – Gibt die Gesamtzielkapazität für die Flotte an
- `DefaultTargetCapacityType` – Gibt an, ob die Standardkaufoption On-Demand oder Spot ist

Um die in der Startvorlage angegebenen Parameter außer Kraft zu setzen, können Sie eine oder mehrere Überschreibungen angeben. Jede Überschreibung kann nach Instance-Typ, Availability Zone, Subnetz und Höchstpreis variieren und eine unterschiedliche gewichtete Kapazität beinhalten. Als Alternative zur Angabe eines Instance-Typs können Sie die Attribute angeben, die eine Instance haben muss, und Amazon EC2 identifiziert alle Instance-Typen mit diesen Attributen. Weitere Informationen finden Sie unter Geben Sie Attribute für die Auswahl von Instance-Typen für EC2-Flotte oder Spot-Flotte an.

Für EC2 Flotten des Typs `instant` können Sie anstelle der AMI-ID einen Systems Manager Manager-Parameter angeben. Sie können den Systems-Manager-Parameter in der Überschreibung oder in der Startvorlage angeben. Weitere Informationen finden Sie unter Verwenden eines Systems-Manager-Parameters anstelle einer AMI-ID.

Die Flottenparameter in einer JSON-Datei angeben. Informationen zu allen möglichen Parametern, die Sie angeben können, finden Sie unter Alle EC2 Flottenkonfigurationsoptionen anzeigen.

Flottenkonfigurationsbeispiele finden Sie unter CLI-Beispielkonfigurationen für EC2 Fleet.

Derzeit gibt es keine Konsolenunterstützung für die Erstellung einer EC2 Flotte.

Um eine EC2 Flotte zu erstellen

Verwenden Sie den Befehl create-fleet, um die Flotte zu erstellen, und geben Sie die JSON-Datei an, welche die Flottenkonfigurationsparameter enthält.

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

Es folgt eine Beispielausgabe für eine Flotte des Typs `request` oder `maintain`:

```
{
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
}
```

Es folgt eine Beispielausgabe für eine Flotte des Typs `instant`, die die Zielkapazität gestartet hat:

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ],
```

```
      "InstanceType": "c5.large",
      "Platform": null
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-5678901234abcdef0",
        "i-5432109876abcdef9"
      ]
  ]
}
```

Es folgt eine Beispielausgabe für eine Flotte des Typs `instant`, die die Zielkapazität teilweise mit Fehlern für Instances gestartet hat, die nicht gestartet wurden:

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientInstanceCapacity",
      "ErrorMessage": ""
    },
```

```
  ],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ]
  ]
}
```

Es folgt eine Beispielausgabe für eine Flotte des Typs `instant`, die keine Instances gestartet hat:

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
    {
      "LaunchTemplateAndOverrides": {
```

```
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": []
}
```

Erstellen Sie eine EC2 Flotte, die fehlerhafte Spot-Instances ersetzt

EC2 Fleet überprüft alle zwei Minuten den Integritätsstatus der Instances in der Flotte. Der Zustand einer Instance lautet entweder `healthy` oder `unhealthy`.

EC2 Fleet ermittelt den Integritätsstatus einer Instance anhand der von Amazon bereitgestellten Statuschecks EC2. Eine Instance wird als `unhealthy` bestimmt, wenn der Status der Instance-Statusprüfung oder der Systemstatusprüfung für drei aufeinanderfolgende Zustandsprüfungen `impaired` ist. Weitere Informationen finden Sie unter Statuschecks für EC2 Amazon-Instances.

Sie können Ihre Flotte so konfigurieren, dass nicht voll funktionsfähige Spot-Instances ersetzt werden. Nach der Festlegung von `ReplaceUnhealthyInstances` auf `true` wird eine Spot Instance ersetzt, wenn sie als `unhealthy` gemeldet wird. Die Flotte kann die Zielkapazität einige Minuten lang unterschreiten, während eine nicht voll funktionsfähige Spot-Instance ersetzt wird.

Voraussetzungen

- Der Ersatz von Gesundheitschecks wird nur für EC2 Flotten unterstützt, die eine Zielkapazität beibehalten (Flotten vom Typ`maintain`), nicht für Flotten des Typs oder. `request` `instant`
- Der Austausch von Zustandsprüfungen wird nur für Spot-Instances unterstützt. Dieses Feature wird für On-Demand-Instances nicht unterstützt.
- Sie können Ihre EC2 Flotte so konfigurieren, dass fehlerhafte Instances nur ersetzt werden, wenn Sie sie erstellen.

- Benutzer können die Ersetzung im Rahmen von Zustandsprüfungen nur verwenden, wenn sie über die Berechtigung zum Aufrufen der `ec2:DescribeInstanceStatus`-Aktion verfügen.

Um eine EC2 Flotte so zu konfigurieren, dass sie fehlerhafte Spot-Instances ersetzt

1. Verwenden Sie die Informationen zum Erstellen einer EC2 Flotte inErstellen Sie eine Flotte EC2 .
2. Um die Flotte so zu konfigurieren, dass sie nicht voll funktionsfähige Spot Instances ersetzt, geben Sie in der JSON-Datei für `ReplaceUnhealthyInstances` `true` an.

Alle EC2 Flottenkonfigurationsoptionen anzeigen

Um die vollständige Liste der EC2 Flottenkonfigurationsparameter anzuzeigen, können Sie eine JSON-Datei generieren. Eine Beschreibung jedes Parameters finden Sie unter create-fleet.

Um eine JSON-Datei mit allen möglichen EC2 Flottenparametern zu generieren

Verwenden Sie den Befehl create-fleet (AWS CLI) und den `--generate-cli-skeleton` Parameter, um eine EC2 Fleet-JSON-Datei zu generieren, und leiten Sie die Ausgabe in eine Datei weiter, um sie zu speichern.

```
aws ec2 create-fleet \
    --generate-cli-skeleton input > ec2createfleet.json
```

Es folgt eine Beispielausgabe.

```
{
    "DryRun": true,
    "ClientToken": "",
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch"
            }
        },
        "InstanceInterruptionBehavior": "hibernate",
        "InstancePoolsToUseCount": 0,
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
```

```
        "MaxTotalPrice": ""
    },
    "OnDemandOptions": {
        "AllocationStrategy": "prioritized",
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        },
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
    },
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "",
                "LaunchTemplateName": "",
                "Version": ""
            },
            "Overrides": [
                {
                    "InstanceType": "r5.metal",
                    "MaxPrice": "",
                    "SubnetId": "",
                    "AvailabilityZone": "",
                    "WeightedCapacity": 0.0,
                    "Priority": 0.0,
                    "Placement": {
                        "AvailabilityZone": "",
                        "Affinity": "",
                        "GroupName": "",
                        "PartitionNumber": 0,
                        "HostId": "",
                        "Tenancy": "dedicated",
                        "SpreadDomain": "",
                        "HostResourceGroupArn": ""
                    },
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 0
                        },
                        "MemoryMiB": {
```

```
            "Min": 0,
            "Max": 0
        },
        "CpuManufacturers": [
            "amd"
        ],
        "MemoryGiBPerVCpu": {
            "Min": 0.0,
            "Max": 0.0
        },
        "ExcludedInstanceTypes": [
            ""
        ],
        "InstanceGenerations": [
            "previous"
        ],
        "SpotMaxPricePercentageOverLowestPrice": 0,
        "OnDemandMaxPricePercentageOverLowestPrice": 0,
        "BareMetal": "included",
        "BurstablePerformance": "required",
        "RequireHibernateSupport": true,
        "NetworkInterfaceCount": {
            "Min": 0,
            "Max": 0
        },
        "LocalStorage": "excluded",
        "LocalStorageTypes": [
            "ssd"
        ],
        "TotalLocalStorageGB": {
            "Min": 0.0,
            "Max": 0.0
        },
        "BaselineEbsBandwidthMbps": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorTypes": [
            "inference"
        ],
        "AcceleratorCount": {
            "Min": 0,
            "Max": 0
        },
```

```
                        "AcceleratorManufacturers": [
                            "amd"
                        ],
                        "AcceleratorNames": [
                            "a100"
                        ],
                        "AcceleratorTotalMemoryMiB": {
                            "Min": 0,
                            "Max": 0
                        }
                    }
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 0,
        "OnDemandTargetCapacity": 0,
        "SpotTargetCapacity": 0,
        "DefaultTargetCapacityType": "on-demand",
        "TargetCapacityUnitType": "memory-mib"
    },
    "TerminateInstancesWithExpiration": true,
    "Type": "instant",
    "ValidFrom": "1970-01-01T00:00:00",
    "ValidUntil": "1970-01-01T00:00:00",
    "ReplaceUnhealthyInstances": true,
    "TagSpecifications": [
        {
            "ResourceType": "fleet",
            "Tags": [
                {
                    "Key": "",
                    "Value": ""
                }
            ]
        }
    ],
    "Context": ""
}
```

Kennzeichnen Sie eine neue oder bestehende EC2 Fleet-Anfrage sowie die Instances und Volumes, die sie startet

Um Ihre EC2 Flottenanfragen und die damit gestarteten Instances und Volumes zu kategorisieren und zu verwalten, können Sie sie mit benutzerdefinierten Metadaten kennzeichnen. Sie können einer EC2 Flottenanfrage bei der Erstellung oder danach ein Tag zuweisen. Ebenso können Sie den Instances und Volumes ein Tag zuweisen, wenn sie von der Flotte gestartet werden oder später.

Wenn Sie eine Flottenanforderung markieren, werden die Instances und Volumes, die von der Flotte gestartet werden, nicht automatisch markiert. Sie müssen die von der Flotte gestarteten Instances und Volumes explizit markieren. Sie können festlegen, dass Tags nur der Flottenanforderung, nur den Instances, die von der Flotte gestartet werden oder nur den Volumes zugewiesen werden, die den Instances zugeordnet sind, die von der Flotte gestartet wurden oder allen von ihnen.

> **Note**
>
> Bei `instant`-Flottentypen können Sie Volumes markieren, die an On-Demand-Instances und Spot-Instances angehängt sind. Bei `request`- oder `maintain`-Flottentypen können Sie nur Volumes markieren, die an On-Demand-Instances angehängt sind.

Weitere Informationen zur Funktionsweise von Tags (Markierungen) finden Sie unter Kennzeichnen Sie Ihre EC2 Amazon-Ressourcen.

Voraussetzung

Gewähren Sie dem Benutzer die Berechtigung zum Markieren von Ressourcen. Weitere Informationen finden Sie unter Beispiel: Markieren von Ressourcen.

So gewähren Sie einem Benutzer die Berechtigung zum Markieren von Ressourcen

Erstellen Sie eine IAM-Richtlinie, die Folgendes beinhaltet:

- Die Aktion `ec2:CreateTags`. Dadurch erhält der Benutzer die Berechtigung zum Erstellen von Tags.
- Die Aktion `ec2:CreateFleet`. Dadurch erhält der Benutzer die Erlaubnis, eine EC2 Flottenanfrage zu erstellen.
- Für `Resource` wird empfohlen, dass Sie `"*"` angeben. Dadurch können Benutzer alle Ressourcentypen markieren.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Um eine neue EC2 Flottenanfrage zu taggen

Um eine EC2 Flottenanfrage bei der Erstellung zu taggen, geben Sie das Schlüssel-Wert-Paar in der JSON-Datei an, die zur Erstellung der Flotte verwendet wurde. Der Wert für `ResourceType` muss `fleet` sein. Wenn Sie einen anderen Wert angeben, schlägt die Flottenanforderung fehl.

Um Instances und Volumes zu taggen, die von einer Flotte gestartet wurden EC2

Um Instances und Volumes zu taggen, wenn sie von der Flotte gestartet werden, geben Sie die Tags in der Startvorlage an, auf die in der EC2 Flottenanfrage verwiesen wird.

> **Note**
>
> Sie können keine an Spot-Instances angehängt Volumes markieren, die von einem `request`- oder `maintain`-Flottentyp gestartet werden.

Um eine bestehende EC2 Flottenanfrage, Instance und ein Volume zu taggen

Verwenden Sie den Befehl create-tags, um vorhandene Ressourcen zu markieren.

```
aws ec2 create-tags \
```

```
    --resources fleet-12a34b55-67cd-8ef9-
ba9b-9208dEXAMPLE i-1234567890abcdef0 vol-1234567890EXAMPLE \
    --tags Key=purpose,Value=test
```

Beschreiben Sie eine EC2 Flotte, ihre Instanzen und ihre Ereignisse

Sie können Ihre EC2 Flottenkonfiguration, die Instances in Ihrer EC2 Flotte und den Ereignisverlauf Ihrer EC2 Flotte beschreiben.

Aufgaben

- Beschreiben Sie Ihre EC2 Flotte
- Beschreiben Sie alle Instanzen in Ihrer EC2 Flotte
- Beschreiben Sie den Ereignisverlauf für Ihre EC2 Flotte

Beschreiben Sie Ihre EC2 Flotte

AWS CLI

Um Ihre EC2 Flotte zu beschreiben

Verwenden Sie den Befehl describe-fleets.

```
aws ec2 describe-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Es folgt eine Beispielausgabe.

```
{
    "Fleets": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2022-02-09T03:35:52+00:00",
            "FleetId": "fleet-364457cd-3a7a-4ed9-83d0-7b63e51bb1b7",
            "FleetState": "active",
            "ExcessCapacityTerminationPolicy": "termination",
            "FulfilledCapacity": 2.0,
            "FulfilledOnDemandCapacity": 0.0,
            "LaunchTemplateConfigs": [
                {
                    "LaunchTemplateSpecification": {
```

```
                        "LaunchTemplateName": "my-launch-template",
                        "Version": "$Latest"
                    }
                }
            ],
            "TargetCapacitySpecification": {
                "TotalTargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "SpotTargetCapacity": 2,
                "DefaultTargetCapacityType": "spot"
            },
            "TerminateInstancesWithExpiration": false,
            "Type": "maintain",
            "ReplaceUnhealthyInstances": false,
            "SpotOptions": {
                "AllocationStrategy": "capacity-optimized",
                "InstanceInterruptionBehavior": "terminate"
            },
            "OnDemandOptions": {
                "AllocationStrategy": "lowestPrice"
            }
        }
    ]
}
```

PowerShell

Um Ihre EC2 Flotte zu beschreiben

Verwenden Sie das cmdlet Get-EC2FleetList.

```
Get-EC2FleetList `
    -FleetId fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Beschreiben Sie alle Instanzen in Ihrer EC2 Flotte

Die zurückgegebene Liste der laufenden Instances wird regelmäßig aktualisiert und kann veraltet sein.

AWS CLI

Um die Instances für die angegebene EC2 Flotte zu beschreiben

Verwenden Sie den Befehl describe-fleet-instances.

```
aws ec2 describe-fleet-instances \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Es folgt eine Beispielausgabe.

```
{
    "ActiveInstances": [
        {
            "InstanceId": "i-09cd595998cb3765e",
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-86k84j6p"
        },
        {
            "InstanceId": "i-09cf95167ca219f17",
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-dvxi7fsm"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

PowerShell

Um die Instances für die angegebene EC2 Flotte zu beschreiben

Verwenden Sie das cmdlet Get-EC2FleetInstanceList.

```
Get-EC2FleetInstanceList `
    -FleetId fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Beschreiben Sie den Ereignisverlauf für Ihre EC2 Flotte

Weitere Informationen über die Ereignisse im Ereignisverlauf finden Sie unter EC2 Arten von Flottenereignissen.

AWS CLI

Um die Ereignisse für die angegebene EC2 Flotte zu beschreiben

Verwenden Sie den Befehl describe-fleet-history.

```
aws ec2 describe-fleet-history \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --start-time 2020-06-01T00:00:00Z
```

Es folgt eine Beispielausgabe.

```
{
    "HistoryRecords": [
        {
            "EventInformation": {
                "EventSubType": "submitted"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:05.000Z"
        },
        {
            "EventInformation": {
                "EventSubType": "active"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:15.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "t2.small, ami-07c8bc5c1ce9598c3, ...",
                "EventSubType": "progress"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-083a1c446e66085d2"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
```

```
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-090db02406cc3c2d6"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
    "LastEvaluatedTime": "1970-01-01T00:00:00.000Z",
    "StartTime": "2020-06-01T00:00:00.000Z"
}
```

PowerShell

Um die Ereignisse für die angegebene EC2 Flotte zu beschreiben

Verwenden Sie das cmdlet Get-EC2FleetHistory.

```
Get-EC2FleetHistory `
    -FleetId fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE `
    -UtcStartTime 2020-06-01T00:00:00Z
```

Modifizieren Sie eine EC2 Flotte

Sie können die Gesamtzielkapazität, die Spot-Kapazität und die On-Demand-Kapazität einer EC2 Flotte ändern. Sie können auch festlegen, ob laufende Instances beendet werden sollen, wenn die neue Gesamtzielkapazität unter die aktuelle Größe der Flotte fällt.

Überlegungen

Beachten Sie bei der Änderung einer EC2 Flotte Folgendes:

- Flottenart — Sie können nur einen EC2 Flottentyp ändern`maintain`. Sie können eine EC2 Flotte vom Typ `request` oder nicht änder`instant`.
- Flottenparameter — Sie können die folgenden Parameter einer EC2 Flotte ändern:
  - `target-capacity-specification` – Zielkapazität erhöhen oder verringern für:
    - `TotalTargetCapacity`
    - `OnDemandTargetCapacity`

    - `SpotTargetCapacity`
  - `excess-capacity-termination-policy`— Ob laufende Instances beendet werden sollen, wenn die Gesamtzielkapazität der EC2 Flotte unter die aktuelle Flottengröße sinkt. Folgende sind gültige Werte:
    - `no-termination`
    - `termination`
- Verhalten der Flotte bei Erhöhung der Gesamtzielkapazität — Wenn Sie die Gesamtzielkapazität erhöhen, startet die EC2 Flotte die zusätzlichen Instances entsprechend der angegebenen Instance-Kaufoption`DefaultTargetCapacityType`, bei der es sich entweder um On-Demand-Instances oder Spot-Instances handelt, und entsprechend der angegebenen Zuweisungsstrategie.
- Verhalten der Flotte bei Verringerung der Spot-Zielkapazität — Wenn Sie die Spot-Zielkapazität verringern, löscht die EC2 Flotte alle offenen Anfragen, die die neue Zielkapazität überschreiten. Sie können anfordern, dass die Spot-Flotte Spot Instances beendet, bis die Größe der Flotte die neue Zielkapazität erreicht. Wenn eine EC2 Flotte eine Spot-Instance beendet, weil die Zielkapazität verringert wurde, erhält die Instance eine Benachrichtigung über eine Unterbrechung der Spot-Instance.

  Instances werden auf der Grundlage der Zuweisungsstrategie für die Beendigung ausgewählt:

  - `capacity-optimized` – Beendet Instances aus Pools mit der geringsten verfügbaren Kapazität.
  - `price-capacity-optimized` – Verwendet eine Kombination aus Preis und verfügbarer Kapazität: beendet Instances aus Pools mit der geringsten verfügbaren Kapazität und dem höchsten Preis unter diesen Pools.
  - `diversified` – Beendet Instances über alle Pools hinweg.
  - `lowest-price` – Beendet Instances aus Pools mit dem höchsten Preis.

  Alternativ können Sie verlangen, dass EC2 Fleet die Flotte auf ihrer aktuellen Größe belässt, aber keine Spot-Instances ersetzt, die unterbrochen wurden oder die Sie manuell beenden.
- Flottenstatus — Sie können eine EC2 Flotte ändern, die sich im `active` Status `submitted` oder befindet. Wenn Sie eine Flotte ändern, wird sie in den `modifying`-Zustand versetzt.

Befehle zum Ändern einer EC2 Flotte

AWS CLI

Um die Gesamtzielkapazität einer EC2 Flotte zu ändern

Verwenden Sie den Befehl modify-fleet.

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=20
```

Wenn Sie die Zielkapazität verringern, die aktuelle Größe der Flotte jedoch beibehalten möchten, können Sie das vorherige Bespiel wie folgt ändern:

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=10 \
    --excess-capacity-termination-policy no-termination
```

PowerShell

Um die Gesamtzielkapazität einer EC2 Flotte zu ändern

Verwenden Sie das cmdlet Edit-EC2Fleet.

```
Edit-EC2Fleet `
    -FleetId "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TargetCapacitySpecification_TotalTargetCapacity 20
```

Wenn Sie die Zielkapazität verringern, die aktuelle Größe der Flotte jedoch beibehalten möchten, können Sie das vorherige Bespiel wie folgt ändern:

```
Edit-EC2Fleet `
    -FleetId "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TargetCapacitySpecification_TotalTargetCapacity 20 `
    -ExcessCapacityTerminationPolicy "NoTermination"
```

Löschen Sie eine EC2 Flottenanfrage und die Instances in der Flotte

Wenn Sie eine EC2 Flottenanfrage nicht mehr benötigen, können Sie sie löschen. Nachdem Sie eine Flottenanforderung gelöscht haben, werden alle der Flotte zugeordneten Spot-Anfragen abgebrochen, sodass keine neuen Spot Instances gestartet werden.

Wenn Sie eine EC2 Flottenanfrage löschen, müssen Sie auch angeben, ob Sie alle zugehörigen Instanzen beenden möchten. Dazu gehören sowohl On-Demand-Instances als auch Spot-Instances. Bei `instant` Flotten muss EC2 Fleet die Instances beenden, wenn die Flotte gelöscht wird. Eine gelöschte `instant`-Flotte mit laufenden Instances wird nicht unterstützt.

> **Warning**
>
> Das Beenden einer Instance ist dauerhaft und irreversibel.
> Nachdem Sie eine Instance beendet haben, können Sie keine Verbindung mehr zu ihr herstellen und sie kann nicht wiederhergestellt werden. Alle angehängten Amazon-EBS-Volumes, die so konfiguriert sind, dass sie beim Beenden gelöscht werden, werden ebenfalls dauerhaft gelöscht und können nicht wiederhergestellt werden. Alle auf den Instance-Speicher-Volumes gespeicherten Daten gehen dauerhaft verloren. Weitere Informationen finden Sie unter Wie die Kündigung von Instances funktioniert.
> Bevor Sie eine Instance beenden, stellen Sie sicher, dass Sie alle Daten, die Sie nach der Beendigung behalten müssen, im persistenten Speicher gesichert haben.

Wenn Sie festlegen, dass die Instances beendet werden müssen, wenn die Flottenanforderung abgebrochen wird, wechselt die Flottenanforderung in den `deleted_terminating`-Status. Andernfalls befindet sie sich im `deleted_running`-Zustand und die Instances werden weiter ausgeführt, bis sie unterbrochen oder von Ihnen manuell beendet werden.

Einschränkungen

- Sie können bis zu 25 Flotten vom Typ `instant` in einem einzigen Vorgang löschen.
- Sie können bis zu 100 Flotten vom Typ `maintain` oder `request` in einem Vorgang löschen.
- Sie können bis zu 125 Flotten in einem einzigen Vorgang löschen, sofern Sie das oben angegebene Kontingent für jeden Flottentyp nicht überschreiten.
- Wenn Sie die angegebene Anzahl an zu löschenden Flotten überschreiten, werden keine Flotten gelöscht.

- Eine gelöschte `instant`-Flotte mit laufenden Instances wird nicht unterstützt. Wenn Sie eine `instant` Flotte löschen, beendet Amazon EC2 automatisch alle ihre Instances. Bei `instant`-Flotten mit mehr als 1 000 Instances schlägt die Löschanforderung möglicherweise fehl. Wenn Ihre Flotte über mehr als 1 000 Instances verfügt, beenden Sie die meisten Instances zunächst manuell, sodass 1 000 oder weniger übrig bleiben. Löschen Sie dann die Flotte, und die verbleibenden Instances werden automatisch beendet.

AWS CLI

Um eine EC2 Flottenanfrage zu löschen und ihre Instances zu beenden

Verwenden Sie den Befehl delete-fleets mit der Option `--terminate-instances`.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

Es folgt eine Beispielausgabe.

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_terminating",
            "PreviousFleetState": "active",
            "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
        }
    ]
}
```

Um eine EC2 Flottenanfrage zu löschen, ohne ihre Instanzen zu beenden

Ändern Sie das vorherige Beispiel, indem Sie stattdessen die Option `--no-terminate-instances` verwenden. Beachten Sie, dass `--no-terminate-instances` für `instant`-Flotten nicht unterstützt wird.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

Es folgt eine Beispielausgabe.

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_running",
            "PreviousFleetState": "active",
            "FleetId": "fleet-4b8aaae8-dfb5-436d-a4c6-3dafa4c6b7dcEXAMPLE"
        }
    ]
}
```

PowerShell

Um eine EC2 Flottenanfrage zu löschen und ihre Instanzen zu beenden

Verwenden Sie das Remove-EC2FleetCmdlet mit dem `-TerminateInstance` Parameter.

```
Remove-EC2Fleet `
    -FleetId "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TerminateInstance $true
```

Um eine EC2 Fleet-Anfrage zu löschen, ohne ihre Instanzen zu beenden

Ändern Sie das vorherige Beispiel, indem Sie den Wert des Parameters `-TerminateInstance` ändern.

```
Remove-EC2Fleet `
    -FleetId "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TerminateInstance $false
```

Beheben von Fehlern, wenn eine Flotte nicht gelöscht werden kann

Wenn eine EC2 Flottenanforderung nicht gelöscht werden kann, werden `UnsuccessfulFleetDeletions` in der Ausgabe die ID der EC2 Flottenanforderung, ein Fehlercode und eine Fehlermeldung zurückgegeben.

Die Fehlercodes sind:

- `ExceededInstantFleetNumForDeletion`

- `fleetIdDoesNotExist`
- `fleetIdMalformed`
- `fleetNotInDeletableState`
- `NoTerminateInstancesNotSupported`
- `UnauthorizedOperation`
- `unexpectedError`

Fehlerbehebung bei **`ExceededInstantFleetNumForDeletion`**

Wenn Sie versuchen, mehr als 25 `instant`-Flotten in einer einzigen Anfrage zu löschen, wird der `ExceededInstantFleetNumForDeletion`-Fehler zurückgegeben. Es folgt eine Beispielausgabe für diesen Fehler.

```
{
    "UnsuccessfulFleetDeletions": [
     {
          "FleetId": " fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
          "Error": {
                 "Message": "Can’t delete more than 25 instant fleets in a single
 request.",
                 "Code": "ExceededInstantFleetNumForDeletion"
           }
     },
     {
           "FleetId": "fleet-9a941b23-0286-5bf4-2430-03a029a07e31",
           "Error": {
                 "Message": "Can’t delete more than 25 instant fleets in a single
 request.",
                 "Code": "ExceededInstantFleetNumForDeletion"
            }
     }
     .
     .
     .
     ],
     "SuccessfulFleetDeletions": []
}
```

Fehlerbehebung bei **`NoTerminateInstancesNotSupported`**

Wenn Sie angeben, dass die Instances in einer `instant`-Flotte beim Löschen der Flotte nicht beendet werden dürfen, wird der `NoTerminateInstancesNotSupported`-Fehler zurückgegeben. `--no-terminate-instances` wird nicht für `instant`-Flotten unterstützt. Es folgt eine Beispielausgabe für diesen Fehler.

```
{
      "UnsuccessfulFleetDeletions": [
            {
                  "FleetId": "fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
                  "Error": {
                         "Message": "NoTerminateInstances option is not supported for
 instant fleet",
                         "Code": "NoTerminateInstancesNotSupported"
                   }
            }
       ],
       "SuccessfulFleetDeletions": []
}
```

Fehlerbehebung bei **`UnauthorizedOperation`**

Wenn Sie keine Berechtigung zum Beenden von Instances haben, erhalten Sie den `UnauthorizedOperation`-Fehler beim Löschen einer Flotte, die ihre Instances beenden muss. Das Folgende ist die Fehlerantwort.

```
<Response><Errors><Error><Code>UnauthorizedOperation</Code><Message>You are not
 authorized to perform this
operation. Encoded authorization failure message: VvuncIxj7Z_CPGNYXWqnuFV-
YjByeAU66Q9752NtQ-I3-qnDLWs6JLFd
KnSMMiq5s6cGqjjPtEDpsnGHzzyHasFHOaRYJpaDVravoW25azn6KNkUQQlFwhJyujt2dtNCdduJfrqcFYAjlEiRMkfDHt7
BHturzDK6A560Y2nDSUiMmAB1y9UNtqaZJ9SNe5sNxKMqZaqKtjRbk02RZu5V2vn9VMk6fm2aMVHbY9JhLvGypLcMUjtJ76
VPiU5v2s-
UgZ7h0p2yth6ysUdhlONg6dBYu8_y_HtEI54invCj4CoK0qawqzMNe6rcmCQHvtCxtXsbkgyaEbcwmrm2m01-
EMhekLFZeJLr
DtYOpYcEl4_nWFX1wtQDCnNNCmxnJZAoJvb3VMDYpDTsxjQv1PxODZuqWHs23YXWVywzgnLtHeRf2o4lUhGBw17mXsS07k7
PT9vrHtQiILor5VVTsjSPWg7edj__1rsnXhwPSu8gI48ZLRGrPQqFq0RmKO_QIE8N8s6NWzCK4yoX-9gDcheurOGpkprPIC
</Message></Error></Errors><RequestID>89b1215c-7814-40ae-a8db-41761f43f2b0</
RequestID></Response>
```

Um den Fehler zu beheben, müssen Sie die `ec2:TerminateInstances`-Aktion der IAM-Richtlinie hinzufügen, wie im folgenden Beispiel gezeigt.

Mit Spot-Flotten arbeiten

Zum Verwenden einer Spot-Flotte erstellen Sie eine Anforderung mit der Gesamtzielkapazität für Spot Instances, einem optionalen On-Demand-Anteil, und geben Sie entweder manuell ein AMI und ein Schlüsselpaar an oder geben Sie eine Startvorlage an, die die Konfiguration für die Instances in der Flotte enthält. Sie können optional zusätzliche Parameter angeben oder die Flotte Standardwerte verwenden lassen. Sie können die Flottenanforderung sowie ihre Instances und Volumes auch taggen, wenn Sie die Flotte erstellen.

Die Flotte startet On-Demand-Instances, wenn freie Kapazität vorhanden ist, und startet Spot Instances, wenn Ihr Höchstpreis den Spot-Preis übersteigt und Kapazität verfügbar ist.

Sobald Ihre Flotte gestartet ist, können Sie die Flottenanforderung, die Instances in der Flotte und alle Flottenereignisse beschreiben. Sie können bei Bedarf auch zusätzliche Tags zuweisen.

Wenn Sie Flottenparameter ändern müssen, z. B. die Gesamtzielkapazität, können Sie die Flotte ändern, vorausgesetzt, sie wurde so konfiguriert, dass sie die Kapazität beibehält. Sie können die Zielkapazität einer einmaligen Anfrage nach der Übermittlung nicht mehr ändern.

Eine Flotten-Anforderung bleibt solange aktiv, bis sie abläuft oder Sie sie verwerfen (löschen). Wenn Sie die Flottenanforderung stornieren, können Sie die Instances entweder beenden oder diese laufen lassen. Wenn Sie sich dafür entscheiden, sie laufen zu lassen, werden die On-Demand Instances ausgeführt, bis Sie sie beenden, und die Spot Instances laufen, bis sie unterbrochen werden oder Sie sie beenden.

Themen

- Status von Spot-Flotten-Anforderungen
- Spot-Flotten-Berechtigungen
- Erstellen einer Spot-Flotte
- Eine neue Spot-Flotte sowie die Instances und Volumes, die sie startet, markieren
- Eine Spot-Flottenanforderung, ihre Instances und den Ereignisverlauf beschreiben
- Ändern einer Spot-Flotten-Anforderung
- Spot-Flotten-Anforderung abbrechen (löschen)
- Automatische Skalierung für Spot-Flotten verstehen

Status von Spot-Flotten-Anforderungen

Eine Spot-Flotte-Anfrage kann einen von verschiedenen Status haben, wobei jeder Status auf eine andere Phase des Lebenszyklus der Anfrage und der Verwaltung der Instances hinweist.

Eine Spot-Flotten-Anforderung einen der folgenden Status aufweisen:

`submitted`

Die Spot-Flotte-Anfrage wird geprüft und Amazon EC2 bereitet sich darauf vor, die angestrebte Anzahl von Instances zu starten. Wenn eine Anforderung Ihre Spot-Flottenlimits überschreiten würde, wird sie sofort abgebrochen.

`active`

Die Spot-Flotte wurde validiert und Amazon EC2 versucht, die angestrebte Anzahl laufender Spot-Instances aufrechtzuerhalten. Die Anforderung bleibt so lange in diesem Zustand, bis sie geändert oder abgebrochen wird.

`modifying`

Die Spot-Flotten-Anforderung wird geändert. Die Anforderung bleibt in diesem Zustand, bis die Änderung vollständig bearbeitet oder die Anforderung abgebrochen wird. Nur ein `maintain`-Flottentyp kann geändert werden. Dieser Status gilt nicht für einen einmaligen `request`-Flottentyp.

`cancelled_running`

Die Spot-Flotte wird abgebrochen (gelöscht) und startet keine weiteren Spot Instances. Die bestehenden Instances laufen weiter, bis sie unterbrochen oder manuell beendet werden. Die Anforderung bleibt so lange in diesem Zustand, bis alle Instances unterbrochen oder beendet wurden.

`cancelled_terminating`

Die Spot-Flotten-Anforderung ist abgebrochen (gelöscht) und die zugehörigen Instances sind beendet. Die Anforderung bleibt so lange in diesem Zustand, bis alle Instances beendet wurden.

`cancelled`

Die Spot-Flotten-Anforderung ist abgebrochen (gelöscht) und hat keine ausgeführten Instances. Die Anforderung wird zwei Tage nach Beendigung der zugehörigen Instances gelöscht.

Spot-Flotten-Berechtigungen

Wenn Ihre Benutzer eine Spot-Flotte erstellen oder verwalten sollen, müssen Sie diesen die erforderlichen Berechtigungen gewähren.

Wenn Sie die EC2 Amazon-Konsole verwenden, um eine Spot-Flotte zu erstellen, werden zwei serviceverknüpfte Rollen mit dem Namen `AWSServiceRoleForEC2SpotFleet` und und eine Rolle mit dem Namen `aws-ec2-spot-fleet-tagging-role` erstelltAWSServiceRoleForEC2Spot, die der Spot-Flotte die Rechte gewähren, Ressourcen in Ihrem Namen anzufordern, zu starten, zu beenden und zu taggen. Wenn Sie die AWS CLI oder eine API verwenden, müssen Sie sicherstellen, dass diese Rollen vorhanden sind.

Verwenden Sie die folgenden Anweisungen, um die erforderlichen Berechtigungen zu erteilen und die Rollen zu erstellen.

Berechtigungen und Rollen

- Benutzern die Berechtigung für Spot-Flotte gewähren
- Serviceverknüpfte Rolle für Spot-Flotte
- Serviceverknüpfte Rolle für Spot-Instances
- IAM-Rolle zum Markieren einer Spot-Flotte

Benutzern die Berechtigung für Spot-Flotte gewähren

Wenn Ihre Benutzer eine Spot-Flotte erstellen oder verwalten, stellen Sie sicher, dass Sie ihnen die erforderlichen Berechtigungen gewähren.

So erstellen Sie eine Richtlinie für Spot-Flotte

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Policies und Create policy aus.
3. Wählen Sie auf der Seite Richtlinie erstellen die Option JSON aus und ersetzen Sie den Text durch Folgendes.

   JSON

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:CreateTags",
                "ec2:RequestSpotFleet",
                "ec2:ModifySpotFleetRequest",
                "ec2:CancelSpotFleetRequests",
                "ec2:DescribeSpotFleetRequests",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeSpotFleetRequestHistory"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole",
                "iam:ListRoles",
                "iam:ListInstanceProfiles"
            ],
            "Resource": "*"
        }
    ]
}
```

Die vorangehende Beispielrichtlinie gewährt einem Benutzer die Berechtigungen, die für die meisten Spot-Flotten-Anwendungsfälle erforderlich sind. Um den Benutzer auf bestimmte API-Aktionen zu beschränken, geben Sie stattdessen nur diese API-Aktionen an.

Erforderlich EC2 und IAM APIs

Folgendes APIs muss in der Richtlinie enthalten sein:

- `ec2:RunInstances` – erforderlich zum Launchen von Instances in einer Spot-Flotte

- `ec2:CreateTags` – erforderlich zum Markieren der Spot-Flotten-Anforderung, der Instances oder der Volumes
- `iam:PassRole` – erforderlich, um die Spot-Flotten-Rolle anzugeben
- `iam:CreateServiceLinkedRole` – erforderlich zum Erstellen der serviceverknüpften Rolle
- `iam:ListRoles` – erforderlich zum Aufzählen vorhandener IAM-Rollen
- `iam:ListInstanceProfiles` – erforderlich zum Aufzählen vorhandener Instance-Profile

> **Important**
>
> Wenn Sie in der Startspezifikation oder Startvorlage eine Rolle für das IAM-Instance-Profil angeben, müssen Sie dem Benutzer die Berechtigung gewähren, die Rolle an den Service zu übergeben. Schließen Sie hierzu in der IAM-Richtlinie `"arn:aws:iam::*:role/`*`IamInstanceProfile-role`*`"` als Ressource für die Aktion `iam:PassRole` ein. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erteilen von Benutzerberechtigungen zur Übergabe einer Rolle an einen AWS Dienst.

Spot-Flotte APIs

Fügen Sie Ihrer Richtlinie bei Bedarf die folgenden Spot Fleet API-Aktionen hinzu:

- `ec2:RequestSpotFleet`
- `ec2:ModifySpotFleetRequest`
- `ec2:CancelSpotFleetRequests`
- `ec2:DescribeSpotFleetRequests`
- `ec2:DescribeSpotFleetInstances`
- `ec2:DescribeSpotFleetRequestHistory`

Optionales IAM APIs

(Optional) Um einem Benutzer das Erstellen von Rollen oder Instance-Profilen mithilfe der IAM-Konsole zu ermöglichen, müssen Sie der Richtlinie die folgenden Aktionen hinzufügen:

- `iam:AddRoleToInstanceProfile`

- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

4. Wählen Sie Review policy (Richtlinie prüfen) aus.
5. Geben Sie auf der Seite Review policy (Richtlinie überprüfen) einen Richtlinienamen und eine Beschreibung ein und wählen Sie anschließend Create policy (Richtlinie erstellen) aus.
6. Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

   - Benutzer und Gruppen in AWS IAM Identity Center:

     Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

   - Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

     Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.

   - IAM-Benutzer:
     - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
     - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Serviceverknüpfte Rolle für Spot-Flotte

Amazon EC2 verwendet dienstbezogene Rollen für die Berechtigungen, die erforderlich sind, um andere AWS Dienste in Ihrem Namen aufzurufen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit einem Service verknüpft ist. AWS Mit Diensten verknüpfte Rollen bieten eine sichere Möglichkeit, Berechtigungen an AWS Dienste zu delegieren, da nur der verknüpfte Dienst eine dienstbezogene Rolle übernehmen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollen im IAM-Benutzerhandbuch.

Amazon EC2 verwendet die angegebene serviceverknüpfte Rolle AWSServiceRoleForEC2SpotFleet, um Instances in Ihrem Namen zu starten und zu verwalten.

> **Important**
>
> Wenn Sie in Ihrer Spot-Flotte ein verschlüsseltes AMI oder einen verschlüsselten Amazon EBS-Snapshot angeben, müssen Sie der AWSServiceRoleForEC2SpotFleetRolle die Berechtigung zur Verwendung des CMK erteilen, damit Amazon Instances in Ihrem Namen starten EC2 kann. Weitere Informationen finden Sie unter Gewähren Sie Zugriff auf CMKs zur Verwendung mit verschlüsselten Snapshots AMIs und EBS-Snapshots.

Berechtigungen erteilt von AWSService RoleFor EC2 SpotFleet

Die AWSServiceRoleForEC2SpotFleetRolle gewährt der Spot-Flotte die Berechtigung, Instances in Ihrem Namen anzufordern, zu starten, zu beenden und zu taggen. Amazon EC2 verwendet diese servicebezogene Rolle, um die folgenden Aktionen durchzuführen:

- `ec2:RequestSpotInstances` - Spot-Instances-Anforderung
- `ec2:RunInstances` – Starten von Instances
- `ec2:TerminateInstances` – Beenden von Instances
- `ec2:DescribeImages`- Beschreiben Sie Amazon Machine Images (AMIs) für die Instanzen
- `ec2:DescribeInstanceStatus` – Beschreiben des Status der Instances
- `ec2:DescribeSubnets` – Beschreiben der Subnetze für die Instances
- `ec2:CreateTags` – Hinzufügen von Tags zur Spot-Flotten-Anforderung, zu Instances und zu Volumes
- `elasticloadbalancing:RegisterInstancesWithLoadBalancer` – Hinzufügen der angegebenen Instances zum angegebenen Load Balancer
- `elasticloadbalancing:RegisterTargets` – Registrieren der die angegebenen Ziele bei der angegebenen Zielgruppe

Erstellen der serviceverknüpften Rolle

Größtenteils müssen Sie die serviceverknüpfte Rolle nicht manuell erstellen. Amazon EC2 erstellt die AWSServiceRoleForEC2SpotFleetserviceverknüpfte Rolle, wenn Sie zum ersten Mal eine Spot-Flotte mithilfe der Konsole erstellen.

Wenn Sie vor Oktober 2017, als Amazon EC2 begann, diese servicebezogene Rolle zu unterstützen, eine aktive Spot-Flotte-Anfrage hatten, EC2 hat Amazon die AWSServiceRoleForEC2SpotFleetRolle in Ihrem AWS Konto erstellt. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Eine neue Rolle wurde in meinem AWS Konto angezeigt.

Wenn Sie die AWS CLI oder eine API verwenden, um eine Spot-Flotte zu erstellen, müssen Sie zunächst sicherstellen, dass diese Rolle existiert.

Um die AWSService RoleFor EC2 SpotFleet Rolle für Spot-Flotte mithilfe der Konsole zu erstellen

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Rollen aus.
3. Wählen Sie Create role (Rolle erstellen) aus.
4. Gehen Sie auf der Seite Select trusted entity (Vertrauenswürdige Entität auswählen) wie folgt vor:
   a. Wählen Sie unter Vertrauenswürdiger Entitätstyp die Option AWS -Service aus.
   b. Wählen Sie unter Anwendungsfall für Service oder Anwendungsfall die Option aus EC2.
   c. Wählen Sie für Anwendungsfall die Option EC2 - Spot-Flotte aus.

      > **Note**
      >
      > Der Anwendungsfall EC2 — Spot Fleet erstellt automatisch eine Richtlinie mit den erforderlichen IAM-Berechtigungen und schlägt AWSEC2SpotFleetServiceRolePolicyals Rollennamen vor.

   d. Wählen Sie Weiter aus.
5. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next (Weiter) aus.
6. Wählen Sie auf der Seite Benennen, Überprüfen und Erstellen die Option Rolle erstellen aus.

Um die AWSService RoleFor EC2 SpotFleet Rolle für Spot Fleet mit dem zu erstellen AWS CLI

Verwenden Sie den create-service-linked-role-Befehl wie folgt:

```
aws iam create-service-linked-role --aws-service-name spotfleet.amazonaws.com
```

Wenn Sie Spot Fleet nicht mehr verwenden müssen, empfehlen wir Ihnen, die AWSServiceRoleForEC2SpotFleetRolle zu löschen. Nachdem diese Rolle aus Ihrem Konto gelöscht wurde, erstellt Amazon EC2 die Rolle erneut, wenn Sie über die Konsole eine Spot-Flotte anfordern. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Gewähren Sie Zugriff auf CMKs zur Verwendung mit verschlüsselten Snapshots AMIs und EBS-Snapshots

Wenn Sie in Ihrer Spot-Flottenanfrage ein verschlüsseltes AMI oder einen verschlüsselten Amazon EBS-Snapshot angeben und einen vom Kunden verwalteten Schlüssel für die Verschlüsselung verwenden, müssen Sie der AWSServiceRoleForEC2SpotFleetRolle die Berechtigung zur Verwendung des CMK erteilen, damit Amazon Instances in Ihrem Namen starten EC2 kann. Dazu müssen Sie eine Erteilung zum CMK hinzufügen, wie im Folgenden gezeigt:

Bei der Einrichtung von Berechtigungen ist die Erteilung von Berechtigung eine Alternative zu Schüsselrichtlinien. Weitere Informationen finden Sie unter Verwenden von Erteilungen und Verwenden von Schlüsselrichtlinien in AWS KMS im Developer-Handbuch für AWS Key Management Service .

Um der AWSService RoleFor EC2 SpotFleet Rolle Berechtigungen zur Nutzung des CMK zu erteilen

- Verwenden Sie den Befehl create-grant, um dem CMK einen Grant hinzuzufügen und den Principal (die mit dem AWSServiceRoleForEC2SpotFleetService verknüpfte Rolle) anzugeben, dem die Berechtigung erteilt wird, die mit dem Grant erlaubten Operationen auszuführen. Der CMK wird durch den Parameter `key-id` und den ARN des CMK spezifiziert. Der Principal wird durch den `grantee-principal` Parameter und den ARN der AWSServiceRoleForEC2SpotFleetdienstverknüpften Rolle angegeben.

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
spotfleet.amazonaws.com/AWSServiceRoleForEC2SpotFleet \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Serviceverknüpfte Rolle für Spot-Instances

Amazon EC2 verwendet die servicebezogene Rolle namens AWSServiceRoleForEC2Spot, um Spot-Instances in Ihrem Namen zu starten und zu verwalten. Weitere Informationen finden Sie unter Serviceverknüpfte Rolle für Spot-Instance-Anforderungen.

IAM-Rolle zum Markieren einer Spot-Flotte

Die IAM-Rolle `aws-ec2-spot-fleet-tagging-role` gewährt der Spot-Flotte die Berechtigung, die Spot-Flotten-Anforderung, -Instances und -Volumes zu markieren. Weitere Informationen finden Sie unter Eine neue Spot-Flotte sowie die Instances und Volumes, die sie startet, markieren.

> **Important**
>
> Wenn Sie sich dafür entscheiden, Instances in der Flotte zu markieren und gleichzeitig die Zielkapazität beizubehalten (die Spot-Flotten-Anfrage ist vom Typ `maintain`), können die Unterschiede in den Berechtigungen, die für den Benutzer und die `IamFleetRole` festgelegt sind, zu einem inkonsistenten Tag-Verhalten der Instances in der Flotte führen. Wenn `IamFleetRole` die `CreateTags`-Berechtigung nicht enthält, werden einige der von der Flotte gestarteten Instances möglicherweise nicht markiert. Während wir daran arbeiten, diese Inkonsistenz zu beheben, um sicherzustellen, dass alle Instances, die von der Flotte gestartet werden, markiert sind, empfehlen wir, die `aws-ec2-spot-fleet-tagging-role`-Rolle für die `IamFleetRole` zu verwenden. Um eine bestehende Rolle zu verwenden, können Sie alternativ die `AmazonEC2SpotFleetTaggingRole` AWS verwaltete Richtlinie an die bestehende Rolle anhängen. Andernfalls müssen Sie die `CreateTags`-Berechtigung manuell zu Ihrer vorhandenen Richtlinie hinzufügen.

So erstellen Sie die IAM-Rolle zum Markieren einer Spot-Flotte:

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Rollen aus.
3. Wählen Sie Create role (Rolle erstellen) aus.
4. Wählen Sie auf der Seite Select trusted entity (Auswahl der vertrauenswürdigen Entität) unter Trusted entity type (Auswahl der vertrauenswürdigen Entität) die Option AWS service (-Service) aus.
5. Wählen Sie unter Anwendungsfall unter Anwendungsfälle für andere AWS Dienste die Option EC2Spot Fleet Tagging ausEC2 .

6. Wählen Sie Weiter aus.
7. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next (Weiter) aus.
8. Geben Sie auf der Seite Name, review, and create (Benennen, überprüfen und erstellen) für Role name (Rollenname) einen Namen für die Rolle ein (z. B. **`aws-ec2-spot-fleet-tagging-role`**).
9. Überprüfen Sie die Informationen auf der Seite, und wählen Sie dann Create role (Rolle erstellen) aus.

Serviceübergreifende Confused-Deputy-Prävention

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine Entität, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine Entität mit größeren Rechten zwingen kann, die Aktion auszuführen. Wir empfehlen, dass Sie die globalen Bedingungskontext-Schlüssel `aws:SourceArn` und `aws:SourceAccount` in der `aws-ec2-spot-fleet-tagging-role`-Vertrauensrichtlinie verwenden, um die Berechtigungen, welche die Spot-Flotte einem anderen Service erteilt, auf die Ressource zu beschränken.

Um die SourceAccount Bedingungsschlüssel aws: SourceArn und aws: zur **`aws-ec2-spot-fleet-tagging-role`** Vertrauensrichtlinie hinzuzufügen

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Rollen.
3. Suchen Sie die `aws-ec2-spot-fleet-tagging-role`, die Sie zuvor erstellt haben, und wählen Sie den Link (nicht das Kontrollkästchen) aus.
4. Wählen Sie unter Summary (Zusammenfassung) die Registerkarte Trust Relationships (Vertrauensstellungen) und dann Edit trust policy (Vertrauensrichtlinie bearbeiten) aus.
5. Fügen Sie in der JSON-Anweisung ein `Condition`-Element hinzu, das Ihre globalen `aws:SourceAccount`- und `aws:SourceArn`-Bedingungskontextschlüssel zur Verhinderung des Confused-Deputy-Problems folgendermaßen festlegt:

```
"Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-request/
sfr-*"
      },
      "StringEquals": {
```

```
        "aws:SourceAccount": "111122223333"
      }
```

> **Note**
>
> Wenn der `aws:SourceArn`-Wert die Konto-ID enthält und Sie beide globalen Bedingungskontextschlüssel verwenden, müssen der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn`-Wert dieselbe Konto-ID verwenden, wenn sie in der gleichen Richtlinienanweisung verwendet wird.

Die endgültige Vertrauensrichtlinie wird folgendermaßen aussehen:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "spotfleet.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-
request/sfr-*"
      },
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      }
    }
  }
}
```

6. Wählen Sie Richtlinie aktualisieren.

Die folgende Tabelle enthält potenzielle Werte für `aws:SourceArn`, um den Umfang Ihrer `aws-ec2-spot-fleet-tagging-role` in unterschiedlichem Grad an Spezifität einzuschränken.

API-Operation	Aufgerufener Service	Scope	**aws:SourceArn**
RequestSpotFleet	AWS STS (AssumeRole)	Beschränken Sie die AssumeRole Funktion aws-ec2-spot-fleet-tagging-role spot-fleet-requests auf das angegebene Konto.	arn:aws:ec2:*: *123456789012* :spot-fleet-request/sfr-*
RequestSpotFleet	AWS STS (AssumeRole)	Beschränkt die AssumeRole Funktion aws-ec2-spot-fleet-tagging-role spot-fleet-requests auf das angegebene Konto und die angegebene Region. Beachten Sie, dass diese Rolle in anderen Regionen nicht verwendbar ist.	arn:aws:ec2: *us-east-1* :*123456789012* :spot-fleet-request/sfr-*
RequestSpotFleet	AWS STS (AssumeRole)	Begrenzen Sie die AssumeRole -Funktion in aws-ec2-spot-fleet-tagging-role nur auf Maßnahmen , welche die Flotte sfr-11111111-1111-1111-1111-111111111111 betreffen . Beachten Sie, dass diese Rolle	arn:aws:ec2: *us-east-1* :*123456789012* :spot-fleet-request/sfr-*11111111-1111-1111-1111-111111111111*

API-Operation	Aufgerufener Service	Scope	`aws:SourceArn`
		möglicherweise nicht für andere Spot-Flotten verwendbar ist. Außerdem kann diese Rolle nicht verwendet werden, um neue Spot-Flotten zu starten. request-spot-fleet	

Erstellen einer Spot-Flotte

Mit dem AWS-Managementkonsole können Sie schnell eine Spot-Flotte-Anfrage erstellen, indem Sie nur ein AMI und Ihre gewünschte Gesamtzielkapazität auswählen. Amazon konfiguriert EC2 eine Flotte, die Ihren Anforderungen am besten entspricht und die Best Practices von Spot befolgt. Andernfalls können Sie jede der Standardeinstellungen ändern.

Wenn Sie On-Demand-Instances in Ihre Flotte aufnehmen möchten, müssen Sie in Ihrer Anfrage eine Startvorlage angeben und die gewünschte On-Demand-Kapazität angeben.

Die Flotte startet On-Demand-Instances, wenn freie Kapazität vorhanden ist, und Spot Instances, wenn Ihr Höchstpreis den Spot-Preis übersteigt und Kapazität verfügbar ist.

Wenn Ihre Flotte Spot-Instances umfasst und dem Typ entspricht`maintain`, versucht Amazon, EC2 die Zielkapazität Ihrer Flotte aufrechtzuerhalten, wenn Ihre Spot-Instances unterbrochen werden.

Erforderliche Berechtigungen

Weitere Informationen finden Sie unter the section called “Spot-Flotten-Berechtigungen”.

Aufgaben

- Schnelle Erstellung einer Spot-Flottenanforderung
- Eine Spot-Flottenanforderung mit definierten Parametern erstellen
- Eine Spot-Flotte erstellen, die fehlerhafte Spot Instances ersetzt

Schnelle Erstellung einer Spot-Flottenanforderung

Gehen Sie wie folgt vor, um mithilfe der EC2 Amazon-Konsole schnell eine Spot-Flottenanfrage zu erstellen.

So erstellen Sie eine Spot-Flottenanforderung mit den empfohlenen Einstellungen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wenn Sie noch keine Erfahrung mit Spot haben, wird eine Willkommensseite angezeigt. Wählen Sie Get started aus. Wählen Sie andernfalls Spot-Flottenanforderung erstellen.
4. Wählen Sie unter Startparameter die Option Startparameter manuell konfigurieren aus.
5. Wählen Sie für AMI ein AMI aus.
6. Geben Sie unter Zielkapazität für Gesamtzielkapazität die Anzahl der anzufordernden Einheiten an. Als Einheitentyp können Sie InstancesCPUs, v oder Memory (GiB) wählen.
7. Überprüfen Sie für Ihre Flottenanforderung auf einen Blick Ihre Flottenkonfiguration und wählen Sie Start aus.

Eine Spot-Flottenanforderung mit definierten Parametern erstellen

Sie können eine Spot-Flotte mit von Ihnen definierten Parametern erstellen.

Console

So erstellen Sie eine Spot-Flottenanforderung mit definierten Parametern

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wenn Sie noch keine Erfahrung mit Spot haben, wird eine Willkommensseite angezeigt. Wählen Sie Get started aus. Wählen Sie andernfalls Spot-Flottenanforderung erstellen.
4. Für Startparameter können Sie die Startparameter entweder manuell konfigurieren oder eine Startvorlage verwenden, und zwar wie folgt:

    a. [Manuell konfigurieren] Um die Startparameter in der EC2 Amazon-Konsole zu definieren, wählen Sie Startparameter manuell konfigurieren und gehen Sie dann wie folgt vor:

i. Wählen Sie für AMI eines der von AMIs bereitgestellten Standardoptionen aus AWS, oder wählen Sie Search for AMI, um ein AMI aus unserer Benutzergemeinschaft AWS Marketplace, das oder eines Ihrer eigenen zu verwenden.

> **Note**
>
> Wenn ein in den Startparametern angegebenes AMI abgemeldet oder deaktiviert ist, können keine neuen Instances über das AMI gestartet werden. Bei Flotten, die darauf eingestellt sind, die Zielkapazität beizubehalten, wird die Zielkapazität nicht beibehalten.

ii. (Optional) Wählen Sie für Key pair name (Schlüsselpaarname= ein bestehendes Schlüsselpaar aus oder erstellen Sie ein neues.

[Bestehendes Schlüsselpaar] Wählen Sie das Schlüsselpaar aus.

[Neues Schlüsselpaar] Wählen Sie Neues Schlüsselpaar erstellen aus, um zur Seite Schlüsselpaare zu gelangen. Wenn Sie fertig sind, kehren Sie zur Seite Spot-Anfragen zurück und aktualisieren Sie die Liste.

iii. (Optional) Erweitern Sie Zusätzliche Startparameter und gehen Sie wie folgt vor:

A. (Optional) Um die Amazon-EBS-Optimierung zu aktivieren, wählen Sie für EBS-optimiert die Option EBS-optimierte Instance starten aus.

B. (Optional) Um temporären Speicher auf Blockebene für Ihre Instances hinzuzufügen, wählen Sie für Instance store (Instance-Speicher) die Option Attach at launch (Beim Start anhängen) aus.

C. (Optional) Um Speicher hinzuzufügen, wählen Sie Neues Volume hinzufügen aus und geben Sie je nach Instance-Typ zusätzliche Instance-Speicher-Volumes oder Amazon-EBS-Volumes an.

D. (Optional) Die grundlegende Überwachung ist standardmäßig für Ihre Instances aktiviert. Um die detaillierte Überwachung zu aktivieren, wählen Sie unter Überwachung die Option CloudWatch Detaillierte Überwachung aktivieren aus.

E. (Optional:) Wenn Sie für Tenancy eine Dedicated-Spot-Instance ausführen möchten, wählen Sie die Option Dedicated - run a dedicated instance (Dedicated – Dedicated-Instance ausführen) aus.

F. (Optional) Wählen Sie für Security groups (Sicherheitsgruppen) eine oder mehrere Sicherheitsgruppen aus oder erstellen Sie eine neue.

[Bestehende Sicherheitsgruppe] Wählen Sie eine oder mehrere Sicherheitsgruppen aus.

[Neue Sicherheitsgruppe] Wählen Sie Neue Sicherheitsgruppe erstellen aus, um zur Seite Sicherheitsgruppen zu gelangen. Wenn Sie fertig sind, kehren Sie zu den Spot-Anfragen zurück und aktualisieren Sie die Liste.

G. (Optional) Um Ihre Instances vom Internet aus erreichbar zu machen, wählen Sie für Automatische Zuweisung von IPv4 öffentlichen IP-Adressen die Option Aktivieren aus.

H. (Optional) Um Ihre Spot-Instances mit einer IAM-Rolle zu starten, geben Sie für IAM instance profile (IAM-Instance-Profil) die Rolle an.

I. (Optional) Wenn Sie ein Start-Skript ausführen möchten, kopieren Sie dieses in User data.

J. (Optional) Um ein Tag hinzuzufügen, wählen Sie Tag erstellen aus, geben Sie den Schlüssel und Wert für das Tag ein und wählen Sie Erstellen aus. Wiederholen Sie diesen Schritt für jeden Tag (Markierung).

Damit die Instances und die Spot-Flottenanforderung mit demselben Tag markiert werden, stellen Sie für jedes Tag sicher, dass sowohl Instance als auch Flotte ausgewählt ist. Um nur die von der Flotte gestarteten Instances zu markieren, löschen Sie Fleet. Um nur die Spot-Flottenanforderung zu markieren, löschen Sie Instances.

b. [Startvorlage] Um eine Konfiguration zu verwenden, die Sie in einer Startvorlage erstellt haben, wählen Sie Startvorlage verwenden und wählen Sie für Startvorlage eine Startvorlage aus.

> **Note**
>
> Wenn Sie On-Demand-Kapazität in Ihrer Spot-Flotte verwenden möchten, müssen Sie eine Startvorlage angeben.

5. Gehen Sie für Additional request details (Zusätzliche Anforderungsdetails) wie folgt vor:

a. Überprüfen Sie die zusätzlichen Details der Anfrage. Um Änderungen vorzunehmen, deaktivieren Sie Apply defaults (Standardeinstellungen anwenden).

b. (Optional) Für IAM fleet role (IAM-Flottenrolle) können Sie die Standardrolle verwenden oder eine andere Rolle auswählen. Um nach dem Ändern der Rolle die Standardrolle zu verwenden, wählen Sie Use default role (Standardrolle verwenden).

c. (Optional) Sie können eine Anfrage erstellen, die nur während eines bestimmten Zeitraums gültig ist, indem Sie Request valid from und Request valid until bearbeiten.

d. (Optional) Standardmäßig EC2 beendet Amazon Ihre Spot-Instances, wenn die Spot-Flotte-Anfrage abläuft. Um sie nach Ablauf Ihrer Anfrage am Laufen zu halten, deaktivieren Sie Terminate the instances when the request expires (Instances beenden, wenn die Anfrage abläuft).

e. (Optional) Um Ihre Spot-Instances mit einem Load Balancer zu registrieren, wählen Sie die Option Receive traffic from one or more load balancers (Datenverkehr von einem oder mehreren Load Balancern entgegennehmen) und legen Sie einen oder mehrere Classic Load Balancer oder Zielgruppen fest.

6. Führen Sie für die Zielkapazität die folgenden Schritte aus:

a. Geben Sie für Gesamtzielkapazität die Anzahl der anzufordernden Einheiten an. Als Einheitentyp können Sie InstancesCPUs, v oder Memory (MiB) wählen. Um eine Zielkapazität von 0 anzugeben (damit Sie später Kapazität hinzufügen können), wählen Sie Zielkapazität erhalten aus.

b. (Optional) Geben Sie für On-Demand-Basiskapazität einschließen die Anzahl der anzufordernden On-Demand-Einheiten an. Die Zahl muss unter der Total target capacity (Zielkapazität insgesamt) liegen. Amazon EC2 berechnet die Differenz und ordnet die Differenz den anzufordernden Spot-Einheiten zu.

> **Important**
>
> Um optionale On-Demand-Kapazität anzugeben, müssen Sie zunächst eine Startvorlage auswählen.

c. (Optional) Standardmäßig EC2 beendet Amazon Spot-Instances, wenn sie unterbrochen werden. Um die Zielkapazität aufrechtzuerhalten, wählen Sie Zielkapazität aufrechterhalten aus. Sie können dann angeben, dass Amazon Spot-Instances EC2

beendet, stoppt oder in den Ruhezustand versetzt, wenn sie unterbrochen werden. Hierzu wählen sie die entsprechende Option unter Interruption behavior aus.

> **Note**
>
> Wenn ein in den Startparametern angegebenes AMI abgemeldet oder deaktiviert ist, können keine neuen Instances über das AMI gestartet werden. In diesem Fall wird bei Flotten, die darauf eingestellt sind, die Zielkapazität beizubehalten, die Zielkapazität nicht aufrechterhalten.

d. (Optional) Damit die Spot-Flotte eine Ersatz-Spot-Instance starten kann, wenn eine Benachrichtigung zum Instance-Neuausgleich für eine vorhandene Spot-Instance in der Flotte ausgegeben wird, wählen Sie Neuausgleich der Kapazität und dann eine Instance-Ersetzungsstrategie aus. Wenn Sie Vor dem Beenden starten wählen, geben Sie die Verzögerung (in Sekunden) an, bis Amazon die alten Instances EC2 beendet. Weitere Informationen finden Sie unter Den Kapazitätsausgleich in der EC2-Flotte und der Spot-Flotte verwenden, um gefährdete Spot Instances zu ersetzen.

e. (Optional) Um den Betrag zu kontrollieren, den Sie pro Stunde für alle Spot-Instances in Ihrer Flotte zahlen, wählen Sie Maximalkosten für Spot-Instances einstellen und geben dann den maximalen Gesamtbetrag ein, den Sie pro Stunde zu zahlen bereit sind. Ist der maximale Gesamtbetrag erreicht, stoppt die Spot-Flotte das Starten von Spot-Instances auch dann, wenn die Zielkapazität noch nicht erreicht ist. Weitere Informationen finden Sie unter Ausgabenlimit für Ihre EC2-Flotte oder Spot-Flotte festlegen.

7. Gehen Sie unter Netzwerk wie folgt vor:

a. Wählen Sie für Netzwerk eine vorhandene VPC aus oder erstellen Sie eine neue.

[Vorhandene VPC] Wählen Sie die VPC aus.

[Neue VPC] Wählen Sie Create new VPC (Neue VPC erstellen aus, um zur Amazon VPC-Konsole zu gelangen. Wenn Sie fertig sind, kehren Sie zu dieser Bildschirmseite zurück und aktualisieren Sie die Liste.

b. (Optional) Lassen EC2 Sie Amazon für Availability Zone die Availability Zones für Ihre Spot-Instances auswählen, oder geben Sie eine oder mehrere Availability Zones an.

Wenn Sie mehr als ein Subnetz in einer Availability Zone haben, wählen Sie das geeignete Subnetz unter Subnet (Subnetz) aus. Um Subnetze hinzuzufügen, wählen Sie Create new subnet (Neues Subnetz) aus, um die Amazon VPC-Konsole aufzurufen.

Wenn Sie fertig sind, kehren Sie zu dieser Bildschirmseite zurück und aktualisieren Sie die Liste.

8. Für die Anforderungen an den Instance-Typ können Sie entweder Instance-Attribute angeben und Amazon EC2 anhand dieser Attribute die optimalen Instance-Typen identifizieren lassen, oder Sie können eine Liste von Instances angeben. Weitere Informationen finden Sie unter Geben Sie Attribute für die Auswahl von Instance-Typen für EC2-Flotte oder Spot-Flotte an.

   a. Wenn Sie Specify instance attributes that match your compute requirements (Instance-Attribute angeben, die Ihren Computinganforderungen entsprechen) auswählen, geben Sie Ihre Instance-Attribute wie folgt an:

      i. Geben Sie für v CPUs die gewünschte Mindest- und Höchstzahl von v einCPUs. Um kein Limit anzugeben, wählen Sie Kein Minimum oder Kein Maximum oder beides aus.

      ii. Geben Sie für Arbeitsspeicher (GiB) den gewünschten Mindest- und Höchstwert ein. Um kein Limit anzugeben, wählen Sie Kein Minimum, Kein Maximum oder beides aus.

      iii. (Optional) Für Zusätzliche Instance-Attribute können Sie optional ein oder mehrere Attribute angeben, um Ihre Datenverarbeitungsanforderungen genauer auszudrücken. Jedes zusätzliche Attribut fügt Ihrer Anforderung weitere Einschränkungen hinzu. Sie können die zusätzlichen Attribute weglassen. In diesem Fall werden die Standardwerte verwendet. Eine Beschreibung der einzelnen Attribute und ihrer Standardwerte finden Sie unter get-spot-placement-scores.

      iv. (Optional) Um die Instance-Typen mit Ihren angegebenen Attributen anzuzeigen, erweitern Sie Vorschau der übereinstimmenden Instance-Typen. Um Instance-Typen von der Verwendung in Ihrer Anfrage auszuschließen, wählen Sie die Instances und dann Ausgewählte Instance-Typen ausschließen aus.

   b. Bei der Auswahl von Instance-Typen manuell auswählen wird von der Spot-Flotte eine Standardliste von Instance-Typen angegeben. Um weitere Instance-Typen auszuwählen, wählen Sie Add instance types (Instance-Typen hinzufügen) und die Instance-Typen aus, die in Ihrer Anfrage verwendet werden sollen, und wählen Sie Auswählen aus. Um Instance-Typen zu löschen, wählen Sie die Instance-Typen und dann Löschen aus.

9. Wählen Sie unter Allokationsstrategie eine Spot-Allokationsstrategie und eine On-Demand-Allokationsstrategie, die Ihren Anforderungen entspricht. Weitere Informationen finden Sie unter Verwenden Sie Zuweisungsstrategien, um festzustellen, wie die EC2-Flotte oder Spot-Flotte die Spot- und On-Demand-Kapazitäten ausfüllt.

10. Überprüfen Sie für Ihre Flottenanfrage auf einen Blick Ihre Flottenkonfiguration und nehmen Sie gegebenenfalls Änderungen vor.
11. (Optional) Um eine Kopie der Startkonfiguration für die herunterzuladen AWS CLI, wählen Sie JSON-Konfiguration.
12. Wenn Sie bereit sind, Ihre Spot-Flotte zu erstellen, klicken Sie auf Starten.

    Der Spot-Flotten-Anforderungstyp lautet `fleet`. Wenn die Anforderung erfüllt wird, werden Anforderungen des Typs `instance` hinzugefügt, für die der Zustand `active` und der Status `fulfilled` lautet.

AWS CLI

So erstellen Sie eine Spot-Flottenanforderung

Verwenden Sie den Befehl request-spot-fleet.

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Beispiel-Konfigurationsdateien finden Sie unter Beispiel für CLI-Konfigurationen der Spot-Flotte.

PowerShell

So erstellen Sie eine Spot-Flottenanforderung

Verwenden Sie das cmdlet Request-EC2SpotFleet. Das folgende Beispiel startet Spot Instances in einer kapazitätsoptimierten Flotte

```
Request-EC2SpotFleet `
    -SpotFleetRequestConfig_TargetCapacity 50 `
    -SpotFleetRequestConfig_AllocationStrategy "CapacityOptimized" `
    -SpotFleetRequestConfig_IamFleetRole "arn:aws:iam::123456789012:role/my-spot-
fleet-role" `
    -SpotFleetRequestConfig_LaunchTemplateConfig @($launchConfig)
```

Definieren Sie die Startkonfiguration wie folgt, und legen Sie dabei die Startvorlage fest und überschreiben Sie die Eigenschaften, die Sie benötigen. Beispielkonfigurationen finden Sie unter Beispiel für CLI-Konfigurationen der Spot-Flotte.

```
$lcSpec = Amazon.EC2.Model.FleetLaunchTemplateSpecification
```

```
# To do - Set FleetLaunchTemplateSpecification properties
$lcOverrides = New-Object Amazon.EC2.Model.LaunchTemplateOverrides
# To do - Set LaunchTemplateOverrides properties
$launchConfig = New-Object Amazon.EC2.Model.LaunchTemplateConfig
$launchConfig.LaunchTemplateSpecification $lcSpec
$launchConfig.Overrides @($lcOverrides)
```

Eine Spot-Flotte erstellen, die fehlerhafte Spot Instances ersetzt

Die Spot-Flotte überprüft den Zustand der Spot-Instances in der Flotte alle zwei Minuten. Der Zustand einer Instance lautet entweder `healthy` oder `unhealthy`.

Spot Fleet ermittelt den Integritätsstatus einer Instance anhand der von Amazon bereitgestellten Statuschecks EC2. Wenn der Status der Instance-Statusprüfung oder der Systemstatusprüfung während drei aufeinanderfolgenden Zustandsprüfungen `impaired` lautet, ist der Zustand der Instance `unhealthy`. Weitere Informationen finden Sie unter Statuschecks für EC2 Amazon-Instances.

Sie können Ihre Flotte so konfigurieren, dass nicht voll funktionsfähige Spot-Instances ersetzt werden. Nach dem Aktivieren von Ersetzungen in Zuge von Zustandsprüfungen wird eine Spot Instance ersetzt, wenn sie als `unhealthy` gemeldet wird. Die Flotte kann die Zielkapazität einige Minuten lang unterschreiten, während eine nicht voll funktionsfähige Spot-Instance ersetzt wird.

Voraussetzungen

- Der Ersetzung von Zustandsprüfungen wird nur für Spot-Flotten unterstützt, welche eine Zielkapazität (Flotten vom Typ `maintain`) aufrechterhalten, nicht für einmalige Spot-Flotten (Flotten des Typs `request`).
- Der Austausch von Zustandsprüfungen wird nur für Spot-Instances unterstützt. Dieses Feature wird für On-Demand-Instances nicht unterstützt.
- Sie können Ihre Spot-Flotte nur beim Erstellen so konfigurieren, dass nicht voll funktionsfähige Instances ersetzt werden.
- Benutzer können die Ersetzung im Rahmen von Zustandsprüfungen nur verwenden, wenn sie über die Berechtigung zum Aufrufen der `ec2:DescribeInstanceStatus`-Aktion verfügen.

Console

So konfigurieren Sie eine Spot-Flotte, dass fehlerhafte Spot Instances ersetzt werden

1. Befolgen Sie die Schritte zum Erstellen einer Spot-Flotte in Eine Spot-Flottenanforderung mit definierten Parametern erstellen.
2. Um die Flotte so zu konfigurieren, dass fehlerhafte Spot Instances ersetzt werden, erweitern Sie Zusätzliche Startparameter und wählen Sie unter Zustandsprüfung die Option Fehlerhafte Instances ersetzen aus. Zum Aktivieren dieser Option müssen Sie zuerst Maintain target capacity (Zielkapazität erhalten) auswählen.

AWS CLI

So konfigurieren Sie eine Spot-Flotte, dass fehlerhafte Spot Instances ersetzt werden

Verwenden Sie den request-spot-fleetBefehl mit der `ReplaceUnhealthyInstances` Eigenschaft von`SpotFleetRequestConfig`.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "lowestPrice",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "TargetCapacity": 10,
        "ReplaceUnhealthyInstances": true
    }
}
```

PowerShell

So konfigurieren Sie eine Spot-Flottenanforderung, dass fehlerhafte Spot Instances ersetzt werden

Verwenden Sie das Request-EC2SpotFleetCmdlet mit dem `-SpotFleetRequestConfig_ReplaceUnhealthyInstance` Parameter.

```
-SpotFleetRequestConfig_ReplaceUnhealthyInstance $true
```

Eine neue Spot-Flotte sowie die Instances und Volumes, die sie startet, markieren

Zur besseren Kategorisierung und Verwaltung Ihrer Spot-Fleet- Anforderungen und der von ihr gestarteten Instances und Volumes können Sie diese mit benutzerdefinierten Metadaten markieren. Sie können einer Spot-Flotten-Anforderung beim Erstellen oder danach eine Markierung zuweisen. Ebenso können Sie den Instances und Volumes ein Tag zuweisen, wenn sie von der Flotte gestartet werden oder später.

Wenn Sie eine Flottenanforderung markieren, werden die Instances und Volumes, die von der Flotte gestartet werden, nicht automatisch markiert. Sie müssen die von der Flotte gestarteten Instances und Volumes explizit markieren. Sie können festlegen, dass Tags nur der Flottenanforderung, nur den Instances, die von der Flotte gestartet werden oder nur den Volumes zugewiesen werden, die den Instances zugeordnet sind, die von der Flotte gestartet wurden oder allen von ihnen.

> **Note**
>
> Sie können nur Volumes markieren, die an On-Demand-Instances angehängt sind. Sie können Volumes, die an Spot-Instances angehängt sind, nicht markieren.

Sie können Tags über die EC2 Amazon-Konsole oder ein Befehlszeilentool zuweisen.

Weitere Informationen zur Funktionsweise von Tags (Markierungen) finden Sie unter Kennzeichnen Sie Ihre EC2 Amazon-Ressourcen.

Inhalt

- Voraussetzung
- Markieren einer neuen Spot-Flotte sowie der Instances und Volumes, die sie startet
- Markieren bestehender Spot-Flotten
- Anzeigen der Tags (Markierungen) für Spot-Flotten-Anforderungen

Voraussetzung

Gewähren Sie dem Benutzer die Berechtigung zum Markieren von Ressourcen. Weitere Informationen finden Sie unter Beispiel: Markieren von Ressourcen.

So gewähren Sie einem Benutzer die Berechtigung zum Markieren von Ressourcen

Erstellen Sie eine IAM-Richtlinie, die Folgendes enthält:

- Die Aktion `ec2:CreateTags`. Dadurch erhält der Benutzer die Berechtigung zum Erstellen von Tags.
- Die Aktion `ec2:RequestSpotFleet`. Dadurch wird dem Benutzer die Berechtigung zum Erstellen einer Spot-Flotten-Anfrage gewährt.
- Für `Resource` müssen Sie `"*"` angeben. Dadurch können Benutzer alle Ressourcentypen markieren.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotFleetRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:RequestSpotFleet"
            ],
            "Resource": "*"
        }
    ]
}
```

Important

Derzeit unterstützen wir keine Berechtigungen auf Ressourcenebene für die `spot-fleet-request`-Ressource. Wenn Sie `spot-fleet-request` als Ressource angeben, erhalten Sie eine nicht autorisierte Ausnahme, wenn Sie versuchen, die Flotte zu markieren. Das folgende Beispiel veranschaulicht, wie die Richtlinie nicht festgelegt wird.

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:RequestSpotFleet"
```

```
    ],
    "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-request/*"
}
```

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Markieren einer neuen Spot-Flotte sowie der Instances und Volumes, die sie startet

Eine neue Spot-Flotten-Anforderung und die Instances und Volumes, die sie startet, mit der Konsole markieren

1. Folgen Sie dem Verfahren unter Eine Spot-Flottenanforderung mit definierten Parametern erstellen.
2. Wie Sie ein Tag hinzufügen, hängt davon ab, ob Sie die Flotte manuell konfiguriert oder eine Startvorlage verwendet haben.

   - Wenn Sie die Flotte manuell konfiguriert haben, gehen Sie folgendermaßen vor:

     Um ein Tag (Markierung) hinzuzufügen, erweitern Sie Zusätzliche Startkonfigurationen, wählen Sie Tag erstellen, und geben Sie den Schlüssel und den Wert für das Tag ein. Wiederholen Sie diesen Schritt für jeden Tag (Markierung).

Sie können die Spot-Flotten-Anforderung und die Instances jeweils mit demselben Tag (Markierung) markieren. Um beide zu markieren, stellen Sie sicher, dass sowohl Instances, als auch Flotte ausgewählt sind. Um nur die Spot-Flottenanforderung zu markieren, löschen Sie Instances. Um nur die von der Flotte gestarteten Instances zu markieren, löschen Sie Fleet.

> **Note**
>
> Wenn Sie eine Flotte manuell konfigurieren, gibt es keine Möglichkeit, Volumes zu taggen. Volume-Tags (Markierungen) werden nur für Volumes unterstützt, die an On-Demand-Instances angefügt sind. Wenn Sie eine Flotte manuell konfigurieren, können Sie keine On-Demand-Instances angeben.

- Wenn Sie eine Startvorlage verwendet haben, gehen Sie folgendermaßen vor:

  Um der Flottenanforderung ein Tag hinzuzufügen, wählen Sie unter Tags Tag erstellen und geben Sie den Schlüssel und den Wert für das Tag ein. Wiederholen Sie diesen Schritt für jeden Tag (Markierung).

  Um die Ressourcen in Ihrer Flotte zu taggen, müssen Sie Tags in der Startvorlage angeben.

Um eine neue Spot-Flotte-Anfrage und die damit gestarteten Instances und Volumes zu taggen, verwenden Sie den AWS CLI

Um eine Spot-Flotten-Anforderung beim Erstellen zu markieren, und um die Instances und Volumes zu markieren, wenn sie von der Flotte gestartet werden, konfigurieren Sie die Spot-Flotten-Anforderung wie folgt:

Tags (Markierungen) für Spot-Flotten-Anforderungen:

- Legen Sie die Tags für die Spot-Flotten-Anforderung in `SpotFleetRequestConfig` fest.
- Legen Sie für `ResourceType` die Option `spot-fleet-request` fest. Wenn Sie einen anderen Wert angeben, schlägt die Flottenanforderung fehl.
- Geben Sie für `Tags` das Schlüssel-Wert-Paar an. Sie können mehr als ein Schlüssel-Wert-Paar angeben.

Instance-Tags (Markierungen):

- Geben Sie die Tags für die Instances in `LaunchSpecifications` an.
- Legen Sie für `ResourceType` die Option `instance` fest. Wenn Sie einen anderen Wert angeben, schlägt die Flottenanforderung fehl.
- Geben Sie für `Tags` das Schlüssel-Wert-Paar an. Sie können mehr als ein Schlüssel-Wert-Paar angeben.

  Alternativ können Sie die Markierungen für die Instance in der Startvorlage angeben, auf die in der Spot-Flotten-Anforderung verwiesen wird.

Volume-Tags (Markierungen):

- Geben Sie die Markierungen für die Volumes in der Startvorlage an, auf die in der Spot-Flotten-Anforderung verwiesen wird. Die Volume-Markierung in `LaunchSpecifications` wird nicht unterstützt.

Im folgenden Beispiel wird die Spot-Flotten-Anforderung mit zwei Tags (Markierungen) markiert: Key=Environment und Value=Production sowie Key=Cost-Center und Value=123. Die Instances, die von der Flotte gestartet werden, werden mit einer Markierung markiert (diese entspricht einer der Tags (Markierungen) für die Spot-Flotten-Anforderung): Key=Cost-Center und Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
```

```
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1,
        "TagSpecifications": [
            {
                "ResourceType": "spot-fleet-request",
                "Tags": [
                    {
                        "Key": "Environment",
                        "Value":"Production"
                    },
                    {
                        "Key": "Cost-Center",
                        "Value":"123"
                    }
                ]
            }
        ]
    }
}
```

Um Instances zu taggen, die von einer Spot-Flotte gestartet wurden, mit dem AWS CLI

Um Instances zu markieren, wenn sie von der Flotte gestartet werden, können Sie entweder die Markierungen in der Startvorlage angeben, auf die in der Spot-Flotten-Anforderung verwiesen wird oder die Markierungen in der Spot-Flotten-Anforderung wie folgt angeben:

- Geben Sie die Tags für die Instances in `LaunchSpecifications` an.
- Legen Sie für `ResourceType` die Option `instance` fest. Wenn Sie einen anderen Wert angeben, schlägt die Flottenanforderung fehl.
- Geben Sie für `Tags` das Schlüssel-Wert-Paar an. Sie können mehr als ein Schlüssel-Wert-Paar angeben.

Im folgenden Beispiel werden die Instances, die von der Flotte gestartet werden, mit einem Tags (Markierungen) gekennzeichnet: Key=Cost-Center und Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1
    }
}
```

Um Volumes, die an On-Demand-Instances angehängt sind, die von einer Spot-Flotte gestartet wurden, mit dem AWS CLI

Um Volumes zu markieren, wenn sie von der Flotte erstellt werden, müssen Sie die Markierungen in der Startvorlage angeben, auf die in der Spot-Flotten-Anforderung verwiesen wird.

> **Note**
>
> Volume-Tags (Markierungen) werden nur für Volumes unterstützt, die an On-Demand-Instances angefügt sind. Sie können Volumes, die an Spot-Instances angehängt sind, nicht markieren.
> Die Volume-Markierung in `LaunchSpecifications` wird nicht unterstützt.

Markieren bestehender Spot-Flotten

So markieren Sie eine vorhandene Spot-Flotten-Anforderung mithilfe der Konsole:

Nachdem Sie eine Spot-Flotten-Anforderung erstellt haben, können Sie der Flottenanforderung mithilfe der Konsole Tags hinzufügen.

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus.
4. Wählen Sie die Registerkarte Tags (Markierungen), und wählen Sie Create Tags (Tags (Markierungen) erstellen).

Um eine bestehende Spot-Flotte-Anfrage mit dem zu kennzeichnen AWS CLI

Sie können den Befehl create-Tags verwenden, um vorhandene Ressourcen zu markieren. Im folgenden Beispiel wird die vorhandene Spot-Flotten-Anforderung mit Key=purpose und Value=test markiert.

```
aws ec2 create-tags \
    --resources sfr-11112222-3333-4444-5555-66666EXAMPLE \
    --tags Key=purpose,Value=test
```

Anzeigen der Tags (Markierungen) für Spot-Flotten-Anforderungen

So zeigen Sie Tags (Markierungen) für Spot-Flotten-Anforderungen mithilfe der Konsole an:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.

3. Wählen Sie Ihre Spot-Flotten-Anforderung und dann die Registerkarte Tags (Tags (Markierungen)) aus.

So beschreiben Sie Tags (Markierungen) für Spot-Flotten-Anforderungen:

Verwenden Sie den Befehl describe-tags, um die Tags (Markierungen) für die angegebene Ressource anzuzeigen. Im folgenden Beispiel beschreiben Sie die Tags (Markierungen) für die angegebene Spot-Flotten-Anforderung.

```
aws ec2 describe-tags \
    --filters "Name=resource-id,Values=sfr-11112222-3333-4444-5555-66666EXAMPLE"
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Production"
        },
        {
            "Key": "Another key",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Another value"
        }
    ]
}
```

Sie können die Tags (Markierungen) einer Spot-Flotten-Anforderung auch anzeigen, indem Sie die Spot-Flotten-Anforderung beschreiben.

Verwenden Sie den describe-spot-fleet-requestsBefehl, um die Konfiguration der angegebenen Spot-Flotte-Anfrage anzuzeigen, die alle Tags enthält, die für die Flottenanforderung angegeben wurden.

```
aws ec2 describe-spot-fleet-requests \
    --spot-fleet-request-ids sfr-11112222-3333-4444-5555-66666EXAMPLE
```

```
{
    "SpotFleetRequestConfigs": [
```

```
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2020-02-13T02:49:19.709Z",
            "SpotFleetRequestConfig": {
                "AllocationStrategy": "capacityOptimized",
                "OnDemandAllocationStrategy": "lowestPrice",
                "ExcessCapacityTerminationPolicy": "Default",
                "FulfilledCapacity": 2.0,
                "OnDemandFulfilledCapacity": 0.0,
                "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-
tagging-role",
                "LaunchSpecifications": [
                    {
                        "ImageId": "ami-0123456789EXAMPLE",
                        "InstanceType": "c4.large"
                    }
                ],
                "TargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "Type": "maintain",
                "ReplaceUnhealthyInstances": false,
                "InstanceInterruptionBehavior": "terminate"
            },
            "SpotFleetRequestId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "SpotFleetRequestState": "active",
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
                },
                {
                    "Key": "Another key",
                    "Value": "Another value"
                }
            ]
        }
    ]
}
```

Eine Spot-Flottenanforderung, ihre Instances und den Ereignisverlauf beschreiben

Sie können Ihre Spot-Flottenkonfiguration, die Instances in Ihrer Spot-Flotte und den Ereignisverlauf Ihrer Spot-Flotte beschreiben.

Console

So beschreiben Sie Ihre Spot-Flotte

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus. Die ID beginnt mit sfr-. Um die Konfigurationsdetails anzuzeigen, wählen Sie Description (Beschreibung) aus.
4. Um die Spot-Instances für die Spot-Flotte aufzulisten, wählen Sie Instances aus.
5. Zum Anzeigen des Verlaufs für die Spot-Flotte wählen Sie History (Verlauf) aus.

AWS CLI

So beschreiben Sie Ihre Spot-Flottenanforderung

Verwenden Sie den Befehl describe-spot-fleet-requests.

```
aws ec2 describe-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

So beschreiben Sie die laufenden Instances für die angegebene Spot-Flottenanforderung

Verwenden Sie den Befehl describe-spot-fleet-instances.

```
aws ec2 describe-spot-fleet-instances \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

So beschreiben Sie den Ereignisverlauf für die angegebene Spot-Flottenanforderung

Verwenden Sie den Befehl describe-spot-fleet-request-history.

```
aws ec2 describe-spot-fleet-request-history \
```

```
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --start-time 2024-05-18T00:00:00Z
```

PowerShell

So beschreiben Sie Ihre Spot-Flottenanforderung

Verwenden Sie das cmdlet Get-EC2SpotFleetRequest.

```
Get-EC2SpotFleetRequest
```

So beschreiben Sie die laufenden Instances für die angegebene Spot-Flottenanforderung

Verwenden Sie das cmdlet Get-EC2SpotFleetInstance.

```
Get-EC2SpotFleetInstance `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
```

So beschreiben Sie den Ereignisverlauf für die angegebene Spot-Flottenanforderung

Verwenden Sie das cmdlet Get-EC2SpotFleetRequestHistory.

```
Get-EC2SpotFleetRequestHistory `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -UtcStartTime 2024-05-18T00:00:00Z
```

Ändern einer Spot-Flotten-Anforderung

Sie können eine aktive Spot-Flotten-Anforderung ändern, um die folgenden Aufgaben auszuführen:

- Erhöhen der Zielkapazität und des On-Demand-Anteils
- Verringern der Zielkapazität und des On-Demand-Anteils

Wenn Sie die Gesamtzielkapazität erhöhen, startet die Spot-Flotte die zusätzlichen Spot Instances gemäß der Zuweisungsstrategie für die Spot-Flottenanforderung. Wenn Sie den On-Demand-Anteil erhöhen, startet die Spot-Flotte zusätzliche On-Demand-Instances.

Wenn Sie die Zielkapazität verringern, bricht die Spot-Flotte alle offenen Anforderungen ab, welche die neue Zielkapazität überschreiten. Sie können anfordern, dass die Spot-Flotte Spot-Instances

beendet, bis die Größe der Flotte die neue Zielkapazität erreicht hat. Wenn die Zuweisungsstrategie `diversified` lautet, beendet die Spot-Flotte Instances in allen Pools. Alternativ können Sie anfordern, dass die Spot-Flotte ihre aktuelle Größe beibehält, dabei jedoch keine Spot-Instances ersetzt, die unterbrochen werden oder die Sie manuell beenden.

Überlegungen

- Sie können eine einmalige Spot-Flotten-Anforderung nicht ändern. Sie können eine Spot-Flotten-Anforderung nur ändern, wenn Sie beim Erstellen der Spot-Flotten-Anforderung Maintain target capacity (Zielkapazität erhalten) ausgewählt hatten.
- Wenn eine Spot-Flotte eine Instance aufgrund einer Verringerung der Zielkapazität beendet, erhält die Instance eine Benachrichtigung über die Unterbrechung einer Spot-Instance.

Console

So ändern Sie eine Spot-Flottenanforderung

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus.
4. Wählen Sie Actions (Aktionen)und dann Modify target capacity (Zielkapazität bearbeiten) aus.
5. Führen Sie unter Modify target capacity die folgenden Schritte aus:
   a. Geben Sie die neue Zielkapazität und den neuen On-Demand-Anteil ein.
   b. (Optional) Wenn Sie die Zielkapazität verringern, die aktuelle Größe der Flotte jedoch beibehalten möchten, heben Sie die Auswahl von Terminate instances (Instances beenden) auf.
   c. Klicken Sie auf Submit (Absenden).

AWS CLI

So ändern Sie eine Spot-Flottenanforderung

Verwenden Sie den modify-spot-fleet-requestBefehl, um die Zielkapazität der angegebenen Spot-Flotte-Anfrage zu aktualisieren.

```
aws ec2 modify-spot-fleet-request \
```

```
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 20
```

Sie können den vorherigen Befehl folgendermaßen ändern, um die Zielkapazität der angegebenen Spot-Flotte zu verringern, ohne dadurch Spot-Instances zu beenden.

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 10 \
    --excess-capacity-termination-policy NoTermination
```

PowerShell

So ändern Sie eine Spot-Flottenanforderung

Verwenden Sie das Edit-EC2SpotFleetRequestCmdlet, um die Zielkapazität der angegebenen Spot-Flottenanforderung zu aktualisieren.

```
Edit-EC2SpotFleetRequest `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TargetCapacity 20
```

Sie können den vorherigen Befehl folgendermaßen ändern, um die Zielkapazität der angegebenen Spot-Flotte zu verringern, ohne dadurch Spot-Instances zu beenden.

```
Edit-EC2SpotFleetRequest `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TargetCapacity 20 `
    -ExcessCapacityTerminationPolicy "NoTermination"
```

Spot-Flotten-Anforderung abbrechen (löschen)

Wenn Sie eine Spot-Flotte nicht mehr benötigen, können Sie die Spot-Flotten-Anfrage abbrechen, was die Anforderung löscht. Nachdem Sie eine Flotten-Anfrage storniert haben, werden auch alle der Flotte zugeordneten Spot-Anfragen storniert, sodass keine neuen Spot-Instances gestartet werden.

Wenn Sie eine Spot-Flotte-Anfrage stornieren, müssen Sie auch angeben, ob Sie alle zugehörige Instances beenden möchten. Dazu gehören sowohl On-Demand-Instances als auch Spot-Instances.

> **Warning**
>
> Das Beenden einer Instance ist dauerhaft und irreversibel.
> Nachdem Sie eine Instance beendet haben, können Sie keine Verbindung mehr zu ihr herstellen und sie kann nicht wiederhergestellt werden. Alle angehängten Amazon-EBS-Volumes, die so konfiguriert sind, dass sie beim Beenden gelöscht werden, werden ebenfalls dauerhaft gelöscht und können nicht wiederhergestellt werden. Alle auf den Instance-Speicher-Volumes gespeicherten Daten gehen dauerhaft verloren. Weitere Informationen finden Sie unter Wie die Kündigung von Instances funktioniert.
> Bevor Sie eine Instance beenden, stellen Sie sicher, dass Sie alle Daten, die Sie nach der Beendigung behalten müssen, im persistenten Speicher gesichert haben.

Wenn Sie festlegen, dass die Instances beendet werden müssen, wenn die Flotten-Anfrage abgebrochen wird, wechselt die Flotten-Anfrage in den `cancelled_terminating`-Status. Andernfalls befindet sie sich im `cancelled_running`-Zustand und die Instances werden weiter ausgeführt, bis sie unterbrochen oder von Ihnen manuell beendet werden.

Einschränkungen

- Sie können bis zu 100 Flotten in einer einzigen Anfrage abbrechen. Wenn Sie die angegebene Anzahl überschreiten, werden keine Flotten abgebrochen.

Console

So können Sie eine Spot-Flottenanforderung abbrechen (löschen)

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus.
4. Wählen Sie Actions (Aktionen), Cancel request (Anforderungen abbrechen).
5. Gehen Sie im Dialogfeld Spot-Anfrage stornieren wie folgt vor:

   a. Um die zugeordneten Instances gleichzeitig mit dem Abbrechen der Spot-Flotten-Anforderung zu beenden, belassen Sie das Kontrollkästchen Instances beenden aktiviert. Um die Spot-Flotten-Anfrage zu storinieren, ohne die zugehörigen Instances zu beenden, deaktivieren Sie das Kontrollkästchen Instances beenden.

b. Wählen Sie Bestätigen aus.

AWS CLI

So können Sie eine Spot-Flottenanforderung abbrechen (löschen) und die zugehörigen Instances beenden

Verwenden Sie den Befehl cancel-spot-fleet-requests mit der Option `--terminate-instances`.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

Es folgt eine Beispielausgabe.

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_terminating",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

So können Sie eine Spot-Flottenanforderung abbrechen (löschen), ohne die zugehörigen Instances zu beenden

Ändern Sie das vorherige Beispiel, indem Sie stattdessen die Option `--no-terminate-instances` verwenden.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

Es folgt eine Beispielausgabe.

```
{
    "SuccessfulFleetRequests": [
```

```
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_running",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

PowerShell

So können Sie eine Spot-Flottenanforderung abbrechen (löschen) und die zugehörigen Instances beenden

Verwenden Sie das Stop-EC2SpotFleetRequestCmdlet mit dem `-TerminateInstance` Parameter.

```
Stop-EC2SpotFleetRequest `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TerminateInstance $true
```

So können Sie eine Spot-Flottenanforderung abbrechen (löschen), ohne die zugehörigen Instances zu beenden

Ändern Sie das vorherige Beispiel, indem Sie den Wert des Parameters `-TerminateInstance` ändern.

```
Stop-EC2SpotFleetRequest `
    -SpotFleetRequestId "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE" `
    -TerminateInstance $false
```

Automatische Skalierung für Spot-Flotten verstehen

Automatische Skalierung ermöglicht Ihrer Spot-Flotte die Zielkapazität automatisch abhängig von der Nachfrage zu erhöhen oder zu verringern. Bei der automatischen Skalierung kann eine Spot-Flotte als Reaktion auf eine oder mehrere Skalierungsrichtlinien innerhalb eines bestimmten Bereichs entweder Instances starten (aufskalieren) oder Instances beenden (abskalieren).

Die automatische Skalierung für Spot Fleet wird durch eine Kombination aus Amazon EC2 CloudWatch, Amazon und Application Auto Scaling ermöglicht APIs. Spot-Flottenanfragen werden

mit Amazon EC2, Alarme mit CloudWatch und Skalierungsrichtlinien mit Application Auto Scaling erstellt.

Typen der automatischen Skalierung

Die Spot-Flotte unterstützt die folgenden Typen automatischer Skalierung:

- Zielverfolgungsskalierung – Erhöht oder verringert die aktuelle Kapazität der Flotte anhand eines Zielwerts für eine bestimmte Metrik. Dies ähnelt der Art und Weise, wie Ihr Thermostat die Temperatur in Ihrem Zuhause konstant hält – Sie wählen eine Temperatur aus und das Thermostat erledigt den Rest.
- Step scaling (Schrittweise Skalierung) – Erhöht oder verringert die aktuelle Kapazität der Flotte anhand einer Gruppe von Skalierungsanpassungen, die als Schrittanpassungen bezeichnet werden und je nach Umfang der Alarmüberschreitung variieren.
- Scheduled scaling (Geplante Skalierung) – Erhöht oder verringert die aktuellen Kapazität der Flotte anhand von Datum und Uhrzeit.

Überlegungen

Überlegen Sie bei Verwendung der automatischen Skalierung für Ihre Spot-Flotte folgendes:

- Instance-Gewichtung – Wenn Sie Instance-Gewichtung verwenden, denken Sie daran, dass Spot-Flotten bei Bedarf die Zielkapazität überschreiten können. Die erfüllte Kapazität kann eine Gleitkommazahl sein, die Zielkapazität muss jedoch eine Ganzzahl sein, sodass die Spot-Flotte auf die nächste Ganzzahl aufgerundet wird. Sie müssen diese Verhalten berücksichtigen, wenn Sie sich das Ergebnis einer Skalierungsrichtlinie ansehen, wenn ein Alarm ausgelöst wird. Nehmen wir beispielsweise an, dass die Zielkapazität 30 und die erfüllte Kapazität 30,1 beträgt und die Skalierungsrichtlinie 1 abzieht. Wenn der Alarm ausgelöst wird, zieht der Auto Scaling-Prozess 1 von 30,1 ab und erhält 29,1. Dies wird auf 30 aufgerundet, sodass keine Skalierungsaktion erfolgt. Nehmen wir jetzt an, dass Sie Instance-Gewichtungen von 2, 4 und 8 sowie die Zielkapazität 10 ausgewählt haben, jedoch keine Instances mit der Gewichtung 2 verfügbar waren. Die Spot-Flotte hat so Instances mit den Gewichtungen 4 und 8 für eine erfüllte Kapazität von 12 bereitgestellt. Wenn die Skalierungsrichtlinie die Zielkapazität um 20 % verringert und ein Alarm ausgelöst wird, zieht der Auto Scaling-Prozess 12*0,2 von 12 ab und erhält 9,6. Dies wird auf 10 aufgerundet, sodass keine Skalierungsaktion erfolgt.
- Ruhephase – Die für die Spot-Flotte erstellten Skalierungsrichtlinien unterstützen eine Ruhephase. Dabei handelt es sich um die Anzahl an Sekunden, nachdem eine Skalierung abgeschlossen ist,

bei der sich vorherige Skalierungen basierend auf Auslösern auf zukünftige Skalierungsereignisse auswirken können. Bei Richtlinien für die Erweiterung wird während Ruhephasen die Kapazität, die durch das vorherige Skalierungsereignis hinzugefügt wurde, welches die Ruhephase initiiert hat, als Teil der gewünschten Kapazität für die nächste Erweiterung berechnet. Der Zweck ist eine kontinuierliche (jedoch nicht exzessive) Erweiterung. Bei Richtlinien für die Verkleinerung wird die Ruhephase verwendet, um nachfolgende Anforderungen für die Erweiterung zu sperren, bis sie abgelaufen ist. Der Zweck ist eine vorsichtige Verkleinerung, um die Verfügbarkeit Ihrer Anwendung zu schützen. Wenn während der Ruhephase nach einer Erweiterung jedoch ein anderer Alarm eine Verkleinerung auslöst, skaliert das Auto Scaling Ihr skalierbares Ziel sofort.

- Detailierte Überwachung nutzen – Wir empfehlen, Instance-Metriken in einem Intervall von 1 Minute zu skalieren, weil so eine schnellere Reaktion auf Änderungen an der Auslastung sichergestellt wird. Werden Metriken in einem Intervall von 5 Minuten skaliert, kann dies zu einer verringerten Reaktionszeit und zu einer Skalierung von veralteten Metrikdaten führen. Um Metrikdaten für Ihre Instance an CloudWatch in 1-Minuten-Intervallen zu senden, müssen Sie die detaillierte Überwachung aktivieren. Weitere Informationen erhalten Sie unter Verwalte die detaillierte Überwachung deiner EC2 Instances und Eine Spot-Flottenanforderung mit definierten Parametern erstellen.
- AWS CLI— Wenn Sie den für die Konfiguration der Skalierung AWS CLI für Spot Fleet verwenden, verwenden Sie die Befehle zur automatischen Skalierung von Anwendungen.

IAM-Berechtigungen für automatische Skalierung von Spot-Flotten

Die automatische Skalierung für Spot Fleet wird durch eine Kombination aus Amazon EC2 CloudWatch, Amazon und Application Auto Scaling ermöglicht APIs. Spot-Flottenanfragen werden mit Amazon EC2, Alarme mit CloudWatch und Skalierungsrichtlinien mit Application Auto Scaling erstellt. Zusätzlich zu den IAM-Berechtigungen, die für die Verwendung von Spot Fleet und Amazon erforderlich sind EC2, muss der Benutzer, der auf die Flottenskalierungseinstellungen zugreift, über die entsprechenden Berechtigungen für die Dienste verfügen, die automatische Skalierung unterstützen.

Um die automatische Skalierung für Spot-Flotte zu verwenden, müssen Benutzer auch die Berechtigung haben, die Aktionen in der folgenden Beispielrichtlinie zu verwenden.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:*",
                "ec2:DescribeSpotFleetRequests",
                "ec2:ModifySpotFleetRequest",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarmHistory",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DisableAlarmActions",
                "cloudwatch:EnableAlarmActions",
                "iam:CreateServiceLinkedRole",
                "sns:CreateTopic",
                "sns:Subscribe",
                "sns:Get*",
                "sns:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Sie können auch eigene IAM-Richtlinien erstellen, mit denen sich die Berechtigungen für Aufrufe der Application Auto Scaling-API präziser kontrollieren lassen. Weitere Informationen finden Sie unter Serviceverknüpfte Rollen für Application Auto Scaling im Benutzerhandbuch zum Application Auto Scaling.

Der Application Auto Scaling-Service benötigt außerdem die Erlaubnis, Ihre Spot-Flotte und CloudWatch Alarme zu beschreiben, sowie Berechtigungen, Ihre Spot-Flottenzielkapazität in Ihrem Namen zu ändern. Wenn Sie die automatische Skalierung für Ihre Spot-Flotte aktivieren, wird eine serviceverknüpfte Rolle namens `AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest` erstellt. Diese Service-verknüpfte Rolle gewährt Application Auto Scaling die Berechtigung zum Beschreiben der Alarme für die Richtlinien, zum Überwachen der aktuellen Kapazität der Flotte und zum Ändern der Kapazität der Flotte. Die ursprüngliche verwaltete Spot-Flotten-Rolle für Application Auto Scaling war

`aws-ec2-spot-fleet-autoscale-role`, diese wird jedoch nicht mehr benötigt. Die Service-verknüpfte Rolle ist die Standardrolle für Application Auto Scaling. Weitere Informationen finden Sie unter Serviceverknüpfte Rollen für Application Auto Scaling im Benutzerhandbuch zu Application Auto Scaling.

Skalierung der Zielverfolgung: Skalieren der Spot-Flotte, indem auf einen Wert für eine bestimmte Metrik abgezielt wird

Bei der Zielverfolgungsskalierung erstellen Sie eine Zielverfolgungsskalierungsrichtlinie, indem Sie eine Metrik auswählen und einen Zielwert festlegen. Spot Fleet erstellt und verwaltet dann die CloudWatch Alarme, die die Skalierungsrichtlinie auslösen, und berechnet die Skalierungsanpassung auf der Grundlage der ausgewählten Metrik und des Zielwerts. Die Skalierungsrichtlinie gleicht die Kapazität durch Hinzufügen oder Entfernen von Instances nach Bedarf an, um die Metrik auf oder nahe dem angegebenen Zielwert zu halten. Eine Zielverfolgungsskalierungsrichtlinie hält die Kennzahl nicht nur nahe am Zielwert, sondern sie passt sich auch den Schwankungen der Kennzahl aufgrund eines schwankenden Lastmusters an und minimiert schnelle Kapazitätsschwankungen.

Sie können für eine Spot-Flotte mehrere Zielverfolgungsskalierungsrichtlinie erstellen, sofern jede Richtlinie eine andere Metrik verwendet. Die Flotte skaliert basierend auf der Richtlinie, welche die größte Flotten-Kapazität bereitstellt. Dies ermöglicht Ihnen verschiedene Szenarien, um eine ausreichende Kapazität für Ihre Anwendungs-Workloads sicherzustellen.

Um die Verfügbarkeit der Anwendung sicherzustellen, wird die Flotte schnellstmöglich proportional zur Metrik hochskaliert, jedoch etwas langsamer herunterskaliert.

Wenn eine Spot-Flotte eine Instance aufgrund einer Verringerung der Zielkapazität beendet, erhält die Instance eine Benachrichtigung über die Unterbrechung einer Spot-Instance.

> **Note**
>
> Bearbeiten oder löschen Sie nicht die CloudWatch Alarme, die Spot Fleet für eine Skalierungsrichtlinie zur Zielverfolgung verwaltet. Die Spot-Flotte löscht die Alarme automatisch, wenn Sie die Skalierungsrichtlinie für die Zielverfolgung löschen.

Voraussetzungen

- Die Spot-Flottenanforderung muss den Anforderungstyp `maintain` aufweisen. Die automatische Skalierung wird für Anfragen vom Typ `request` nicht unterstützt.

- Konfigurieren Sie IAM-Berechtigungen für automatische Skalierung von Spot-Flotten.
- Überprüfen Sie das Überlegungen.

So konfigurieren Sie eine Richtlinie für die Ziel-Nachverfolgung

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus.
4. Wählen Sie die Registerkarte Auto Scaling am unteren Bildschirmrand. Wenn Sie den Link für Ihre Spot-Flotte ausgewählt haben, gibt es keine Registerkarte. Scrollen Sie stattdessen nach unten zum Abschnitt Auto Scaling.
5. Wenn Auto Scaling nicht konfiguriert ist, wählen Sie Configure aus.
6. Legen Sie anhand von Scale capacity between die Mindest- und Höchstkapazität für Ihre Flotte fest. Ihre Flotte wird durch Auto Scaling nicht auf einen Wert unter der Mindest- bzw. über der Höchstkapazität skaliert.
7. Geben Sie unter Policy Name (Richtlinienname) einen Namen für diese Richtlinie ein.
8. Wählen Sie eine Target metric.
9. Geben Sie einen Target value (Zielwert) für die Metrik ein.
10. Geben Sie für die Abklingzeit einen neuen Wert (in Sekunden) ein oder behalten Sie den Standardwert bei.
11. (Optional) Um die Erstellung einer Abskalierungsrichtlinie auf der Grundlage der aktuellen Konfiguration zu vermeiden, wählen Sie Abskalieren deaktivieren. Sie können eine Richtlinie für die horizontale Skalierung anhand einer anderen Konfiguration erstellen.
12. Wählen Sie Save aus.

Um eine Richtlinie zur Zielverfolgung mit dem zu konfigurieren AWS CLI

1. Registrieren Sie die Spot-Flotte-Anfrage mithilfe des register-scalable-targetBefehls als skalierbares Ziel.
2. Erstellen Sie mit dem put-scaling-policyBefehl eine Skalierungsrichtlinie.

Stufenweise Skalierung: Skalieren der Spot-Flotte anhand von Richtlinien zur stufenweisen Skalierung

Bei Richtlinien zur schrittweisen Skalierung geben Sie CloudWatch Alarme an, um den Skalierungsprozess auszulösen. Wenn Sie beispielsweise skalieren möchten, wenn die CPU-Auslastung ein bestimmtes Niveau erreicht, erstellen Sie anhand der von Amazon bereitgestellten `CPUUtilization` Metrik einen Alarm EC2.

Beim Erstellen einer Richtlinie zur schrittweisen Skalierung müssen Sie einen der folgenden Skalierungsanpassungstypen angeben:

- Add (Hinzufügen) – Erhöhen Sie die Zielkapazität der Flotte um eine angegebene Anzahl von Kapazitätseinheiten oder einen angegebenen Prozentsatz der aktuellen Kapazität.
- Remove (Entfernen) – Verringern Sie die Zielkapazität der Flotte um eine angegebene Anzahl von Kapazitätseinheiten oder einen angegebenen Prozentsatz der aktuellen Kapazität.
- Set to (Festlegen auf) – Legen Sie die Zielkapazität der Flotte auf die angegebene Anzahl an Kapazitätseinheiten fest.

Wenn ein Alarm ausgelöst wird, berechnet der Auto Scaling-Prozess die neue Zielkapazität anhand der erfüllten Kapazität und der Skalierungsrichtlinie und aktualisiert Sie Zielkapazität anschließend entsprechend. Nehmen wir beispielsweise an, dass die Zielkapazität und die erfüllte Kapazität 10 betragen und die Skalierungsrichtlinie 1 hinzufügt. Wenn der Alarm ausgelöst wird, fügt der Auto-Scaling-Prozess 1 bis 10 hinzu, um 11 zu erhalten. Die Spot-Flotte startet also 1 Instance.

Wenn eine Spot-Flotte eine Instance aufgrund einer Verringerung der Zielkapazität beendet, erhält die Instance eine Benachrichtigung über die Unterbrechung einer Spot-Instance.

Voraussetzungen

- Die Spot-Flottenanforderung muss den Anforderungstyp `maintain` aufweisen. Die automatische Skalierung wird für Anfragen vom Typ `request` nicht unterstützt.
- Konfigurieren Sie IAM-Berechtigungen für automatische Skalierung von Spot-Flotten.
- Überlegen Sie, welche CloudWatch Metriken für Ihre Anwendung wichtig sind. Sie können CloudWatch Alarme auf der Grundlage von Metriken AWS oder Ihrer eigenen benutzerdefinierten Metriken erstellen.

- Aktivieren Sie für die AWS Metriken, die Sie in Ihren Skalierungsrichtlinien verwenden werden, die Erfassung von CloudWatch Metriken, falls der Dienst, der die Metriken bereitstellt, sie nicht standardmäßig aktiviert.
- Überprüfen Sie das Überlegungen.

Um einen CloudWatch Alarm zu erstellen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Erweitern Sie im Navigationsbereich Alarme, dann Alle Alarme.
3. Wählen Sie Create Alarm (Alarm erstellen) aus.
4. Wählen Sie auf der Seite Specify metric and conditions (Metrik und Bedingungen angeben) die Option Select metric (Metrik auswählen) aus:
5. Wählen Sie EC2 Spot, dann Fleet Request Metrics und dann eine Metrik aus (z. B. TargetCapacity) und wählen Sie dann Metrik auswählen aus.

   Die Seite Specify metric and conditions (Metrik und Bedingungen festlegen) mit einem Diagramm und weiteren Informationen über die von Ihnen ausgewählte Metrik werden anzeigt.
6. Wählen Sie unter Zeitraum den Auswertungszeitraum für den Alarm aus, z. B. 1 Minute. Beim Auswerten des Alarms wird jeder Zeitraum in einem Datenpunkt zusammengefasst.

   > **Note**
   >
   > Ein kürzerer Zeitraum erzeugt eine höhere Alarmempfindlichkeit.
7. Legen Sie unter Conditions (Bedingungen) den Schwellenwert des Alarms fest. Sie können beispielsweise einen Schwellenwert angeben, damit der Alarm jedes Mal ausgelöst wird, wenn der Wert für die Metrik bei 80 Prozent oder höher liegt.
8. Geben Sie unter Additional configuration (Zusätzliche Konfiguration) für Datapoints to alarm (Datenpunkte bis zum Alarm) an, wie viele Datenpunkte (Auswertungszeiträume) sich im Alarmzustand befinden müssen, damit der Alarm ausgelöst wird, z. B. 1 Bewertungszeitraum oder 2 von 3 Bewertungszeiträumen. Dies erzeugt einen Alarm, der in den ALARM-Zustand übergeht, wenn viele aufeinander folgende Zeiträume überschritten werden. Weitere Informationen finden Sie unter Auswertung eines Alarms im CloudWatch Amazon-Benutzerhandbuch.
9. Wählen Sie für Missing data treatment (Behandlung fehlender Daten) eine der Optionen aus (oder belassen Sie es bei der Standardoption Treat missing data as missing (Fehlende Daten

als fehlend behandeln)). Weitere Informationen finden Sie unter Konfiguration der Behandlung fehlender Daten durch CloudWatch Alarme im CloudWatch Amazon-Benutzerhandbuch.

10. Wählen Sie Next.
11. (Optional) Um eine Benachrichtigung zu einem Skalierungsereignis zu empfangen, können Sie für Notification (Benachrichtigung) das Amazon SNS-Thema auswählen oder erstellen, das zum Empfangen der Benachrichtigungen verwendet werden soll. Andernfalls können Sie die Benachrichtigung jetzt löschen und bei Bedarf später eine hinzufügen.
12. Wählen Sie Next.
13. Geben Sie unter Hinzufügen einer Beschreibung einen Namen und eine Beschreibung für den Alarm ein und klicken Sie auf Weiter.
14. Wählen Sie Alarm erstellen aus.

So konfigurieren Sie die Richtlinie für schrittweise Skalierung für Ihre Spot-Flotte

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus.
4. Wählen Sie die Registerkarte Auto Scaling am unteren Bildschirmrand. Wenn Sie den Link für Ihre Spot-Flotte ausgewählt haben, gibt es keine Registerkarte. Scrollen Sie stattdessen nach unten zum Abschnitt Auto Scaling.
5. Wenn Auto Scaling nicht konfiguriert ist, wählen Sie Configure aus.
6. Legen Sie anhand von Scale capacity between die Mindest- und Höchstkapazität für Ihre Flotte fest. Die Skalierungsrichtlinien lassen Ihre Flotte nicht unter die Mindestkapazität oder über die maximale Kapazität hinaus skalieren.
7. Wählen Sie für Skalierungsrichtlinien, Richtlinientyp Stufenskalierungsrichtlinie aus.
8. Zunächst enthalten Skalierungsrichtlinien Richtlinien für die schrittweise Skalierung mit den Namen ScaleUp und ScaleDown. Sie können diese Richtlinien abschließen oder sie mit Remove policy entfernen. Sie können außerdem Add policy (Richtlinie hinzufügen) auswählen.
9. Gehen Sie wie folgt vor, um eine Richtlinie zu definieren:

    a. Geben Sie unter Policy Name (Richtlinienname) einen Namen für diese Richtlinie ein.

    b. Wählen Sie für Policy trigger einen vorhandenen Alarm aus oder wählen Sie Alarm erstellen, um die CloudWatch Amazon-Konsole zu öffnen und einen Alarm zu erstellen.

c. Definieren Sie für Kapazität ändernden Betrag, um den skaliert werden soll, sowie die untere und obere Grenze der Schrittanpassung. Sie können eine bestimmte Anzahl von Instances oder einen Prozentsatz der bestehenden Flottengröße hinzufügen oder entfernen oder die Flotte auf eine exakte Größe festlegen.

   Um beispielsweise eine Richtlinie zur schrittweisen Skalierung zu erstellen, welche die Kapazität der Flotte um 30 Prozent erhöht, wählen Sie Hinzufügen, geben Sie 30 in das nächste Feld ein, und wählen Sie dann Prozent. Standardmäßig ist die untere Grenze für eine Hinzufügerichtlinie die Alarmschwelle und die obere Grenze ist positiv (+) unendlich. Standardmäßig ist die obere Grenze für eine Entfernerichtlinie die Alarmschwelle und die untere Grenze ist negativ (-) unendlich.

d. (Optional) Um einen weiteren Schritt hinzuzufügen, wählen Sie Schritt hinzufügen.

e. Geben Sie für die Abklingzeit einen neuen Wert (in Sekunden) ein oder behalten Sie den Standardwert bei.

10. Wählen Sie Speichern.

Um Richtlinien für die schrittweise Skalierung für Ihre Spot-Flotte zu konfigurieren, verwenden Sie AWS CLI

1. Registrieren Sie die Spot-Flotte-Anfrage mithilfe des register-scalable-targetBefehls als skalierbares Ziel.
2. Erstellen Sie mit dem put-scaling-policyBefehl eine Skalierungsrichtlinie.
3. Erstellen Sie mit dem put-metric-alarmBefehl einen Alarm, der die Skalierungsrichtlinie auslöst.

Geplante Skalierung: Spot-Flotte nach einem Zeitplan skalieren

Eine Skalierung Ihrer Flotte anhand eines Zeitplans ermöglicht es Ihnen, Ihre Anwendung entsprechend vorhersagbarer Anforderungsänderungen zu skalieren. Durch Erstellen von geplanten Aktionen können Sie die Spot-Flotte anweisen, Skalierungen zu bestimmten Zeitpunkten durchzuführen. Wenn Sie eine geplante Aktion erstellen, geben Sie eine vorhandene Spot-Flotte und die minimale und maximale Kapazität sowie den Zeitpunkt an, an dem die Skalierung durchgeführt werden soll. Geplante Aktionen können so konfiguriert werden, dass sie einmalig oder nach einem wiederkehrenden Zeitplan skalieren. Wenn Sie Änderungen benötigen, können Sie geplante Aktionen bearbeiten oder löschen.

Voraussetzungen

- Geplante Aktionen können nur für bestehende Spot-Flotten erstellt werden. Sie können keine geplante Aktion erstellen, während Sie eine Spot-Flotte erstellen.
- Die Spot-Flottenanforderung muss den Anforderungstyp `maintain` aufweisen. Die automatische Skalierung wird für Anfragen vom Typ `request` nicht unterstützt.
- Konfigurieren Sie IAM-Berechtigungen für automatische Skalierung von Spot-Flotten.
- Überprüfen Sie das Überlegungen.

Erstellen Sie eine einmalige geplante Aktion wie folgt:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus.
4. Wählen Sie die Registerkarte Geplante Skalierung am unteren Bildschirmrand. Wenn Sie den Link für Ihre Spot-Flotte ausgewählt haben, gibt es keine Registerkarte. Scrollen Sie stattdessen nach unten zum Abschnitt Geplante Skalierung.
5. Wählen Sie Geplante Aktion erstellen.
6. Geben Sie unter Name einen neuen Namen für die geplante Aktion ein.
7. Geben Sie einen Wert für Minimum capacity (Minimale Kapazität), Maximum capacity (Maximale Kapazität) oder beides ein.
8. Wählen Sie für Recurrence (Wiederholung) Once (Einmal) aus.
9. (Optional) Wählen Sie ein Datum und eine Uhrzeit für Start time (Startzeit), End time (Endzeit) oder beides.
10. Wählen Sie Erstellen aus.

Einen sich wiederholenden Zeitplan erstellen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus.
4. Wählen Sie die Registerkarte Geplante Skalierung am unteren Bildschirmrand. Wenn Sie den Link für Ihre Spot-Flotte ausgewählt haben, gibt es keine Registerkarte. Scrollen Sie stattdessen nach unten zum Abschnitt Geplante Skalierung.

5. Geben Sie unter Name einen neuen Namen für die geplante Aktion ein.
6. Geben Sie einen Wert für Minimum capacity (Minimale Kapazität), Maximum capacity (Maximale Kapazität) oder beides ein.
7. Wählen Sie für Recurrence (Wiederholung) einen der vordefinierten Zeitpläne (z. B. Every day (Jeden Tag)) oder wählen Sie Custom (Benutzerdefiniert) und geben Sie einen Cron-Ausdruck ein. Weitere Informationen zu den Cron-Ausdrücken, die von der geplanten Skalierung unterstützt werden, finden Sie unter Cron-Ausdrücke im EventBridge Amazon-Benutzerhandbuch.
8. (Optional) Wählen Sie ein Datum und eine Uhrzeit für Start time (Startzeit), End time (Endzeit) oder beides.
9. Klicken Sie auf Submit (Absenden).

So bearbeiten Sie eine geplante Aktion

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus.
4. Wählen Sie die Registerkarte Geplante Skalierung am unteren Bildschirmrand. Wenn Sie den Link für Ihre Spot-Flotte ausgewählt haben, gibt es keine Registerkarte. Scrollen Sie stattdessen nach unten zum Abschnitt Geplante Skalierung.
5. Wählen Sie die geplante Aktion dann Actions (Aktionen) und anschließend Edit (Bearbeiten) aus.
6. Nehmen Sie die notwendigen Änderungen vor und klicken Sie auf Submit (Senden).

So löschen Sie eine geplante Aktion

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus.
4. Wählen Sie die Registerkarte Geplante Skalierung am unteren Bildschirmrand. Wenn Sie den Link für Ihre Spot-Flotte ausgewählt haben, gibt es keine Registerkarte. Scrollen Sie stattdessen nach unten zum Abschnitt Geplante Skalierung.
5. Wählen Sie die geplante Aktion dann Actions (Aktionen) und anschließend Delete (Löschen) aus.
6. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

Um die geplante Skalierung mit dem zu verwalten AWS CLI

Verwenden Sie die folgenden Befehle:

- put-scheduled-action
- describe-scheduled-actions
- delete-scheduled-action

Überwachen Sie Ihre EC2 Flotte oder Spot-Flotte

Eine effektive Überwachung Ihrer EC2 Flotte oder Spot-Flotte ist unerlässlich, um eine optimale Leistung aufrechtzuerhalten und die Zuverlässigkeit zu gewährleisten. Es gibt verschiedene Tools, die Ihnen dabei helfen, dies zu erreichen, darunter Amazon CloudWatch und Amazon EventBridge, die in diesem Thema behandelt werden.

Damit CloudWatch können Sie Kennzahlen sammeln und verfolgen, Alarme einrichten und automatisch auf Änderungen im Status Ihrer Flotte reagieren.

Mit können Sie Ereignisse EventBridge, die von Ihrer Flotte ausgelöst werden, überwachen und programmgesteuert darauf reagieren. Durch die Definition von Regeln in EventBridge können Sie die Reaktionen auf bestimmte Flottenereignisse, wie z. B. das Beenden von Instances oder Änderungen des Flottenstatus, automatisieren und so Ihre betriebliche Effizienz verbessern.

Themen

- Überwachen Sie Ihre EC2 Flotte oder Spot-Flotte mit CloudWatch
- Überwachen Sie mithilfe von Amazon die Ereignisse, die von Ihrer EC2 Flotte oder Spot-Flotte ausgelöst werden, und reagieren Sie programmgesteuert darauf EventBridge

Überwachen Sie Ihre EC2 Flotte oder Spot-Flotte mit CloudWatch

Sie können Ihre EC2 Flotte oder Spot-Flotte anhand der in diesem Abschnitt beschriebenen CloudWatch Amazon-Metriken überwachen.

> **Important**
>
> Um die Genauigkeit zu gewährleisten, empfehlen wir, beim Verwenden dieser Metriken die detaillierte Überwachung zu aktivieren. Weitere Informationen finden Sie unter Verwalte die detaillierte Überwachung deiner EC2 Instances.

Weitere Informationen zur Verwendung finden CloudWatch Sie unterÜberwachen Sie Ihre Instances mit CloudWatch.

EC2 Metriken für Flotte und Spot-Flotte

Der `AWS/EC2Spot` Namespace umfasst die folgenden Metriken für Ihre Flotte sowie die CloudWatch Metriken für die Spot-Instances in Ihrer Flotte. Weitere Informationen finden Sie unter Instance-Metriken.

Metrik	Description
`AvailableInstancePoolsCount`	Die Spot-Kapazitätspools, die in der Flotten-Anforderung angegeben wurden. Einheiten: Anzahl
`BidsSubmittedForCapacity`	Die Kapazität, für die Amazon Flottenanfragen eingereicht EC2 hat. Einheiten: Anzahl
`EligibleInstancePoolCount`	Die in der Flottenanfrage angegebenen Spot-Kapazitätspools, in denen Amazon Anfragen bearbeiten EC2 kann. Amazon erfüllt EC2 keine Anfragen in Pools, in denen der Höchstpreis, den Sie bereit sind, für Spot-Instances zu zahlen, unter dem Spot-Preis liegt oder der Spot-Preis über dem Preis für On-Demand-Instances liegt. Einheiten: Anzahl
`FulfilledCapacity`	Die Kapazität, die Amazon erfüllt EC2 hat.

Metrik	Description
	Einheiten: Anzahl
`MaxPercentCapacityAllocation`	Der Höchstwert von `PercentCapacityAllocation` über alle Flotten-Pools hinweg, die in der Flotten-Anforderung angegeben wurden. Einheiten: Prozent
`PendingCapacity`	Differenz zwischen `TargetCapacity` und `FulfilledCapacity` . Einheiten: Anzahl
`PercentCapacityAllocation`	Dem Spot-Kapazitätspool für die angegebenen Dimensionen zugeordnete Kapazität. Der höchste registriert Wert aller Spot-Kapazitätspools kann mit `MaxPercentCapacityAllocation` ermittelt werden. Einheiten: Prozent
`TargetCapacity`	Die Zielkapazität der Flotten-Anforderung. Einheiten: Anzahl
`TerminatingCapacity`	Die Kapazität, die beendet wird, da die bereitgestellte Kapazität größer als die Zielkapazität ist. Einheiten: Anzahl

Wenn die Maßeinheit einer Metrik `Count` ist, lautet die nützlichste Statistik `Average`.

EC2 Abmessungen der Flotte und der Spot-Flotte

Verwenden Sie die folgenden Dimensionen, um die Daten für Ihre Flotte zu filtern.

Dimensionen	Beschreibung
`AvailabilityZone`	Filtern Sie die Daten nach Availability Zone.

Dimensionen	Beschreibung
`FleetRequestId`	Filtern Sie die Daten nach Flottenanfrage.
`InstanceType`	Filtern Sie die Daten nach Instance-Typ.

Sehen Sie sich die CloudWatch Kennzahlen für Ihre EC2 Flotte oder Spot-Flotte an

Sie können die CloudWatch Kennzahlen für Ihre Flotte in der CloudWatch Amazon-Konsole einsehen. Diese Metriken werden in Überwachungsdiagrammen dargestellt. Diese Grafiken zeigen Datenpunkte, wenn die Flotte aktiv ist.

Metriken werden zuerst nach dem Namespace und dann nach den verschiedenen Kombinationen von Dimensionen in jedem Namespace gruppiert. Sie können beispielsweise alle Flotten-Metriken oder Gruppen von Flotten-Metriken nach Flotten-Anforderungs-ID, Instance-Typ oder Availability Zone anzeigen.

Flottenmetriken anzeigen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Erweitern Sie im Navigationsbereich Metriken und wählen Sie dann Alle Metriken aus.
3. Wählen Sie den EC2 Spot-Namespace.

   > **Note**
   >
   > Wenn der EC2 Spot-Namespace nicht angezeigt wird, gibt es dafür zwei Gründe. Entweder haben Sie EC2 Fleet oder Spot Fleet in der Region noch nie genutzt — nur die AWS Dienste, die Sie nutzen, senden Messwerte an Amazon. CloudWatch Oder, wenn Sie EC2 Fleet oder Spot Fleet in der Region verwendet haben, aber nicht in den letzten zwei Wochen, wird der Namespace nicht angezeigt.

4. (Um die Metriken nach Dimensionen zu filtern, wählen Sie einen der folgenden Schritte aus:

   - Flottenanforderungsmetriken – Gruppieren nach Spot-Flotten-Anforderung
   - Nach Availability Zone – Gruppieren nach Spot-Flotten-Anforderung und Availability Zone
   - Nach Instance-Typ – Gruppieren nach Spot-Flotten-Anforderung und Instance-Typ

- Nach Zone/Instance Verfügbarkeitstyp — Gruppieren Sie nach Flottenanfrage, Availability Zone und Instance-Typ

5. Um die Daten für eine Metrik anzuzeigen, aktivieren Sie das Kontrollkästchen neben der Metrik.

Überwachen Sie mithilfe von Amazon die Ereignisse, die von Ihrer EC2 Flotte oder Spot-Flotte ausgelöst werden, und reagieren Sie programmgesteuert darauf EventBridge

Wenn sich der Status einer EC2 Flotte oder Spot-Flotte ändert, wird eine Benachrichtigung ausgegeben. Die Benachrichtigung wird als Ereignis zur Verfügung gestellt, das an Amazon gesendet wird EventBridge (früher bekannt als Amazon CloudWatch Events). Ereignisse werden auf bestmögliche Weise ausgegeben.

Sie können Amazon verwenden EventBridge , um Regeln zu erstellen, die als Reaktion auf ein Ereignis programmatische Aktionen auslösen. Sie können beispielsweise zwei EventBridge Regeln erstellen: eine wird ausgelöst, wenn sich der Status einer Flotte ändert, und eine weitere, wenn eine Instance in der Flotte beendet wird. Sie können in diesem Beispiel die erste Regel so konfigurieren, dass bei einer Änderung des Flottenstatus die Regel ein SNS-Thema aufruft, um Ihnen eine E-Mail-Benachrichtigung zu senden. Sie können die zweite Regel so konfigurieren, dass beim Beenden einer Instance in der Flotte die Regel eine Lambda-Funktion aufruft, um eine neue Instance zu starten.

> **Note**
>
> Nur Flotten vom Typ `maintain` und `request` emittieren Ereignisse. Flotten des Typs `instant` geben keine Ereignisse aus, da sie synchrone einmalige Anfragen senden und der Zustand der Flotte in der Antwort sofort bekannt ist. Um Amazon EventBridge zur Überwachung von Flottenereignissen verwenden zu können, muss der Anfragetyp `maintain` oder sein`request`.

Anweisungen zum Beschreiben des Ereignisverlaufs einer Flotte finden Sie unter Beschreiben Sie den Ereignisverlauf für Ihre EC2 Flotte.

Themen

- Erstellen Sie EventBridge Amazon-Regeln zur Überwachung von EC2 Fleet- oder Spot-Flottenereignissen
- EC2 Arten von Flottenereignissen
- Ereignistypen für Spot-Flotten

Erstellen Sie EventBridge Amazon-Regeln zur Überwachung von EC2 Fleet- oder Spot-Flottenereignissen

Wenn eine Statusänderungsbenachrichtigung für eine EC2 Flotte oder Spot-Flotte ausgegeben wird, wird sie als Ereignis EventBridge als JSON-Datei an Amazon gesendet. Wenn ein Ereignismuster EventBridge erkannt wird, das einem in einer Regel definierten Muster entspricht, EventBridge ruft es das in der Regel angegebene Ziel (oder die Ziele) auf.

Sie können EventBridge Regeln schreiben, um Aktionen auf der Grundlage übereinstimmender Ereignismuster zu automatisieren.

Die folgenden Felder des Ereignisses bilden das Ereignismuster, das eine Aktion aufruft:

`"source": "aws.ec2fleet"`

Identifiziert, dass das Ereignis von EC2 Fleet stammt.

`"detail-type": "EC2 Fleet State Change"`

Identifiziert den Ereignistyp.

`"detail": { "sub-type": "submitted" }`

Identifiziert den Ereignis-Sub-Typ.

Eine Liste der EC2 Fleet- und Spot-Flottenereignisse sowie Beispielereignisdaten finden Sie unter EC2 Arten von Flottenereignissen undEreignistypen für Spot-Flotten.

Beispiele

- Erstellen Sie eine EventBridge Regel zum Senden einer Benachrichtigung
- Erstellen Sie eine EventBridge Regel zum Auslösen einer Lambda-Funktion

Erstellen Sie eine EventBridge Regel zum Senden einer Benachrichtigung

Im folgenden Beispiel wird eine EventBridge Regel erstellt, nach der jedes Mal, wenn Amazon eine Benachrichtigung über eine Änderung des EC2 Flottenstatus EC2 ausgibt, eine E-Mail, eine Textnachricht oder eine mobile Push-Benachrichtigung sendet. Das Signal in diesem Beispiel wird als `EC2 Fleet State Change`-Ereignis ausgegeben, das die durch die Regel definierte Aktion auslöst.

Voraussetzung

Bevor Sie die EventBridge Regel erstellen, müssen Sie das Amazon SNS SNS-Thema für die E-Mail, Textnachricht oder mobile Push-Benachrichtigung erstellen.

Um eine EventBridge Regel zum Senden einer Benachrichtigung zu erstellen, wenn sich der Status einer EC2 Flotte ändert

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie Regel erstellen aus.
3. Zum Define rule detail (Festlegen der Regeldetails) gehen Sie folgendermaßen vor:
   a. Geben Sie für die Regel einen Name (Namen) und optional eine Beschreibung ein.

      Eine Regel darf nicht denselben Namen wie eine andere Regel in derselben Region und auf demselben Event Bus haben.
   b. Bei Event bus (Ereignisbus) wählen Sie default (Standard) aus. Wenn ein AWS Service in Ihrem Konto ein Ereignis generiert, wird es immer an den Standard-Event-Bus Ihres Kontos weitergeleitet.
   c. Bei Regeltyp wählen Sie Regel mit einem Ereignismuster aus.
   d. Wählen Sie Weiter aus.
4. Bei Build event pattern (Ereignis-Muster erstellen) gehen Sie wie folgt vor:
   a. Wählen Sie als Eventquelle AWS Events oder EventBridge Partnerevents aus.
   b. Bei Event pattern (Ereignismuster) in diesem Beispiel geben Sie das folgende Ereignismuster an, um mit dem `EC2 Fleet Instance Change`-Ereignis übereinzustimmen.

```
{
 "source": ["aws.ec2fleet"],
 "detail-type": ["EC2 Fleet Instance Change"]
```

```
}
```

Um das Ereignismuster hinzuzufügen, können Sie entweder eine Vorlage verwenden, indem Sie Event pattern form (Ereignismusterformular) auswählen oder Sie spezifizieren Ihr eigenes Muster, indem Sie Custom pattern (JSON-Editor) (Benutzerdefiniertes Muster (JSON-Editor)) auswählen, siehe nachfolgend:

i. Gehen Sie wie folgt vor, um eine Vorlage zum Erstellen des Ereignismusters zu erstellen:

A. Wählen Sie Event pattern form (Ereignismusterformular) aus.

B. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.

C. Wählen Sie für AWS Service die Option EC2 Fleet aus.

D. Wählen Sie als Ereignistyp die Option EC2 Fleet Instance Change aus.

E. Um die Vorlage anzupassen, wählen Sie Edit pattern (Muster bearbeiten) und nehmen Sie Ihre Änderungen vor, damit sie dem Beispiel-Ereignismuster entsprechen.

ii. (Alternativ) So geben Sie ein benutzerdefiniertes Ereignismuster an:

A. Wählen Sie Custom pattern (JSON editor) (Benutzerdefiniertes Muster (JSON-Editor)) aus.

B. In dem Feld Event pattern (Ereignismuster) fügen Sie das Ereignismuster für dieses Beispiel hinzu.

c. Wählen Sie Weiter aus.

5. Bei Select target(s) (Ziel(e) auswählen) gehen Sie wie folgt vor:

a. Bei Target types (Zieltypen) wählen Sie AWS -Service aus.

b. Bei Select a target (Ziel auswählen) wählen Sie SNS topic (SNS-Thema) aus, um eine E-Mail, eine SMS oder eine mobile Push-Benachrichtigung zu senden, wenn das Ereignis eintritt.

c. Wählen Sie für Topic (Thema) ein vorhandenes Thema aus. Sie müssen zuerst mit der Amazon-SNS-Konsole ein Amazon-SNS-Thema erstellen. Weitere Informationen finden Sie unter Verwenden von Amazon SNS für application-to-person (A2P) -Messaging im Amazon Simple Notification Service Developer Guide.

d. (Optional) Unter Additional settings (Zusätzliche Einstellungen) können Sie optional zusätzliche Einstellungen konfigurieren. Weitere Informationen finden Sie im EventBridge

Amazon-Benutzerhandbuch unter EventBridge Amazon-Regeln erstellen, die auf Ereignisse reagieren (Schritt 16).

e. Wählen Sie Weiter aus.

6. (Optional) Bei Tags können Sie Ihrer Regel optional einen Tag oder mehrere Tags hinzufügen und dann Next (Weiter) auswählen.
7. Bei Review and create (Überprüfen und erstellen) gehen Sie wie folgt vor:

   a. Überprüfen Sie die Details der Regel und ändern Sie sie nach Bedarf.

   b. Wählen Sie Regel erstellen aus.

Weitere Informationen finden Sie unter EventBridge Amazon-Regeln und EventBridge Amazon-Ereignismuster im EventBridge Amazon-Benutzerhandbuch.

Erstellen Sie eine EventBridge Regel zum Auslösen einer Lambda-Funktion

Im folgenden Beispiel wird eine EventBridge Regel erstellt, die jedes Mal eine Lambda-Funktion auslöst, wenn Amazon EC2 beim Start einer Instance eine EC2 Fleet-Instance-Änderungsbenachrichtigung ausgibt. Das Signal in diesem Beispiel wird als `EC2 Fleet Instance Change`-Ereignis, Sub-Typ `launched`, ausgegeben, das die durch die Regel definierte Aktion auslöst.

Bevor Sie die EventBridge Regel erstellen, müssen Sie die Lambda-Funktion erstellen.

Um die Lambda-Funktion zu erstellen, die in der EventBridge Regel verwendet werden soll

1. Öffnen Sie die AWS Lambda Konsole unter. https://console.aws.amazon.com/lambda/
2. Wählen Sie Create function (Funktion erstellen).
3. Geben Sie einen Namen für Ihre Funktion ein, konfigurieren Sie den Code und wählen Sie dann Create function (Funktion erstellen).

   Weitere Informationen finden Sie unter Erstellen Ihrer ersten Lambda-Funktion im Entwicklerhandbuch für AWS Lambda .

Um eine EventBridge Regel zum Auslösen einer Lambda-Funktion zu erstellen, wenn sich der Status einer Instanz in einer EC2 Flotte ändert

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.

2. Wählen Sie Regel erstellen aus.
3. Zum Define rule detail (Festlegen der Regeldetails) gehen Sie folgendermaßen vor:

   a. Geben Sie für die Regel einen Name (Namen) und optional eine Beschreibung ein.

      Eine Regel darf nicht denselben Namen wie eine andere Regel in derselben Region und auf demselben Event Bus haben.

   b. Bei Event bus (Ereignisbus) wählen Sie default (Standard) aus. Wenn ein AWS Service in Ihrem Konto ein Ereignis generiert, wird es immer an den Standard-Event-Bus Ihres Kontos weitergeleitet.

   c. Bei Regeltyp wählen Sie Regel mit einem Ereignismuster aus.

   d. Wählen Sie Weiter aus.
4. Bei Build event pattern (Ereignis-Muster erstellen) gehen Sie wie folgt vor:

   a. Wählen Sie als Eventquelle AWS Events oder EventBridge Partnerevents aus.

   b. Für Event pattern (Ereignismuster) in diesem Beispiel geben Sie das folgende Ereignismuster an, das dem `EC2 Fleet Instance Change`-Ereignis und `launched`-Subtyp übereinstimmt.

      ```
      {
       "source": ["aws.ec2fleet"],
       "detail-type": ["EC2 Fleet Instance Change"],
       "detail": {
         "sub-type": ["launched"]
      }
      ```

      Um das Ereignismuster hinzuzufügen, können Sie entweder eine Vorlage verwenden, indem Sie Event pattern form (Ereignismusterformular) auswählen oder Sie spezifizieren Ihr eigenes Muster, indem Sie Custom pattern (JSON-Editor) (Benutzerdefiniertes Muster (JSON-Editor)) auswählen, siehe nachfolgend:

      i. Gehen Sie wie folgt vor, um eine Vorlage zum Erstellen des Ereignismusters zu erstellen:

         A. Wählen Sie Event pattern form (Ereignismusterformular) aus.

         B. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.

         C. Wählen Sie für AWS Service die Option EC2 Fleet aus.

D. Wählen Sie als Ereignistyp die Option EC2 Fleet Instance Change aus.

E. Wählen Sie Edit pattern (Muster bearbeiten) aus und fügen Sie `"detail": {"sub-type": ["launched"]` hinzu, um dem Beispiel-Ereignismuster zu entsprechen. Fügen Sie für das richtige JSON-Format ein Komma (`,`) nach der vorhergehenden eckigen Klammer (`]`) ein.

ii. (Alternativ) So geben Sie ein benutzerdefiniertes Ereignismuster an:

A. Wählen Sie Custom pattern (JSON editor) (Benutzerdefiniertes Muster (JSON-Editor)) aus.

B. In dem Feld Event pattern (Ereignismuster) fügen Sie das Ereignismuster für dieses Beispiel hinzu.

c. Wählen Sie Weiter aus.

5. Bei Select target(s) (Ziel(e) auswählen) gehen Sie wie folgt vor:

a. Bei Target types (Zieltypen) wählen Sie AWS -Service aus.

b. Bei Select a target (Ziel auswählen) wählen Sie SNS topic (SNS-Thema) aus, um eine E-Mail, eine SMS oder eine mobile Push-Benachrichtigung zu senden, wenn das Ereignis eintritt.

c. Wählen Sie für Topic (Thema) Lambda function (Lambda-Funktion) und für Function (Funktion) die Funktion, die Sie erstellt haben, um beim Auftreten des Ereignisses zu reagieren.

d. (Optional) Unter Additional settings (Zusätzliche Einstellungen) können Sie optional zusätzliche Einstellungen konfigurieren. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch unter EventBridge Amazon-Regeln erstellen, die auf Ereignisse reagieren (Schritt 16).

e. Wählen Sie Weiter aus.

6. (Optional) Bei Tags können Sie Ihrer Regel optional einen Tag oder mehrere Tags hinzufügen und dann Next (Weiter) auswählen.

7. Bei Review and create (Überprüfen und erstellen) gehen Sie wie folgt vor:

a. Überprüfen Sie die Details der Regel und ändern Sie sie nach Bedarf.

b. Wählen Sie Regel erstellen aus.

Ein Tutorial zum Erstellen einer Lambda-Funktion und einer EventBridge Regel, die die Lambda-Funktion ausführt, finden Sie unter Tutorial: Log the State of an Amazon EC2 Instance Using EventBridge im AWS Lambda Developer Guide.

EC2 Arten von Flottenereignissen

Es gibt fünf EC2 Flotten-Ereignistypen. Für jeden Ereignistyp gibt es mehrere Sub-Typen.

Event types (Ereignistypen)

- EC2 Änderung des Flottenstatus
- EC2 Änderung der Fleet Spot-Instance-Anfrage
- EC2 Änderung der Flotteninstanz
- EC2 Informationen zur Flotte
- EC2 Flottenfehler

EC2 Änderung des Flottenstatus

EC2 Fleet sendet ein `EC2 Fleet State Change` Ereignis an Amazon, EventBridge wenn sich der Status einer EC2 Flotte ändert.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "715ed6b3-b8fc-27fe-fad6-528c7b8bf8a2",
    "detail-type": "EC2 Fleet State Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:20Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "sub-type": "active"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`active`

Die EC2 Flottenanfrage wurde validiert und Amazon EC2 versucht, die angestrebte Anzahl laufender Instances beizubehalten.

`deleted`

Die EC2 Flottenanfrage wurde gelöscht und hat keine laufenden Instances. Die EC2 Flotte wird zwei Tage nach Beendigung ihrer Instances gelöscht.

`deleted_running`

Die EC2 Flottenanfrage wird gelöscht und startet keine weiteren Instances. Die bestehenden Instances laufen weiter, bis sie unterbrochen oder beendet werden. Die Anforderung bleibt so lange in diesem Zustand, bis alle Instances unterbrochen oder beendet wurden.

`deleted_terminating`

Die EC2 Flottenanfrage wird gelöscht und die zugehörigen Instanzen werden beendet. Die Anforderung bleibt so lange in diesem Zustand, bis alle Instances beendet wurden.

`expired`

Die EC2 Flottenanfrage ist abgelaufen. Wenn die Anforderung mit `TerminateInstancesWithExpiration` erstellt wurde, zeigt ein nachfolgendes `terminated`-Ereignis an, dass die Instances beendet werden.

`modify_in_progress`

Die EC2 Flottenanfrage wird geändert. Die Anforderung bleibt in diesem Zustand, bis die Änderung vollständig verarbeitet wurde.

`modify_succeeded`

Die EC2 Flottenanfrage wurde geändert.

`submitted`

Die EC2 Flottenanfrage wird geprüft und Amazon bereitet EC2 sich darauf vor, die angestrebte Anzahl von Instances zu starten.

`progress`

Die EC2 Flottenanfrage wird gerade bearbeitet.

EC2 Änderung der Fleet Spot-Instance-Anfrage

EC2 Fleet sendet ein `EC2 Fleet Spot Instance Request Change` Ereignis an Amazon, EventBridge wenn sich der Status einer Spot-Instance-Anfrage in der Flotte ändert.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "19331f74-bf4b-a3dd-0f1b-ddb1422032b9",
    "detail-type": "EC2 Fleet Spot Instance Request Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:05Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/
fleet-83fd4e48-552a-40ef-9532-82a3acca5f10"
    ],
    "detail": {
        "spot-instance-request-id": "sir-rmqske6h",
        "description": "SpotInstanceRequestId sir-rmqske6h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`active`

Die Spot-Instance-Anforderung wurde erfüllt und ist mit einer Spot-Instance verknüpft.

`cancelled`

Sie haben die Spot-Instance-Anforderung storniert oder die Spot-Instance-Anforderung ist abgelaufen.

`disabled`

Sie haben die Spot-Instance angehalten.

`submitted`

Die Spot-Instance-Anforderung wird gesendet.

EC2 Änderung der Flotteninstanz

EC2 Fleet sendet ein `EC2 Fleet Instance Change` Ereignis an Amazon, EventBridge wenn sich der Status einer Instance in der Flotte ändert.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "542ce428-c8f1-0608-c015-e8ed6522c5bc",
    "detail-type": "EC2 Fleet Instance Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:23Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "instance-id": "i-0c594155dd5ff1829",
        "description": "{\"instanceType\":\"c5.large\",\"image\":\"ami-6057e21a\",
\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":\"us-east-1d\"}",
        "sub-type": "launched"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`launched`

Eine neue Instance wurde gestartet.

`terminated`

Die Instance wurde beendet.

`termination_notified`

Eine Benachrichtigung zur Instance-Kündigung wurde gesendet, wenn eine Spot-Instance von Amazon EC2 während des Scale-Down beendet wurde, als die Zielkapazität der Flotte heruntergefahren wurde, beispielsweise von einer Zielkapazität von 4 auf eine Zielkapazität von 3.

EC2 Informationen zur Flotte

EC2 Fleet sendet ein `EC2 Fleet Information` Ereignis an Amazon EventBridge , wenn beim Versand ein Fehler auftritt. Das Informationsereignis hindert die Flotte nicht daran, ihre Zielkapazität zu erreichen.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "76529817-d605-4571-7224-d36cc1b2c0c4",
    "detail-type": "EC2 Fleet Information",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T08:17:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-8becf5fe-
bb9e-415d-8f54-3fa5a8628b91"
    ],
    "detail": {
        "description": "c4.xlarge, ami-0947d2ba12ee1ff75, Linux/UNIX, us-east-1a,
 Spot price in either SpotFleetRequestConfigData or SpotFleetLaunchSpecification or
 LaunchTemplate or LaunchTemplateOverrides is less than Spot market price $0.0619",
        "sub-type": "launchSpecUnusable"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`fleetProgressHalted`

Keiner der Preise in den Startspezifikationen ist gültig, da er unter dem Spot-Preis liegt (alle Startspezifikationen haben `launchSpecUnusable`-Ereignisse ausgelöst). Eine Startspezifikation könnte gültig werden, wenn sich der Spot-Preis ändert.

`launchSpecTemporarilyBlacklisted`

Die Konfiguration ist nicht gültig und mehrere Versuche, Instances zu starten, sind fehlgeschlagen. Weitere Informationen finden Sie in der Beschreibung des Ereignisses.

`launchSpecUnusable`

Der Preis in einer Startspezifikation ist nicht gültig, da er unter dem Spot-Preis liegt.

`registerWithLoadBalancersFailed`

Der Versuch, Instances bei Load Balancern zu registrieren, ist fehlgeschlagen. Weitere Informationen finden Sie in der Beschreibung des Ereignisses.

EC2 Flottenfehler

EC2 Fleet sendet ein `EC2 Fleet Error` Ereignis an Amazon EventBridge , wenn beim Versand ein Fehler auftritt. Das Fehlerereignis verhindert, dass die Flotte versucht, ihre Zielkapazität zu erfüllen.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "69849a22-6d0f-d4ce-602b-b47c1c98240e",
    "detail-type": "EC2 Fleet Error",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-10-07T01:44:24Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-9bb19bc6-60d3-4fd2-ae47-
d33e68eafa08"
    ],
    "detail": {
        "description": "m3.large, ami-00068cd7555f543d5, Linux/UNIX: IPv6 is not
 supported for the instance type 'm3.large'. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`iamFleetRoleInvalid`

Die EC2 Flotte verfügt nicht über die erforderlichen Berechtigungen, um eine Instance zu starten oder zu beenden.

`allLaunchSpecsTemporarilyBlacklisted`

Keine der Konfigurationen ist gültig, und mehrere Versuche, Instances zu starten, sind fehlgeschlagen. Weitere Informationen finden Sie in der Beschreibung des Ereignisses.

`spotInstanceCountLimitExceeded`

Sie haben das Limit für die Anzahl der Spot-Instances erreicht, die Sie starten können.

`spotFleetRequestConfigurationInvalid`

Die Konfiguration ist nicht gültig. Weitere Informationen finden Sie in der Beschreibung des Ereignisses.

Ereignistypen für Spot-Flotten

Es gibt fünf Spot-Flotten-Ereignistypen. Für jeden Ereignistyp gibt es mehrere Sub-Typen.

Event types (Ereignistypen)

- EC2 Änderung des Flottenstatus erkennen
- EC2 Änderung der Spot-Instance-Anfrage für Spot-Flotten
- EC2 Änderung der Spot-Flotteninstanz
- EC2 Informationen zur Spot-Flotte
- EC2 Flottenfehler erkennen

EC2 Änderung des Flottenstatus erkennen

Spot-Flotte sendet ein `EC2 Spot Fleet State Change` Ereignis an Amazon, EventBridge wenn sich der Status einer Spot-Flotte ändert.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "d1af1091-6cc3-2e24-203a-3b870e455d5b",
    "detail-type": "EC2 Spot Fleet State Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:57:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-4b6d274d-0cea-4b2c-
b3be-9dc627ad1f55"
    ],
    "detail": {
```

```
        "sub-type": "submitted"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`active`

Die Spot-Flotte-Anfrage wurde validiert und Amazon EC2 versucht, die angestrebte Anzahl laufender Instances beizubehalten.

`cancelled`

Die Spot-Flotten-Anforderung wird storniert und hat keine ausgeführten Instances. Die Spot-Flotte wird zwei Tage nach Beendigung der zugehörigen Instances gelöscht.

`cancelled_running`

Die Spot-Flotten-Anforderung wird storniert und startet keine weiteren Instances. Die bestehenden Instances laufen weiter, bis sie unterbrochen oder beendet werden. Die Anforderung bleibt so lange in diesem Zustand, bis alle Instances unterbrochen oder beendet wurden.

`cancelled_terminating`

Die Spot-Flotten-Anforderung wird storniert und die zugehörigen Instances werden beendet. Die Anforderung bleibt so lange in diesem Zustand, bis alle Instances beendet wurden.

`expired`

Die Spot-Flotten-Anforderung ist abgelaufen. Wenn die Anforderung mit `TerminateInstancesWithExpiration` erstellt wurde, zeigt ein nachfolgendes `terminated`-Ereignis an, dass die Instances beendet werden.

`modify_in_progress`

Die Spot-Flotten-Anforderung wird geändert. Die Anforderung bleibt in diesem Zustand, bis die Änderung vollständig verarbeitet wurde.

`modify_succeeded`

Die Spot-Flotten-Anforderung wurde geändert.

`submitted`

Die Spot-Flotte-Anfrage wird geprüft und Amazon EC2 bereitet sich darauf vor, die angestrebte Anzahl von Instances zu starten.

`progress`

Die Spot-Flotten-Anforderung wird gerade erfüllt.

EC2 Änderung der Spot-Instance-Anfrage für Spot-Flotten

Spot Fleet sendet ein `EC2 Spot Fleet Spot Instance Request Change` Ereignis an Amazon, EventBridge wenn sich der Status einer Spot-Instance-Anfrage in der Flotte ändert.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "cd141ef0-14af-d670-a71d-fe46e9971bd2",
    "detail-type": "EC2 Spot Fleet Spot Instance Request Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:53:21Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-
a98d2133-941a-47dc-8b03-0f94c6852ad1"
    ],
    "detail": {
        "spot-instance-request-id": "sir-a2w9gc5h",
        "description": "SpotInstanceRequestId sir-a2w9gc5h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`active`

Die Spot-Instance-Anforderung wurde erfüllt und ist mit einer Spot-Instance verknüpft.

`cancelled`

Sie haben die Spot-Instance-Anforderung storniert oder die Spot-Instance-Anforderung ist abgelaufen.

`disabled`

Sie haben die Spot-Instance angehalten.

`submitted`

Die Spot-Instance-Anforderung wird gesendet.

EC2 Änderung der Spot-Flotteninstanz

Spot Fleet sendet ein `EC2 Spot Fleet Instance Change` Ereignis an Amazon, EventBridge wenn sich der Status einer Instance in der Flotte ändert.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "11591686-5bd7-bbaa-eb40-d46529c2710f",
    "detail-type": "EC2 Spot Fleet Instance Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T07:25:02Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-c8a764a4-bedc-4b62-
af9c-0095e6e3ba61"
    ],
    "detail": {
        "instance-id": "i-08b90df1e09c30c9b",
        "description": "{\"instanceType\":\"r4.2xlarge\",\"image\":
\"ami-032930428bf1abbff\",\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":
\"us-east-1a\"}",
        "sub-type": "launched"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`launched`

Eine neue Instance wurde gestartet.

`terminated`

Die Instance wurde beendet.

`termination_notified`

Eine Benachrichtigung zur Instance-Kündigung wurde gesendet, wenn eine Spot-Instance von Amazon EC2 während des Scale-Down beendet wurde, als die Zielkapazität der Flotte heruntergefahren wurde, beispielsweise von einer Zielkapazität von 4 auf eine Zielkapazität von 3.

EC2 Informationen zur Spot-Flotte

Spot Fleet sendet ein `EC2 Spot Fleet Information` Ereignis an Amazon EventBridge, wenn beim Versand ein Fehler auftritt. Das Informationsereignis hindert die Flotte nicht daran, ihre Zielkapazität zu erreichen.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "73a60f70-3409-a66c-635c-7f66c5f5b669",
    "detail-type": "EC2 Spot Fleet Information",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-08T20:56:12Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-2531ea06-
af18-4647-8757-7d69c94971b1"
    ],
    "detail": {
        "description": "r3.8xlarge, ami-032930428bf1abbff, Linux/UNIX, us-east-1a, Spot
 bid price is less than Spot market price $0.5291",
        "sub-type": "launchSpecUnusable"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`fleetProgressHalted`

Keiner der Preise in den Startspezifikationen ist gültig, da er unter dem Spot-Preis liegt (alle Startspezifikationen haben `launchSpecUnusable`-Ereignisse ausgelöst). Eine Startspezifikation könnte gültig werden, wenn sich der Spot-Preis ändert.

`launchSpecTemporarilyBlacklisted`

Die Konfiguration ist nicht gültig und mehrere Versuche, Instances zu starten, sind fehlgeschlagen. Weitere Informationen finden Sie in der Beschreibung des Ereignisses.

`launchSpecUnusable`

Der Preis in einer Startspezifikation ist nicht gültig, da er unter dem Spot-Preis liegt.

`registerWithLoadBalancersFailed`

Der Versuch, Instances bei Load Balancern zu registrieren, ist fehlgeschlagen. Weitere Informationen finden Sie in der Beschreibung des Ereignisses.

EC2 Flottenfehler erkennen

Spot Fleet sendet ein `EC2 Spot Fleet Error` Ereignis an Amazon EventBridge , wenn beim Versand ein Fehler auftritt. Das Fehlerereignis verhindert, dass die Flotte versucht, ihre Zielkapazität zu erfüllen.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "10adc4e7-675c-643e-125c-5bfa1b1ba5d2",
    "detail-type": "EC2 Spot Fleet Error",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T06:56:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/
sfr-38725d30-25f1-4f30-83ce-2907c56dba17"
    ],
    "detail": {
        "description": "r4.2xlarge, ami-032930428bf1abbff, Linux/UNIX: The
 associatePublicIPAddress parameter can only be specified for the network interface
 with DeviceIndex 0. ",
```

```
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`iamFleetRoleInvalid`

Die Spot-Flotte verfügt nicht über die erforderlichen Berechtigungen zum Starten oder Beenden einer Instance.

`allLaunchSpecsTemporarilyBlacklisted`

Keine der Konfigurationen ist gültig, und mehrere Versuche, Instances zu starten, sind fehlgeschlagen. Weitere Informationen finden Sie in der Beschreibung des Ereignisses.

`spotInstanceCountLimitExceeded`

Sie haben das Limit für die Anzahl der Spot-Instances erreicht, die Sie starten können.

`spotFleetRequestConfigurationInvalid`

Die Konfiguration ist nicht gültig. Weitere Informationen finden Sie in der Beschreibung des Ereignisses.

Tutorials für EC2-Flotte

Es gibt verschiedene Möglichkeiten, eine EC2-Flotte zu konfigurieren. Welche Konfiguration Sie wählen, hängt von Ihrem speziellen Anwendungsfall ab.

Die folgenden Tutorials behandeln einige der möglichen Anwendungsfälle und enthalten die Aufgaben, die zu ihrer Implementierung erforderlich sind.

Anwendungsfall	Link zum Tutorial
Verwenden Sie die Gewichtung von Instances , um die Verfügbarkeit und Leistung Ihrer EC2-Flotte zu verwalten. Mit der Instance-Gewichtung weisen Sie jedem Instance-Typ in Ihrer EC2-Flotte eine Gewichtung zu, um deren Rechenkapazität und	Tutorial: EC2-Flotte konfigurieren um Instance-Gewichtung zu verwenden

Anwendungsfall	Link zum Tutorial
Leistung im Verhältnis zueinander darzustellen. Basierend auf der Gewichtung kann die Flotte eine beliebige Kombination der angegeben en Instance-Typen verwenden, sofern sie die gewünschte Zielkapazität erfüllen kann.	
Verwenden Sie On-Demand-Kapazität, um die Verfügbarkeit in Spitzenzeiten sicherzustellen, profitieren Sie jedoch von zusätzlicher Spot-Kapazität zu geringeren Kosten. Konfigurieren Sie Ihre EC2-Flotte so, dass On-Demand-Instances als primäre Kapazität verwendet werden, um die verfügbare Kapazität in Spitzenzeiten sicherzustellen. Weisen Sie Spot Instances außerdem eine gewisse Kapazität zu, um von vergünstigten Preisen zu profitieren. Denken Sie dabei daran, dass Spot Instances unterbrochen werden können, wenn Amazon EC2 die Kapazität zurück benötigt.	Tutorial: EC2-Flotte für die Verwendung von On-Demand Instances als primäre Kapazität konfigurieren

Anwendungsfall	Link zum Tutorial
Verwenden Sie Kapazitätsreservierungen, um Rechenkapazität für Ihre On-Demand-Instances zu reservieren. Sie können eine EC2-Flotte so konfigurieren, dass sie die `targeted`Kapazitätsreservierungen beim Starten von On-Demand-Instances zuerst verwendet. Wenn Sie strenge Kapazitätsanforderungen haben und geschäftskritische Workloads ausführen, die ein gewisses Maß an langfristiger oder kurzfristiger Kapazitätssicherung erfordern, empfehlen wir Ihnen, eine Kapazitätsreservierung zu erstellen, um sicherzustellen, dass Sie immer Zugriff auf Amazon-EC2-Kapazität haben; wenn und so lange Sie sie benötigen.	Tutorial: EC2 Fleet so konfigurieren, dass On-Demand Instances mit gezielten Kapazitätsreservierungen gestartet werden
Verwenden Sie Kapazitätsblöcke, um stark nachgefragte GPU-Instances für Ihre ML-Workloads zu reservieren. Konfigurieren Sie Ihre EC2-Flotte, um Instances in Kapazitätsblöcken zu starten.	Tutorial: Ihre EC2-Flotte konfigurieren, um Instances in Kapazitätsblöcken zu starten

Tutorial: EC2-Flotte konfigurieren um Instance-Gewichtung zu verwenden

In dieser Anleitung wird ein fiktives Unternehmen mit dem Namen Example Corp verwendet, um das Anfordern einer EC2-Flotte mit Instance-Gewichtung zu veranschaulichen.

Ziel

Example Corp, ein Pharmaunternehmen, möchte die Rechenleistung von Amazon EC2 zum Prüfen chemischer Verbindungen nutzen, die im Kampf gegen Krebs eingesetzt werden könnten.

Planung

Example Corp macht sich zunächst mit den Bewährten Methoden für Spot vertraut. Als Nächstes ermittelt Example Corp die Anforderungen für die eigene EC2-Flotte.

Instance-Typen

Example Corp verfügt über eine rechen- und speicherintensive Anwendung, welche die beste Leistung bei mindestens 60 GB Speicher und mit mindestens acht virtuellen CPUs (vCPUs) aufweist. Das Unternehmen möchte diese Ressourcen für die Anwendung zum geringstmöglichen Preis maximieren. Example Corp entscheidet, dass die folgenden EC2-Instance-Typen die Anforderungen erfüllen würden:

Instance-Typ	Arbeitsspeicher (GiB)	vCPUs
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

Zielkapazität in Einheiten

Bei der Instance-Gewichtung kann die Zielkapazität einer Anzahl von Instances (Standard) oder einer Kombination von Faktoren entsprechen, wie beispielsweise Kerne (vCPUs), Arbeitsspeicher (GiBs) und Speicher (GBs). Example Corp betrachtet die Basis für ihre Anwendung (60 GB RAM und acht vCPUs) als eine Einheit und entscheidet, dass ein 20-Faches dieser Menge ihre Anforderungen erfüllen würde. Also legt das Unternehmen für seine EC2-Flotte-Anfrage eine Zielkapazität von 20 fest.

Instance-Gewichtungen

Nach dem Festlegen der Zielkapazität berechnet Example Corp die Instance-Gewichtungen. Zum Berechnen der Instance-Gewichtungen der einzelnen Instance-Typen ermitteln sie die folgenden Einheiten der einzelnen Instance-Typen, die zum Erreichen der Zielkapazität erforderlich sind:

- r3.2xlarge (61,0 GB, 8 vCPUs) = 1 Einheit von 20

- r3.4xlarge (122,0 GB, 16 vCPUs) = 2 Einheiten von 20
- r3.8xlarge (244,0 GB, 32 vCPUs) = 4 Einheiten von 20

Aus diesem Grund weist Example Corp die Instance-Gewichtungen 1, 2 und 4 den entsprechenden Startkonfigurationen in ihrer EC2-Flotte-Anfrage zu.

Preis pro Einheitsstunde

Example Corp verwendet den On-Demand-Preis pro Instance-Stunde als Startpunkt für den Preis. Es wäre auch möglich, frühere Spot-Preise oder eine Kombination aus beidem zu verwenden. Zum Berechnen des Preises pro Einheitsstunde teilen sie den Startpreis pro Instance-Stunde durch die Gewichtung. Beispiel:

Instance-Typ	On-Demand-Preis	Instance-Gewichtung	Preis pro Einheitsstunde
r3.2xlarge	0,7 USD	1	0,7 USD
r3.4xLarge	$1.4	2	0,7 USD
r3.8xLarge	$2,8	4	0,7 USD

Example Corp könnte einen globalen Preis pro Einheitsstunde in Höhe von 0,7 USD angeben und für alle drei Instance-Typen wettbewerbsfähig sein. Sie könnten auch einen globalen Preis pro Einheitsstunde in Höhe von 0,7 USD und einen spezifischen Preis pro Einheitsstunde in Höhe von 0,9 USD in der `r3.8xlarge`-Startspezifikation verwenden.

Überprüfen der Berechtigungen

Vor dem Erstellen einer EC2-Flotte überprüft Example Corp, ob eine IAM-Rolle mit den erforderlichen Berechtigungen verfügbar ist. Weitere Informationen finden Sie unter EC2 Voraussetzungen für die Flotte.

Erstellen einer Startvorlage

Als Nächstes erstellt Example Corp eine Startvorlage. Die Startvorlagen-ID wird im folgenden Schritt verwendet. Weitere Informationen finden Sie unter Erstellen Sie eine EC2 Amazon-Startvorlage.

Erstellen der EC2-Flotte

Example Corp erstellt eine Datei mit dem Namen `config.json` und der folgenden Konfiguration für die EC2-Flotte: Ersetzen Sie im folgenden Beispiel die Ressourcenbezeichner durch Ihre eigenen Ressourcenbezeichner.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "r3.2xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 1
                },
                {
                    "InstanceType": "r3.4xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 2
                },
                {
                    "InstanceType": "r3.8xlarge",
                    "MaxPrice": "0.90",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 4
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    }
```

```
}
```

Example Corp erstellt die EC2-Flotte mit dem folgenden create-fleet-Befehl:

```
aws ec2 create-fleet --cli-input-json file://config.json
```

Weitere Informationen finden Sie unter Erstellen Sie eine EC2 Flotte.

Bereitstellung

Die Zuweisungsstrategie legt fest, aus welchen Spot-Kapazitätspools Ihre Spot-Instances stammen.

Bei der `lowest-price`-Strategie (der Standardstrategie) stammen die Spot-Instances aus dem Pool mit dem niedrigsten Preis pro Einheit zum Zeitpunkt der Bereitstellung. Zum Bereitstellen von 20 Kapazitätseinheiten startet die EC2-Flotte entweder 20 `r3.2xlarge`-Instances (20 geteilt durch 1), 10 `r3.4xlarge`-Instances (20 geteilt durch 2) oder 5 `r3.8xlarge`-Instances (20 geteilt durch 4).

Würde Example Corp die `diversified`-Strategie verwenden, dann würden die Spot-Instances aus allen drei Pools stammen. Die EC2-Flotte würde 6 `r3.2xlarge`-Instances (die 6 Einheiten bereitstellen), 3 `r3.4xlarge`-Instances (die 6 Einheiten bereitstellen) und 2 `r3.8xlarge`-Instances (die 8 Einheiten bereitstellen) mit insgesamt 20 Einheiten starten.

Tutorial: EC2-Flotte für die Verwendung von On-Demand Instances als primäre Kapazität konfigurieren

In dieser Anleitung wird ein fiktives Unternehmen mit dem Namen ABC Online verwendet, um das Anfordern einer EC2-Flotte mit On-Demand als Primärkapazität und Spot-Kapazität, wenn verfügbar, zu veranschaulichen.

Ziel

ABC Online, ein Restaurantlieferservice, möchte in der Lage sein, Amazon-EC2-Kapazität für alle EC2-Instance-Typen und Kaufoptionen bereitzustellen, um die gewünschte Größe, Leistung und Kosten zu erreichen.

Plan

ABC Online benötigt eine feste Kapazität, um in Spitzenzeiten arbeiten zu können, möchte aber von einer erhöhten Kapazität zu einem niedrigeren Preis profitieren. ABC Online ermittelt die folgenden Anforderungen für die eigene EC2-Flotte:

- On-Demand-Instance-Kapazität – ABC Online benötigt 15 On-Demand-Instances, um sicherzustellen, dass der Datenverkehr in Spitzenzeiten verarbeitet werden kann.
- Spot-Instance-Kapazität – Um die Leistung zu verbessern, aber zu einem niedrigeren Preis, plant ABC Online die Bereitstellung von 5 Spot Instances.

Überprüfen der Berechtigungen

Vor dem Erstellen einer EC2-Flotte prüft ABC Online, ob eine IAM-Rolle mit den erforderlichen Berechtigungen verfügbar ist. Weitere Informationen finden Sie unter EC2 Voraussetzungen für die Flotte.

Erstellen einer Startvorlage

Als Nächstes erstellt ABC Online eine Startvorlage. Die Startvorlagen-ID wird im folgenden Schritt verwendet. Weitere Informationen finden Sie unter Erstellen Sie eine EC2 Amazon-Startvorlage.

Erstellen der EC2-Flotte

ABC Online erstellt eine Datei mit dem Namen `config.json` und der folgenden Konfiguration für die EC2-Flotte: Ersetzen Sie im folgenden Beispiel die Ressourcenbezeichner durch Ihre eigenen Ressourcenbezeichner.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "2"
            }

        }
    ],
    "TargetCapacitySpecification": {
```

```
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity":15,
        "DefaultTargetCapacityType": "spot"
    }
}
```

ABC Online erstellt die EC2-Flotte mit dem folgenden create-fleet-Befehl:

```
aws ec2 create-fleet --cli-input-json file://config.json
```

Weitere Informationen finden Sie unter Erstellen Sie eine EC2 Flotte.

Bereitstellung

Die Zuweisungsstrategie legt fest, dass die On-Demand-Kapazität immer erfüllt ist, während der Saldo der Zielkapazität als Spot erfüllt ist, wenn Kapazität und Verfügbarkeit vorhanden sind.

Tutorial: EC2 Fleet so konfigurieren, dass On-Demand Instances mit gezielten Kapazitätsreservierungen gestartet werden

Dieses Tutorial führt Sie durch alle Schritte, die Sie ausführen müssen, damit Ihre EC2-Flotte On-Demand-Instances in `targeted` Kapazitätsreservierungen startet.

Sie erfahren, wie Sie eine Flotte so konfigurieren, dass `targeted`-On-Demand-Kapazitätsreservierungen zuerst beim Starten von On-Demand-Instances verwendet werden. Außerdem erfahren Sie, wie Sie die Flotte so konfigurieren, dass die Flotte, wenn die gesamte On-Demand-Zielkapazität die Anzahl der verfügbaren ungenutzten Kapazitätsreservierungen überschreitet, die angegebene Zuordnungsstrategie verwendet, um die Instance-Pools auszuwählen, in denen die verbleibende Zielkapazität gestartet werden soll.

EC2-Flotte-Konfiguration

In diesem Tutorial ist die Flotte konfiguriert wie folgt:

- Zielkapazität: 10 On-Demand-Instances
- Nicht verwendete `targeted`-Kapazitätsreservierungen: 6 (geringer als die On-Demand-Zielkapazität der Flotte von 10 On-Demand-Instances)
- Anzahl der Kapazitätsreservierungspools: 2 (`us-east-1a` und `us-east-1b`)

- Anzahl der Kapazitätsreservierungen pro Pool: 3
- On-Demand-Zuordnungsstrategie: `lowest-price` (Wenn die Anzahl der nicht genutzten Kapazitätsreservierungen kleiner als die On-Demand-Zielkapazität ist, bestimmt die Flotte die Pools, in denen die verbleibende On-Demand-Kapazität basierend auf der On-Demand-Zuordnungsstrategie gestartet werden soll.)

  Beachten Sie, dass Sie auch die `prioritized`-Zuordnungsstrategie anstelle der `lowest-price`-Zuordnungsstrategie verwenden können.

Starten von On-Demand-Instances in targeted-Kapazitätsreservierungen müssen Sie eine Reihe von Schritten wie folgt ausführen:

- Schritt 1: Erstellen von Kapazitätsreservierungen
- Schritt 2: Erstellen einer Ressourcengruppe für Kapazitätsreservierung
- Schritt 3: Hinzufügen der Kapazitätsreservierungen zur Ressourcengruppe der Kapazitätsreservierung
- (Optional) Schritt 4: Anzeigen der Kapazitätsreservierungen in der Ressourcengruppe
- Schritt 5: Erstellen einer Startvorlage, die angibt, dass die Kapazitätsreservierung auf eine bestimmte Ressourcengruppe abzielt
- (Optional) Schritt 6: Beschreiben der Startvorlage
- Schritt 7: Erstellen einer EC2-Flotte
- (Optional) Schritt 8: Anzeigen der Anzahl der verbleibenden ungenutzten Kapazitätsreservierungen

Schritt 1: Erstellen von Kapazitätsreservierungen

Verwenden Sie den Befehl create-capacity-reservation (Kapazitätsreservierung erstellen), um die Kapazitätsreservierungen zu erstellen, drei für `us-east-1a` und weitere drei für `us-east-1b`. Mit Ausnahme der Availability Zone sind die anderen Attribute der Kapazitätsreservierungen identisch.

3 Kapazitätsreservierungen in **`us-east-1a`**

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1a \
    --instance-type c5.xlarge \
    --instance-platform Linux/UNIX \
    --instance-count 3 \
```

```
    --instance-match-criteria targeted
```

Beispiel für die resultierende ID der Kapazitätsreservierung

```
cr-1234567890abcdef1
```

3 Kapazitätsreservierungen in **`us-east-1b`**

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1b \
    --instance-type c5.xlarge \
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Beispiel für die resultierende ID der Kapazitätsreservierung

```
cr-54321abcdef567890
```

Schritt 2: Erstellen einer Ressourcengruppe für Kapazitätsreservierung

Verwenden des `resource-groups`-Dienstes und des Befehls create-group (Erstellen einer Gruppe), um eine Ressourcengruppe für Kapazitätsreservierung zu erstellen In diesem Beispiel hat die Ressourcengruppe den Namen `my-cr-group`. Informationen dazu, warum Sie eine Ressourcengruppe erstellen müssen, finden Sie unter Kapazitätsreservierungen verwenden, um On-Demand-Kapazitäten in der EC2-Flotte zu reservieren.

```
aws resource-groups create-group \
    --name my-cr-group \
    --configuration '{"Type":"AWS::EC2::CapacityReservationPool"}'
 '{"Type":"AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-resource-
types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

Schritt 3: Hinzufügen der Kapazitätsreservierungen zur Ressourcengruppe der Kapazitätsreservierung

Verwenden des `resource-groups`-Dienstes und des Befehls group-resources (Gruppenressourcen), um die Kapazitätsreservierungen, die Sie in Schritt 1 erstellt haben, der

Ressourcengruppe Kapazitätsreservierungen hinzuzufügen. Beachten Sie, dass Sie die On-Demand-Kapazitätsreservierungen anhand ihrer ARNs referenzieren müssen.

```
aws resource-groups group-resources \
    --group my-cr-group \
    --resource-arns \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Beispielausgabe

```
{
   "Failed": [],
   "Succeeded": [
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
   ]
}
```

(Optional) Schritt 4: Anzeigen der Kapazitätsreservierungen in der Ressourcengruppe

Verwenden des `resource-groups`-Dienstes und des Befehls list-group-resources (Gruppenressourcen auflisten), um optional die Ressourcengruppe zu beschreiben, um ihre Kapazitätsreservierungen anzuzeigen.

```
aws resource-groups list-group-resources --group my-cr-group
```

Beispielausgabe

```
{
    "ResourceIdentifiers": [
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-1234567890abcdef1"
        },
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-54321abcdef567890"
```

```
        }
    ]
}
```

Schritt 5: Erstellen einer Startvorlage, die angibt, dass die Kapazitätsreservierung auf eine bestimmte Ressourcengruppe abzielt

Verwenden des Befehls create-launch-template (Startvorlage erstellen), um eine Startvorlage zu erstellen, in der Sie die zu verwendenden Kapazitätsreservierungen angeben können. In diesem Beispiel wird die Flotte `targeted`-Kapazitätsreservierungen verwenden, die einer Ressourcengruppe hinzugefügt wurden. Daher geben die Startvorlagendaten an, dass die Kapazitätsreservierung auf eine bestimmte Ressourcengruppe ausgerichtet ist. In diesem Beispiel hat die Startvorlage den Namen `my-launch-template`.

```
aws ec2 create-launch-template \
    --launch-template-name my-launch-template \
    --launch-template-data \
        '{"ImageId": "ami-0123456789example",
          "CapacityReservationSpecification":
            {"CapacityReservationTarget":
                { "CapacityReservationResourceGroupArn": "arn:aws:resource-groups:us-
east-1:123456789012:group/my-cr-group" }
            }
        }'
```

(Optional) Schritt 6: Beschreiben der Startvorlage

Verwenden Sie den Befehl describe-launch-template-versions, um optional die Startvorlage zu beschreiben, um ihre Konfiguration anzuzeigen.

```
aws ec2 describe-launch-template-versions --launch-template-name my-launch-template
```

Beispielausgabe

```
{
    "LaunchTemplateVersions": [
        {
            "LaunchTemplateId": "lt-01234567890example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
```

```
            "CreateTime": "2021-01-19T20:50:19.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Admin",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0947d2ba12ee1ff75",
                "CapacityReservationSpecification": {
                    "CapacityReservationTarget": {
                        "CapacityReservationResourceGroupArn": "arn:aws:resource-
groups:us-east-1:123456789012:group/my-cr-group"
                    }
                }
            }
        }
    ]
}
```

Schritt 7: Erstellen einer EC2-Flotte

Erstellen Sie eine EC2-Flotte, die die Konfigurationsinformationen für die Instances angibt, die sie starten soll. Die folgende EC2-Flottenkonfiguration zeigt nur die relevanten Konfigurationen für dieses Beispiel. Die Startvorlage `my-launch-template` ist die Startvorlage, die Sie in Schritt 5 erstellt haben. Es gibt zwei Instance-Pools mit jeweils demselben Instance-Typ (`c5.xlarge`), aber mit unterschiedlichen Availability Zones (`us-east-1a` und `us-east-1b`). Der Preis der Instance-Pools ist derselbe, da die Preise für die Region und nicht für die Availability Zone definiert sind. Die gesamte Zielkapazität beträgt 10 und der Standardzielkapazitätstyp ist `on-demand`. Die On-Demand-Zuordnungsstrategie ist `lowest-price`. Die Nutzungsstrategie für Kapazitätsreservierungen ist `use-capacity-reservations-first`.

> **Note**
>
> Der Flottentyp muss sein `instant`. Andere Flotten-Typen unterstützen nicht `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
```

```
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
}
```

Nachdem Sie die `instant`-Flotte mit der vorherigen Konfiguration erstellt haben, werden die folgenden 10 Instances gestartet, um die Zielkapazität zu erreichen:

- Die Kapazitätsreservierungen werden zuerst verwendet, um 6 On-Demand-Instances wie folgt zu starten:
  - 3 On-Demand-Instances werden in die 3 `c5.xlarge` `targeted`Kapazitätsreservierungen in `us-east-1a` gestartet
  - 3 On-Demand-Instances werden in die 3 `c5.xlarge` `targeted`Kapazitätsreservierungen in `us-east-1b` gestartet
- Um die Zielkapazität zu erreichen, werden 4 zusätzliche On-Demand-Instances gemäß der On-Demand-Zuordnungsstrategie in die reguläre On-Demand-Strategie gestartet, die in diesem Beispiel `lowest-price` ist. Da die Pools jedoch denselben Preis haben (da der Preis pro Region und nicht pro Availability Zone ist), startet die Flotte die restlichen 4 On-Demand-Instances in einem der Pools.

(Optional) Schritt 8: Anzeigen der Anzahl der verbleibenden ungenutzten Kapazitätsreservierungen

Nachdem die Flotte gestartet wurde, können Sie optional describe-capacity-reservations (Kapazitätsreservierungen beschreiben) ausführen, um zu sehen, wie viele nicht verwendete Kapazitätsreservierungen noch übrig sind. In diesem Beispiel sollte die folgende Antwort angezeigt werden, die zeigt, dass alle Kapazitätsreservierungen in allen Pools verwendet wurden.

```
{ "CapacityReservationId":  "cr-111",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}

 { "CapacityReservationId":  "cr-222",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}
```

Tutorial: Ihre EC2-Flotte konfigurieren, um Instances in Kapazitätsblöcken zu starten

Dieses Tutorial führt Sie durch die Schritte, die Sie durchführen müssen, damit Ihre EC2-Flotte Instances in Kapazitätsblöcken startet.

In den meisten Fällen sollte die Zielkapazität der Anfrage für die EC2-Flotte kleiner oder gleich der verfügbaren Kapazität der von Ihnen angestrebten Kapazitätsblock-Reservierung sein. Zielkapazitätsanfragen, die die Grenzen der Kapazitätsblock-Reservierung überschreiten, werden nicht erfüllt. Wenn die Anfrage für die Zielkapazität die Grenzen Ihrer Kapazitätsblock-Reservierung überschreitet, erhalten Sie eine `Insufficient Capacity Exception` wegen unzureichender Kapazität für die Kapazität, die die Grenzen Ihrer Kapazitätsblock-Reservierung überschreitet.

> **Note**
>
> Bei Kapazitätsblöcken wird die EC2-Flotte für den Rest der gewünschten Zielkapazität nicht auf den Start von On-Demand-Instances zurückgreifen.

Wenn die EC2-Flotte nicht in der Lage ist, die angeforderte Zielkapazität in einer verfügbaren Kapazitätsblock-Reservierung zu erfüllen, wird die EC2-Flotte so viel Kapazität wie möglich

bereitstellen und die Instances zurückgeben, die gestartet werden konnten. Sie können den Aufruf der EC2-Flotte wiederholen, bis alle Instances bereitgestellt sind.

Nachdem Sie die EC2-Flotten-Anfrage konfiguriert haben, müssen Sie bis zum Startdatum Ihrer Kapazitätsblock-Reservierung warten. Wenn Sie Anfragen an die EC2-Flotte stellen, um in einen Kapazitätsblock zu starten, der noch nicht begonnen hat, erhalten Sie eine `Insufficient Capacity Error`.

Nachdem Ihre Kapazitätsblock-Reservierung aktiv wird, können Sie EC2-Flotten-API-Aufrufe durchführen und die Instances basierend auf den von Ihnen ausgewählten Parametern in Ihrem Kapazitätsblock bereitstellen. Instances, die im Kapazitätsblock laufen, laufen weiter, bis Sie sie manuell stoppen oder beenden oder bis Amazon EC2 die Instances beendet, wenn die Reservierung des Kapazitätsblocks endet.

Weitere Informationen zu Kapazitätsblöcken finden Sie unter Kapazitätsblöcke für ML.

Überlegungen

- Für das Starten von Instances in Kapazitätsblöcke des Typs `instant` werden nur Anfragen vom Typ EC2-Flotte unterstützt. Weitere Informationen finden Sie unter EC2-Flotte des Typs instant konfigurieren.
- Mehrere Kapazitätsblöcke in derselben EC2–Flottenanforderung werden nicht unterstützt.
- Die Verwendung von `OnDemandTargetCapacity` oder `SpotTargetCapacity` bei gleichzeitiger Einstellung von `capacity-block` als `DefaultTargetCapacity` wird nicht unterstützt.
- Wenn `DefaultTargetCapacityType` auf `capacity-block` gesetzt ist, können Sie `OnDemandOptions::CapacityReservationOptions` nicht angeben. Es kommt zu einer Ausnahme.

So konfigurieren Sie ein EC2-Flotte, um Instances in Kapazitätsblöcken zu starten

1. Eine Startvorlage erstellen

   Gehen Sie in der Startvorlage folgendermaßen vor:

   - Für `InstanceMarketOptionsRequest` setzen Sie den Wert `MarketType` auf `capacity-block`.
   - Geben Sie die Kapazitätsblock-Reservierungs-ID an`CapacityReservationID`, um die Kapazitätsblock-Reservierung als Ziel zu verwenden.

Notieren Sie sich den Namen und die Version der Startvorlage. Diese Informationen sind im nächsten Schritt erforderlich.

Weitere Informationen zum Erstellen einer Startvorlage finden Sie unter Erstellen Sie eine EC2 Amazon-Startvorlage.

2. Die EC2-Flotte konfigurieren.

   Erstellen Sie eine Datei, `config.json` und der folgenden Konfiguration für die EC2-Flotte. Ersetzen Sie im folgenden Beispiel die Ressourcenbezeichner durch Ihre eigenen Ressourcenbezeichner.

   Weitere Information zum Konfigurieren einer EC2-Flotte finden Sie unter Erstellen Sie eine EC2 Flotte.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "CBR-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "p5.48xlarge",
                    "AvailabilityZone": "us-east-1a"
                },
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "capacity-block"
    },
    "Type": "instant"
}
```

3. Starten Sie die Flotte.

   Verwenden Sie den folgenden create-fleet-Befehl.

```
aws ec2 create-fleet --cli-input-json file://config.json
```

Weitere Informationen finden Sie unter Erstellen Sie eine Flotte EC2 .

CLI-Beispielkonfigurationen für EC2 Fleet

Sie können Ihre EC2 Flottenkonfiguration in einer JSON-Datei definieren und dann mit dem Befehl create-fleet auf diese Datei verweisen, um Ihre Flotte wie folgt zu erstellen:

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

Die folgenden Beispiele veranschaulichen Startkonfigurationen für verschiedene EC2 Fleet-Anwendungsfälle. Weitere Informationen zu den Konfigurationsparametern finden Sie unter create-fleet.

Beispiele

- Beispiel 1: Starten von Spot-Instances als Standard-Kaufoption
- Beispiel 2: Starten von On-Demand-Instances als Standard-Kaufoption
- Beispiel 3: Starten von On-Demand-Instances als primäre Kapazität
- Beispiel 4: Starten von On-Demand-Instances unter Verwendung von mehreren Kapazitätsreservierungen
- Beispiel 5: Starten von On-Demand-Instances mit Kapazitätsreservierungen, wenn die Gesamtzielkapazität die Anzahl der nicht verwendeten Kapazitätsreservierungen übersteigt
- Beispiel 6: Starten von On-Demand-Instances mithilfe von Ziel-Kapazitätsreservierungen
- Beispiel 7: Konfigurieren des Kapazitätsneuausgleichs, um Ersatz-Spot-Instances zu starten
- Beispiel 8: Starten von Spot Instances in einer kapazitätsoptimierten Flotte
- Beispiel 9: Starten von Spot Instances in einer kapazitätsoptimierten Flotte mit Prioritäten
- Beispiel 10: Starten Sie Spot-Instances in einer Flotte price-capacity-optimized
- Beispiel 11: Konfigurieren von attributbasierter Auswahl von Instance-Typen

Weitere CLI-Beispiele für Flotten des Typs `instant` finden Sie unter EC2-Flotte des Typs instant konfigurieren.

Beispiel 1: Starten von Spot-Instances als Standard-Kaufoption

Das folgende Beispiel spezifiziert die Mindestparameter, die für eine EC2 Flotte erforderlich sind: eine Startvorlage, eine Zielkapazität und eine Standardkaufoption. Die Startvorlage wird durch ihre Startvorlagen-ID und Versionsnummer identifiziert. Die Zielkapazität für die Flotte beträgt 2 Instances, die Standard-Kaufoption ist `spot`, was dazu führt, dass die Flotte 2 Spot-Instances startet.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Beispiel 2: Starten von On-Demand-Instances als Standard-Kaufoption

Im folgenden Beispiel werden die Mindestparameter angegeben, die für eine EC2 Flotte erforderlich sind: eine Startvorlage, eine Zielkapazität und eine Standardkaufoption. Die Startvorlage wird durch ihre Startvorlagen-ID und Versionsnummer identifiziert. Die Zielkapazität für die Flotte beträgt 2 Instances, die Standard-Kaufoption ist `on-demand`, was dazu führt, dass die Flotte 2 On-Demand-Instances startet.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
```

```
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "on-demand"
    }
}
```

Beispiel 3: Starten von On-Demand-Instances als primäre Kapazität

Das folgende Beispiel gibt die Gesamtzielkapazität von 2 Instances für die Flotte und eine Zielkapazität von 1 On-Demand-Instance an. Die Standard-Kaufoption ist `spot`. Die Flotte startet 1 On-Demand-Instance wie angegeben, muss aber noch eine weitere Instance starten, um die gesamte Zielkapazität zu erreichen. Die Kaufoption für die Differenz wird berechnet als `TotalTargetCapacity` – `OnDemandTargetCapacity` = `DefaultTargetCapacityType`, was dazu führt, dass die Flotte 1 Spot Instance launcht.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "OnDemandTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Beispiel 4: Starten von On-Demand-Instances unter Verwendung von mehreren Kapazitätsreservierungen

Sie können eine Flotte so konfigurieren, dass sie On-Demand-Kapazitätsreservierungen zuerst beim Start von On-Demand-Instances verwendet, indem Sie die Nutzungsstrategie für Kapazitätsreservierungen auf `use-capacity-reservations-first` festlegen. Dieses Beispiel zeigt, wie die Flotte die Kapazitätsreservierungen auswählt, die verwendet werden sollen, wenn mehr Kapazitätsreservierungen vorhanden sind, als für die Erreichung der Zielkapazität erforderlich sind.

In diesem Beispiel sieht die Flottenkonfiguration wie folgt aus:

- Zielkapazität: 12 On-Demand-Instances
- Gesamt nicht verwendete Kapazitätsreservierungen: 15 (mehr als die On-Demand-Zielkapazität der Flotte von 12 On-Demand-Instances)
- Anzahl der Kapazitätsreservierungspools: 3 (`m5.large`, `m4.xlarge`, und `m4.2xlarge`)
- Anzahl der Kapazitätsreservierungen pro Pool: 5
- On-Demand-Zuordnungsstrategie `lowest-price` (Wenn mehrere ungenutzte Kapazitätsreservierungen in mehreren Instance-Pools vorhanden sind, bestimmt die Flotte anhand der On-Demand-Zuordnungsstrategie die Pools, in denen die On-Demand-Instances gestartet werden sollen.)

  Beachten Sie, dass Sie auch die `prioritized`-Zuordnungsstrategie anstelle der `lowest-price`-Zuordnungsstrategie verwenden können.

Kapazitätsreservierungen

Das Konto hat die folgenden 15 nicht verwendeten Kapazitätsreservierungen in 3 verschiedenen Pools. Die Anzahl der Kapazitätsreservierungen in jedem Pool wird durch `AvailableInstanceCount` angezeigt.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

```
{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Flottenkonfiguration

Die folgende Flottenkonfiguration zeigt nur die relevanten Konfigurationen für dieses Beispiel. Die gesamte Zielkapazität beträgt 12 und der Standardzielkapazitätstyp ist `on-demand`. Die On-Demand-Zuordnungsstrategie ist `lowest-price`. Die Nutzungsstrategie für Kapazitätsreservierungen ist `use-capacity-reservations-first`.

In diesem Beispiel ist der On-Demand-Instance-Preis:

- `m5.large` - 0,096 USD pro Stunde
- `m4.xlarge` - 0,20 USD pro Stunde
- `m4.2xlarge` - 0,40 USD pro Stunde

> **Note**
>
> Der Flottentyp muss vom Typ `instant` sein. Andere Flotten-Typen unterstützen `use-capacity-reservations-first` nicht.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-abc1234567example",
                "Version": "1"
            },
            "Overrides": [
                {
```

```
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 12,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant"
}
```

Nachdem Sie die `instant`-Flotte mit der vorherigen Konfiguration erstellt haben, werden die folgenden 12 Instances gestartet, um die Zielkapazität zu erreichen:

- 5 `m5.large` On-Demand-Instances in `us-east-1a` – `m5.large` in `us-east-1a` ist der niedrigste Preis, und es gibt fünf verfügbare ungenutzte `m5.large`-Kapazitätsreservierungen
- 5 `m4.xlarge`-On-Demand-Instances in us-east-1a – `m4.xlarge` in `us-east-1a` ist der niedrigste Preis und es gibt fünf verfügbare ungenutzte `m4.xlarge`-Kapazitätsreservierungen.
- 2 `m4.2xlarge`-On-Demand-Instances in us-east-1a – `m4.2xlarge` in `us-east-1a` ist der drittniedrigste Preis und es gibt fünf verfügbare, nicht verwendete `m4.2xlarge`-Kapazitätsreservierungen, von denen nur zwei benötigt werden, um die Zielkapazität zu erfüllen

Nach dem Start der Flotte können Sie nachsehen, wie viele ungenutzte Kapazitätsreservierungen noch übrig sind. describe-capacity-reservations In diesem Beispiel sollten Sie die folgende Antwort sehen, die zeigt, dass alle `m5.large`- und `m4.xlarge`-Kapazitätsreservierungen verwendet wurden, wobei 3 `m4.2xlarge`-Kapazitätsreservierungen nicht verwendet wurden.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 3
}
```

Beispiel 5: Starten von On-Demand-Instances mit Kapazitätsreservierungen, wenn die Gesamtzielkapazität die Anzahl der nicht verwendeten Kapazitätsreservierungen übersteigt

Sie können eine Flotte so konfigurieren, dass sie On-Demand-Kapazitätsreservierungen zuerst beim Start von On-Demand-Instances verwendet, indem Sie die Nutzungsstrategie für Kapazitätsreservierungen auf `use-capacity-reservations-first` festlegen. Dieses Beispiel zeigt, wie die Flotte die Instance-Pools auswählt, in denen On-Demand-Instances gestartet werden sollen, wenn die gesamte Zielkapazität die Anzahl der verfügbaren ungenutzten Kapazitätsreservierungen überschreitet.

In diesem Beispiel sieht die Flottenkonfiguration wie folgt aus:

- Zielkapazität: 16 On-Demand-Instances
- Gesamt nicht verwendete Kapazitätsreservierungen: 15 (weniger als die On-Demand-Zielkapazität der Flotte von 16 On-Demand-Instances)

- Anzahl der Kapazitätsreservierungspools: 3 (`m5.large`, `m4.xlarge`, und `m4.2xlarge`)
- Anzahl der Kapazitätsreservierungen pro Pool: 5
- On-Demand-Zuordnungsstrategie: `lowest-price` (Wenn die Anzahl der nicht genutzten Kapazitätsreservierungen kleiner als die On-Demand-Zielkapazität ist, bestimmt die Flotte die Pools, in denen die verbleibende On-Demand-Kapazität basierend auf der On-Demand-Zuordnungsstrategie gestartet werden soll.)

  Beachten Sie, dass Sie auch die `prioritized`-Zuordnungsstrategie anstelle der `lowest-price`-Zuordnungsstrategie verwenden können.

Kapazitätsreservierungen

Das Konto hat die folgenden 15 nicht verwendeten Kapazitätsreservierungen in 3 verschiedenen Pools. Die Anzahl der Kapazitätsreservierungen in jedem Pool wird durch `AvailableInstanceCount` angezeigt.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
```

```
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Flottenkonfiguration

Die folgende Flottenkonfiguration zeigt nur die relevanten Konfigurationen für dieses Beispiel. Die gesamte Zielkapazität beträgt 16 und der Standardzielkapazitätstyp ist `on-demand`. Die On-Demand-Zuordnungsstrategie ist `lowest-price`. Die Nutzungsstrategie für Kapazitätsreservierungen ist `use-capacity-reservations-first`.

In diesem Beispiel ist der On-Demand-Instance-Preis:

- m5.large – 0,096 USD pro Stunde
- m4.xlarge – 0,20 USD pro Stunde
- m4.2xlarge – 0,40 USD pro Stunde

> **Note**
>
> Der Flottentyp muss `instant` sein. Andere Flotten-Typen unterstützen `use-capacity-reservations-first` nicht.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            },
            "Overrides": [
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
```

```
                    "AvailabilityZone": "us-east-1a",
                    "WeightedCapacity": 1
                },
                {
                    "InstanceType": "m4.2xlarge",
                    "AvailabilityZone": "us-east-1a",
                    "WeightedCapacity": 1
                }
            ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 16,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant",
}
```

Nachdem Sie die `instant`-Flotte mit der vorherigen Konfiguration erstellt haben, werden die folgenden 16 Instances gestartet, um die Zielkapazität zu erreichen:

- 6 `m5.large`-On-Demand-Instances in `us-east-1a` – `m5.large` in `us-east-1a` ist der niedrigste Preis, und es gibt fünf verfügbare ungenutzte `m5.large`-Kapazitätsreservierungen. Die Kapazitätsreservierungen werden zuerst verwendet, um 5 On-Demand-Instances zu starten. Nachdem die verbleibenden `m4.xlarge`- und `m4.2xlarge`-Kapazitätsreservierungen genutzt werden, um die Zielkapazität zu erreichen, wird eine zusätzliche On-Demand-Instance gemäß der On-Demand-Zuordnungsstrategie gestartet, die in diesem Beispiel `lowest-price` ist.
- 5 `m4.xlarge` On-Demand-Instances in `us-east-1a` – `m4.xlarge` in `us-east-1a` ist der zweitniedrigste Preis, und es gibt fünf verfügbare ungenutzte `m4.xlarge`-Kapazitätsreservierungen
- 5 `m4.2xlarge` On-Demand-Instances in `us-east-1a` – `m4.2xlarge` in `us-east-1a` ist der drittniedrigste Preis, und es gibt fünf verfügbare ungenutzte `m4.2xlarge`-Kapazitätsreservierungen

Nach dem Start der Flotte können Sie nachsehen, wie viele ungenutzte Kapazitätsreservierungen noch übrig sind. describe-capacity-reservations In diesem Beispiel sollte die folgende Antwort angezeigt werden, die zeigt, dass alle Kapazitätsreservierungen in allen Pools verwendet wurden.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 0
}
```

Beispiel 6: Starten von On-Demand-Instances mithilfe von Ziel-Kapazitätsreservierungen

Sie können eine Flotte so konfigurieren, dass sie `targeted`-On-Demand-Kapazitätsreservierungen zuerst beim Start von On-Demand-Instances verwendet, indem Sie die Nutzungsstrategie für Kapazitätsreservierungen auf `use-capacity-reservations-first` festlegen. In diesem Beispiel wird gezeigt, wie On-Demand-Instances in `targeted`-Kapazitätsreservierungen, bei denen die Attribute der Kapazitätsreservierungen mit Ausnahme ihrer Availability Zones (`us-east-1a` und `us-east-1b`) gleich sind. Außerdem wird veranschaulicht, wie die Flotte die Instance-Pools auswählt, in denen On-Demand-Instances gestartet werden sollen, wenn die gesamte Zielkapazität die Anzahl der verfügbaren ungenutzten Kapazitätsreservierungen überschreitet.

In diesem Beispiel sieht die Flottenkonfiguration wie folgt aus:

- Zielkapazität: 10 On-Demand-Instances
- Nicht verwendete `targeted`-Kapazitätsreservierungen: 6 (geringer als die On-Demand-Zielkapazität der Flotte von 10 On-Demand-Instances)
- Anzahl der Kapazitätsreservierungspools: 2 (`us-east-1a` und `us-east-1b`)

- Anzahl der Kapazitätsreservierungen pro Pool: 3
- On-Demand-Zuordnungsstrategie: `lowest-price` (Wenn die Anzahl der nicht genutzten Kapazitätsreservierungen kleiner als die On-Demand-Zielkapazität ist, bestimmt die Flotte die Pools, in denen die verbleibende On-Demand-Kapazität basierend auf der On-Demand-Zuordnungsstrategie gestartet werden soll.)

  Beachten Sie, dass Sie auch die `prioritized`-Zuordnungsstrategie anstelle der `lowest-price`-Zuordnungsstrategie verwenden können.

Einen Walkthrough zu den Verfahren, die Sie ausführen müssen, um dieses Beispiel zu erreichen, finden Sie unter Tutorial: EC2 Fleet so konfigurieren, dass On-Demand Instances mit gezielten Kapazitätsreservierungen gestartet werden.

Kapazitätsreservierungen

Das Konto hat die folgenden 6 nicht verwendeten Kapazitätsreservierungen in 2 verschiedenen Pools. In diesem Beispiel unterscheiden sich die Pools durch ihre Availability Zones. Die Anzahl der Kapazitätsreservierungen in jedem Pool wird durch `AvailableInstanceCount` angezeigt.


```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1b",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```


Flottenkonfiguration

Die folgende Flottenkonfiguration zeigt nur die relevanten Konfigurationen für dieses Beispiel. Die gesamte Zielkapazität beträgt 10 und der Standardzielkapazitätstyp ist `on-demand`. Die On-Demand-Zuordnungsstrategie ist `lowest-price`. Die Nutzungsstrategie für Kapazitätsreservierungen ist `use-capacity-reservations-first`.

In diesem Beispiel ist der On-Demand-Instance-Preis für `c5.xlarge` in `us-east-1` 0,17 USD pro Stunde.

> **Note**
>
> Der Flottentyp muss `instant` sein. Andere Flotten-Typen unterstützen `use-capacity-reservations-first` nicht.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
```

```
    },
    "Type": "instant"
}
```

Nachdem Sie die `instant`-Flotte mit der vorherigen Konfiguration erstellt haben, werden die folgenden 10 Instances gestartet, um die Zielkapazität zu erreichen:

- Die Kapazitätsreservierungen werden zuerst verwendet, um 6 On-Demand-Instances wie folgt zu starten:
  - 3 On-Demand-Instances werden in die 3 `c5.xlarge` `targeted`Kapazitätsreservierungen in `us-east-1a` gestartet
  - 3 On-Demand-Instances werden in die 3 `c5.xlarge` `targeted`Kapazitätsreservierungen in `us-east-1b` gestartet
- Um die Zielkapazität zu erreichen, werden 4 zusätzliche On-Demand-Instances gemäß der On-Demand-Zuordnungsstrategie in die reguläre On-Demand-Strategie gestartet, die in diesem Beispiel `lowest-price` ist. Da die Pools jedoch denselben Preis haben (da der Preis pro Region und nicht pro Availability Zone ist), startet die Flotte die restlichen 4 On-Demand-Instances in einem der Pools.

Nach dem Start der Flotte können Sie nachsehen, wie viele ungenutzte Kapazitätsreservierungen noch übrig sind. describe-capacity-reservations In diesem Beispiel sollte die folgende Antwort angezeigt werden, die zeigt, dass alle Kapazitätsreservierungen in allen Pools verwendet wurden.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}
```

Beispiel 7: Konfigurieren des Kapazitätsneuausgleichs, um Ersatz-Spot-Instances zu starten

Im folgenden Beispiel wird die EC2 Flotte so konfiguriert, dass sie eine Ersatz-Spot-Instance startet, wenn Amazon eine Neugewichtsempfehlung für eine Spot-Instance in der Flotte EC2 ausgibt. Um die automatische Ersetzung von Spot-Instances zu konfigurieren, geben Sie für `ReplacementStrategy` `launch-before-terminate` an. Um die Zeitverzögerung vom Start der neuen Ersatz-Spot-Instances bis zum automatischen Löschen der alten Spot-Instances zu konfigurieren, geben Sie für `termination-delay` einen Wert in Sekunden an. Weitere Informationen finden Sie unter Konfigurationsoptionen.

> **Note**
>
> Wir empfehlen die Verwendung von `launch-before-terminate` nur wenn Sie vorhersagen können, wie lange Ihre Verfahren zum Herunterfahren der Instances dauern werden, damit die alten Instances erst beendet werden, nachdem diese Verfahren abgeschlossen sind. Ihnen werden alle Instances in Rechnung gestellt, während sie ausgeführt werden.

Die Effektivität der Strategie zum Kapazitätsausgleich hängt von der Anzahl der Spot-Kapazitätspools ab, die in der Flottenanfrage angegeben sind. EC2 Wir empfehlen, dass Sie die Flotte mit einem diversifizierten Satz von Instance-Typen und Availability Zones konfigurieren und für `AllocationStrategy` `capacity-optimized` angeben. Weitere Informationen darüber, was Sie bei der Konfiguration einer EC2 Flotte für den Kapazitätsausgleich beachten sollten, finden Sie unter. Den Kapazitätsausgleich in der EC2-Flotte und der Spot-Flotte verwenden, um gefährdete Spot Instances zu ersetzen

```
{
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "LaunchTemplate",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "c3.large",
```

```
                        "WeightedCapacity": 1,
                         "Placement": {
                            "AvailabilityZone": "us-east-1a"
                        }
                    },
                    {
                        "InstanceType": "c4.large",
                        "WeightedCapacity": 1,
                         "Placement": {
                            "AvailabilityZone": "us-east-1a"
                        }
                    },
                    {
                        "InstanceType": "c5.large",
                        "WeightedCapacity": 1,
                         "Placement": {
                            "AvailabilityZone": "us-east-1a"
                        }
                    }
                ]
          }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
}
```

Beispiel 8: Starten von Spot Instances in einer kapazitätsoptimierten Flotte

Das folgende Beispiel zeigt, wie Sie eine EC2 Flotte mit einer Spot-Zuweisungsstrategie konfigurieren, die die Kapazität optimiert. Um die Kapazität zu optimieren, müssen Sie `AllocationStrategy` auf `capacity-optimized` festlegen.

Im folgenden Beispiel geben die drei Startspezifikationen drei Spot-Kapazitätspools an. Die Zielkapazität beträgt 50 Spot-Instances. Die EC2 Flotte versucht, 50 Spot-Instances im Spot-Kapazitätspool mit optimaler Kapazität für die Anzahl der Instances, die gestartet werden, zu starten.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           }
                       }
                   ]
           }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"

    }
}
```

Beispiel 9: Starten von Spot Instances in einer kapazitätsoptimierten Flotte mit Prioritäten

Das folgende Beispiel zeigt, wie Sie eine EC2 Flotte mit einer Spot-Zuweisungsstrategie konfigurieren, die die Kapazität optimiert und gleichzeitig die Priorität nach bestem Wissen nutzt.

Bei Verwendung der `capacity-optimized-prioritized`-Zuweisungsstrategie können Sie den `Priority`-Parameter verwenden, um die Prioritäten der Spot-Kapazitätspools anzugeben. Je niedriger die Zahl ist, desto höher ist die Priorität. Sie können die gleiche Priorität auch für mehrere Spot-Kapazitätspools festlegen, wenn sie für Sie die gleiche Priorität haben. Wenn Sie keine Priorität für einen Pool festlegen, wird für den Pool die niedrigste Priorität angenommen.

Um Spot-Kapazitätspools zu priorisieren, müssen Sie auf einstellen. `AllocationStrategy` `capacity-optimized-prioritized` EC2 Fleet optimiert zunächst die Kapazität, berücksichtigt die Prioritäten jedoch nach bestem Wissen und Gewissen (z. B. wenn die Einhaltung der Prioritäten die Fähigkeit von EC2 Fleet, optimale Kapazität bereitzustellen, nicht wesentlich beeinträchtigt). Dies ist eine gute Option für Workloads, bei denen die Möglichkeit von Unterbrechungen minimiert werden muss und die Präferenz für bestimmte Instance-Typen wichtig ist.

Im folgenden Beispiel geben die drei Startspezifikationen drei Spot-Kapazitätspools an. Jeder Pool wird priorisiert. Je niedriger die Zahl ist, desto höher ist die Priorität. Die Zielkapazität beträgt 50 Spot-Instances. Die EC2 Flotte versucht, nach bestem Wissen und Gewissen 50 Spot-Instances in den Spot-Kapazitätspool mit der höchsten Priorität aufzunehmen, optimiert jedoch zuerst die Kapazität.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                        {
                           "InstanceType": "r4.2xlarge",
                           "Priority": 1,
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
```

```
                    },
                     {
                         "InstanceType": "m4.2xlarge",
                         "Priority": 2,
                         "Placement": {
                             "AvailabilityZone": "us-west-2b"
                         },
                     },
                     {
                         "InstanceType": "c5.2xlarge",
                         "Priority": 3,
                         "Placement": {
                             "AvailabilityZone": "us-west-2b"
                         }
                     }
                ]
            }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"
}
```

Beispiel 10: Starten Sie Spot-Instances in einer Flotte price-capacity-optimized

Das folgende Beispiel zeigt, wie eine EC2 Flotte mit einer Spot-Zuweisungsstrategie konfiguriert wird, die sowohl die Kapazität als auch den niedrigsten Preis optimiert. Um die Kapazität zu optimieren und gleichzeitig den Preis zu berücksichtigen, müssen Sie den Spot `AllocationStrategy` auf `price-capacity-optimized` setzen.

Im folgenden Beispiel geben die drei Startspezifikationen drei Spot-Kapazitätspools an. Die Zielkapazität beträgt 50 Spot-Instances. Die EC2 Flotte versucht, 50 Spot-Instances mit optimaler Kapazität für die Anzahl der Instances, die gestartet werden, in den Spot-Kapazitätspool aufzunehmen und gleichzeitig den Pool mit dem niedrigsten Preis auszuwählen.

```
{
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized",
        "MinTargetCapacity": 2,
        "SingleInstanceType": true
```

```
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           }
                       }
                  ]
           }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 50,
        "OnDemandTargetCapacity":0,
        "SpotTargetCapacity":50,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Beispiel 11: Konfigurieren von attributbasierter Auswahl von Instance-Typen

Das folgende Beispiel zeigt, wie eine EC2 Flotte so konfiguriert wird, dass sie die attributbasierte Instance-Typauswahl zur Identifizierung von Instance-Typen verwendet. Um die erforderlichen Instance-Attribute anzugeben, geben Sie die Attribute in der `InstanceRequirements`-Struktur an.

Im folgenden Beispiel werden zwei Instance-Attribute angegeben:

- `VCpuCount`— Ein Minimum von 2 v CPUs ist angegeben. Da kein Maximum angegeben ist, gibt es keine Höchstgrenze.
- `MemoryMiB` – Es werden mindestens 4 MiB Arbeitsspeicher angegeben. Da kein Maximum angegeben ist, gibt es keine Höchstgrenze.

Alle Instance-Typen mit 2 oder mehr v CPUs und 4 MiB oder mehr Speicher werden identifiziert. Aus Gründen des Preisschutzes und der Zuweisungsstrategie könnten jedoch einige Instance-Typen ausgeschlossen werden, wenn EC2 Fleet die Flotte bereitstellt.

Eine Liste und Beschreibungen aller möglichen Attribute, die Sie angeben können, finden Sie InstanceRequirementsin der Amazon EC2 API-Referenz.

```
{
 "SpotOptions": {
  "AllocationStrategy": "price-capacity-optimized"
 },
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }],
 "TargetCapacitySpecification": {
```

```
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
 },
 "Type": "instant"
}
```

Beispiel für CLI-Konfigurationen der Spot-Flotte

Sie können Ihre Spot-Flottenkonfiguration in einer JSON-Datei definieren und dann mithilfe des request-spot-fleet AWS CLI Befehls auf diese Datei verweisen, um Ihre Flotte wie folgt zu erstellen:

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://file_name.json
```

Die folgenden Beispiele veranschaulichen Startkonfigurationen für verschiedene Anwendungsfälle von Spot-Flotte. Weitere Informationen zu den Konfigurationsparametern finden Sie unter request-spot-fleet. Weitere Informationen zum Erstellen einer Spot-Flotte finden Sie unter Erstellen einer Spot-Flotte.

> **Note**
>
> Für eine Spot-Flotte können Sie in einer Startvorlage oder Startspezifikation keine Netzwerkschnittstellen-ID angeben. Achten Sie darauf, dass Sie den `NetworkInterfaceID`-Parameter in Ihrer Startvorlage oder -spezifikation weglassen.

Beispiele

- Beispiel 1: Spot Instances mit der kostengünstigsten Availability Zone in der Region starten
- Beispiel 2: Spot Instances mit der kostengünstigsten Availability Zone aus einer Liste starten
- Beispiel 3: Spot Instances mit dem kostengünstigsten Instance-Typ aus einer Liste starten
- Beispiel 4. Außerkraftsetzen des Preises für die Anforderung
- Beispiel 5: Starten einer Spot-Flotte mit der diversifizierten Zuweisungsstrategie
- Beispiel 6: Starten einer Spot-Flotte mit Instance-Gewichtung
- Beispiel 7: Eine Spot-Flotte mit On-Demand-Kapazität starten
- Beispiel 8: Konfigurieren des Kapazitätsneuausgleichs, um den Ersatz Spot-Instances zu starten
- Beispiel 9: Starten von Spot-Instances in einer kapazitätsoptimierten Flotte
- Beispiel 10: Starten von Spot-Instances in einer kapazitätsoptimierten Flotte mit Prioritäten

- Beispiel 11: Spot Instances in einer priceCapacityOptimized-Flotte starten
- Beispiel 12: Konfigurieren von attributbasierter Auswahl von Instance-Typen

Beispiel 1: Spot Instances mit der kostengünstigsten Availability Zone in der Region starten

Das folgende Beispiel gibt eine einzelne Startspezifikation ohne eine Availability Zone oder ein Subnetz an. Die Spot-Flotte startet die Instances in der kostengünstigsten Availability Zone mit einem Standard-Subnetz. Der Preis, den Sie zahlen, wird den On-Demand-Preis nicht überschreiten.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Beispiel 2: Spot Instances mit der kostengünstigsten Availability Zone aus einer Liste starten

Die folgenden Beispiele geben zwei Startspezifikationen mit verschiedenen Availability Zones oder Subnetzen, aber demselben Instance-Typ und AMI an.

Availability Zones

Die Spot-Flotte startet die Instances in dem Standard-Subnetz der kostengünstigsten Availability Zone, die Sie angegeben haben.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "Placement": {
              "AvailabilityZone": "us-west-2a, us-west-2b"
          },
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Subnets

Sie können Standardsubnetze oder nicht standardmäßige Subnetze angeben. Die nicht standardmäßigen Subnetze können zu einer Standard-VPC oder einer nicht standardmäßigen VPC gehören. Der Spot-Service startet die Instances in dem Subnetz in der kostengünstigsten Availability Zone.

Sie können in einer Spot-Flotten-Anforderung nicht verschiedene Subnetze in derselben Availability Zone angeben.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
```

```
                "GroupId": "sg-1a2b3c4d"
            }
        ],
        "InstanceType": "m3.medium",
        "SubnetId": "subnet-a61dafcf, subnet-65ea5f08",
        "IamInstanceProfile": {
            "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
        }
    }
  ]
}
```

Wenn die Instances in einer Standard-VPC gestartet werden, erhalten sie standardmäßig eine öffentliche IPv4 Adresse. Wenn die Instances in einer nicht standardmäßigen VPC gestartet werden, erhalten sie standardmäßig keine öffentliche IPv4 Adresse. Verwenden Sie eine Netzwerkschnittstelle in der Startspezifikation, um Instances, die in einer nicht standardmäßigen VPC gestartet wurden, eine öffentliche IPv4 Adresse zuzuweisen. Wenn Sie eine Netzwerkschnittstelle angeben, müssen Sie die Subnetz-ID und die Sicherheitsgruppen-ID mithilfe der Netzwerkschnittstelle angeben.

```
  ...
    {
        "ImageId": "ami-1a2b3c4d",
        "KeyName": "my-key-pair",
        "InstanceType": "m3.medium",
        "NetworkInterfaces": [
            {
                "DeviceIndex": 0,
                "SubnetId": "subnet-1a2b3c4d",
                "Groups": [ "sg-1a2b3c4d" ],
                "AssociatePublicIpAddress": true
            }
        ],
        "IamInstanceProfile": {
            "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
        }
    }
  ...
```

Beispiel 3: Spot Instances mit dem kostengünstigsten Instance-Typ aus einer Liste starten

Die folgenden Beispiele geben zwei Startkonfigurationen mit verschiedenen Instance-Typen, aber demselben AMI sowie derselben Availability Zone bzw. demselben Subnetz an. Die Spot-Flotte startet die Instances mit dem angegebenen Instance-Typ mit dem niedrigsten Preis.

Availability Zone

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "c5.4xlarge",
          "Placement": {
            "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "r3.8xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
  ]
}
```

Subnetz

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "c5.4xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "r3.8xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      }
  ]
}
```

Beispiel 4. Außerkraftsetzen des Preises für die Anforderung

Es wird empfohlen, den Standard-Höchstpreis zu verwenden, bei dem es sich um den On-Demand-Preis handelt. Wenn Sie es vorziehen, können Sie einen Höchstpreis für die Flottenanforderung und Höchstpreise für einzelne Startspezifikationen angeben.

Die folgenden Beispiele geben einen Höchstpreis für die Flottenanforderung und Höchstpreise für zwei oder drei Startspezifikationen an. Der Höchstpreis für die Flottenanforderung wird für alle Startspezifikationen verwendet, die keinen Höchstpreis angeben. Die Spot-Flotte startet die Instances mit dem Instance-Typ mit dem niedrigsten Preis.

Availability Zone

```
{
  "SpotPrice": "1.00",
```

```
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "SpotPrice": "0.10"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.4xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "SpotPrice": "0.20"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.8xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
    ]
}
```

Subnetz

```
{
  "SpotPrice": "1.00",
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "SpotPrice": "0.10"
      },
      {
```

```
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.4xlarge",
            "SubnetId": "subnet-1a2b3c4d",
            "SpotPrice": "0.20"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.8xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

Beispiel 5: Starten einer Spot-Flotte mit der diversifizierten Zuweisungsstrategie

Im folgenden Beispiel wird die Zuweisungsstrategie `diversified` verwendet. Die Startspezifikationen weisen verschiedene Instance-Typen, aber dasselbe AMI sowie dieselbe Availability Zone bzw. dasselbe Subnetz auf. Die Spot-Flotte verteilt die 30 Instances auf die drei Startspezifikationen, sodass 10 Instances von jedem Typ vorhanden sind. Weitere Informationen finden Sie unter Verwenden Sie Zuweisungsstrategien, um festzustellen, wie die EC2-Flotte oder Spot-Flotte die Spot- und On-Demand-Kapazitäten ausfüllt.

Availability Zone

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "m3.2xlarge",
```

```
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        }
    ]
}
```

Subnetz

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

Eine bewährte Methode, um die Wahrscheinlichkeit zu erhöhen, dass eine Spot-Anfrage bei einem Ausfall in einer der Availability Zones durch EC2 Kapazität erfüllt werden kann, besteht darin, die einzelnen Zonen zu diversifizieren. Für dieses Szenario müssen Sie jede verfügbare Availability Zone

in die Startspezifikation einfügen. Und anstatt jedes Mal dasselbe Subnetz zu verwenden, sollten Sie drei eindeutige Subnetze verwenden (die jeweils einer anderen Zone zugeordnet sind).

Availability Zone

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2a"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "m3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2c"
          }
      }
  ]
}
```

Subnetz

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
```

```
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-2a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-3a2b3c4d"
        }
    ]
}
```

Beispiel 6: Starten einer Spot-Flotte mit Instance-Gewichtung

Die folgenden Beispiele verwenden die Instance-Gewichtung, d. h. der Preis versteht sich pro Einheitsstunde anstatt pro Instance-Stunde. Jede Startkonfigurationen listet einen anderen Instance-Typ und eine andere Gewichtung auf. Die Spot-Flotte wählt den Instance-Typ mit dem niedrigsten Preis pro Einheitsstunde aus. Die Spot-Flotte berechnet die Anzahl der zu startenden Spot-Instances, indem die Zielkapazität durch die Instance-Gewichtung dividiert wird. Wenn es sich beim Ergebnis nicht um eine Ganzzahl handelt, rundet die Spot-Flotte es auf die nächste Ganzzahl auf, damit die Größe Ihrer Flotte nicht unter der Zielkapazität liegt.

Wenn die `r3.2xlarge`-Anforderung erfolgreich ist, stellt Spot 4 dieser Instances bereit. 20 geteilt durch 6 ergibt insgesamt 3,33 Instances; dies wird auf 4 Instances aufgerundet.

Wenn die `c3.xlarge`-Anforderung erfolgreich ist, stellt Spot 7 dieser Instances bereit. 20 geteilt durch 3 ergibt insgesamt 6,66 Instances; dies wird auf 7 Instances aufgerundet.

Weitere Informationen finden Sie unter Instance-Gewichtung verwenden, um die Kosten und die Leistung Ihrer EC2-Flotte oder Spot-Flotte zu verwalten.

Availability Zone

```
{
  "SpotPrice": "0.70",
```

```
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "WeightedCapacity": 6
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "WeightedCapacity": 3
      }
    ]
}
```

Subnetz

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "WeightedCapacity": 6
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "WeightedCapacity": 3
      }
  ]
}
```

Beispiel 7: Eine Spot-Flotte mit On-Demand-Kapazität starten

Um sicherzustellen, dass Sie immer über Instance-Kapazität verfügen, können Sie eine Anforderung nach On-Demand-Kapazität in Ihre Spot-Flotten-Anforderung aufnehmen. Wenn Kapazität vorhanden ist, ist die On-Demand-Anfrage immer erfüllt. Der Saldo der Zielkapazität wird als Spot erfüllt, wenn Kapazität und Verfügbarkeit vorhanden sind.

Das folgende Beispiel gibt die gewünschte Zielkapazität als 10 an, von denen 5 On-Demand-Kapazität sein müssen. Die Spot-Kapazität wird nicht angegeben; sie ergibt sich aus dem Betrag der Zielkapazität abzüglich der On-Demand-Kapazität. Amazon EC2 bringt 5 Kapazitätseinheiten als On-Demand-Version und 5 Kapazitätseinheiten (10-5=5) als Spot-Version auf den Markt, sofern EC2 Amazon-Kapazität und -Verfügbarkeit verfügbar sind.

```
{
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "AllocationStrategy": "lowestPrice",
  "TargetCapacity": 10,
  "SpotPrice": null,
  "ValidFrom": "2018-04-04T15:58:13Z",
  "ValidUntil": "2019-04-04T15:58:13Z",
  "TerminateInstancesWithExpiration": true,
  "LaunchSpecifications": [],
  "Type": "maintain",
  "OnDemandTargetCapacity": 5,
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-0dbb04d4a6cca5ad1",
        "Version": "2"
      },
      "Overrides": [
        {
          "InstanceType": "t2.medium",
          "WeightedCapacity": 1,
          "SubnetId": "subnet-d0dc51fb"
        }
      ]
    }
  ]
}
```

Beispiel 8: Konfigurieren des Kapazitätsneuausgleichs, um den Ersatz Spot-Instances zu starten

Im folgenden Beispiel wird die Spot-Flotte so konfiguriert, dass sie eine Ersatz-Spot-Instance startet, wenn Amazon eine Neugewichtsempfehlung für eine Spot-Instance in der Flotte EC2 ausgibt. Um die automatische Ersetzung von Spot-Instances zu konfigurieren, geben Sie für `ReplacementStrategy` `launch-before-terminate` an. Um die Zeitverzögerung vom Start der neuen Ersatz-Spot-Instances bis zum automatischen Löschen der alten Spot-Instances zu konfigurieren, geben Sie für `termination-delay` einen Wert in Sekunden an. Weitere Informationen finden Sie unter Konfigurationsoptionen.

> **Note**
>
> Wir empfehlen die Verwendung von `launch-before-terminate` nur, wenn Sie vorhersagen können, wie lange Ihre Verfahren zum Herunterfahren der Instances dauern werden. Dadurch wird sichergestellt, dass die alten Instances erst beendet werden, wenn die Verfahren zum Herunterfahren abgeschlossen sind. Ihnen werden alle Instances in Rechnung gestellt, während sie ausgeführt werden.

Die Wirksamkeit der Kapazitätsneuausgleichsstrategie hängt von der Anzahl der in der Spot-Flotten-Anforderung angegebenen Spot-Kapazitätspools ab. Wir empfehlen, dass Sie die Flotte mit einem diversifizierten Satz von Instance-Typen und Availability Zones konfigurieren und für `AllocationStrategy` `capacityOptimized` angeben. Weitere Informationen darüber, was Sie bei der Konfiguration einer Spot-Flotte für einen Kapazitätsneuausgleich beachten sollten, finden Sie unter Den Kapazitätsausgleich in der EC2-Flotte und der Spot-Flotte verwenden, um gefährdete Spot Instances zu ersetzen.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
        "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "LaunchTemplate",
                    "Version": "1"
                },
```

```
                "Overrides": [
                      {
                          "InstanceType": "c3.large",
                          "WeightedCapacity": 1,
                          "Placement": {
                              "AvailabilityZone": "us-east-1a"
                          }
                      },
                      {
                          "InstanceType": "c4.large",
                          "WeightedCapacity": 1,
                          "Placement": {
                              "AvailabilityZone": "us-east-1a"
                          }
                      },
                      {
                          "InstanceType": "c5.large",
                          "WeightedCapacity": 1,
                          "Placement": {
                              "AvailabilityZone": "us-east-1a"
                          }
                      }
                ]
          }
    ],
        "TargetCapacity": 5,
        "SpotMaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
}
```

Beispiel 9: Starten von Spot-Instances in einer kapazitätsoptimierten Flotte

Im folgenden Beispiel wird veranschaulicht, wie eine Spot-Flotte mit einer Spot-Zuweisungsstrategie konfiguriert wird, die die Kapazität optimiert. Um die Kapazität zu optimieren, müssen Sie `AllocationStrategy` auf `capacityOptimized` festlegen.

Im folgenden Beispiel geben die drei Startspezifikationen drei Spot-Kapazitätspools an. Die Zielkapazität beträgt 50 Spot-Instances. Die Spot-Flotte versucht, 50 Spot-Instances in dem Spot-

Kapazitätspool zu starten, der über die optimale Kapazität für die Anzahl der zu startenden Instances verfügt.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "r4.2xlarge",
                    "AvailabilityZone": "us-west-2a"
                },
                {
                    "InstanceType": "m4.2xlarge",
                    "AvailabilityZone": "us-west-2b"
                },
                {
                    "InstanceType": "c5.2xlarge",
                    "AvailabilityZone": "us-west-2b"
                }
            ]
        }
    ]
}
```

Beispiel 10: Starten von Spot-Instances in einer kapazitätsoptimierten Flotte mit Prioritäten

Im folgenden Beispiel wird veranschaulicht, wie eine Spot-Flotte mit einer Spot-Zuweisungsstrategie konfiguriert wird, die die Kapazität optimiert und dabei die Priorität so weit wie möglich berücksichtigt.

Bei Verwendung der `capacityOptimizedPrioritized`-Zuweisungsstrategie können Sie den `Priority`-Parameter verwenden, um die Prioritäten der Spot-Kapazitätspools anzugeben. Je niedriger die Zahl ist, desto höher ist die Priorität. Sie können die gleiche Priorität auch für mehrere

Spot-Kapazitätspools festlegen, wenn sie für Sie die gleiche Priorität haben. Wenn Sie keine Priorität für einen Pool festlegen, wird für den Pool die niedrigste Priorität angenommen.

Um Spot-Kapazitätspools zu priorisieren, müssen Sie `AllocationStrategy` auf `capacityOptimizedPrioritized` festlegen. Die Spot-Flotte wird zuerst für die Kapazität optimiert, berücksichtigt jedoch so gut wie möglich die Prioritäten (wenn z. B. die Berücksichtigung der Prioritäten keinen wesentlichen Einfluss auf die Fähigkeit der Spot-Flotte zur Bereitstellung optimaler Kapazität hat). Dies ist eine gute Option für Workloads, bei denen die Möglichkeit von Unterbrechungen minimiert werden muss und die Präferenz für bestimmte Instance-Typen wichtig ist.

Im folgenden Beispiel geben die drei Startspezifikationen drei Spot-Kapazitätspools an. Jeder Pool wird priorisiert. Je niedriger die Zahl ist, desto höher ist die Priorität. Die Zielkapazität beträgt 50 Spot-Instances. Die Spot-Flotte versucht nach Möglichkeit, 50 Spot-Instances in dem Spot-Kapazitätspool mit der höchsten Priorität zu starten. Zuerst optimiert sie jedoch die Kapazität.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimizedPrioritized"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "r4.2xlarge",
                   "Priority": 1,
                    "AvailabilityZone": "us-west-2a"
                },
                {
                          "InstanceType": "m4.2xlarge",
                          "Priority": 2,
                          "AvailabilityZone": "us-west-2b"
                },
                {
                          "InstanceType": "c5.2xlarge",
                          "Priority": 3,
                          "AvailabilityZone": "us-west-2b"
                }
```

```
            ]
        }
    ]
}
```

Beispiel 11: Spot Instances in einer priceCapacityOptimized-Flotte starten

Im folgenden Beispiel wird veranschaulicht, wie eine Spot-Flotte mit einer Spot-Zuweisungsstrategie konfiguriert wird, die sowohl die Kapazität als auch den Preis optimiert. Um die Kapazität zu optimieren und gleichzeitig den Preis zu berücksichtigen, müssen Sie den Spot `AllocationStrategy` auf `priceCapacityOptimized` setzen.

Im folgenden Beispiel geben die drei Startspezifikationen drei Spot-Kapazitätspools an. Die Zielkapazität beträgt 50 Spot-Instances. Die Spot-Flotte versucht, 50 Spot Instances in dem Spot-Kapazitätspool zu starten, der über die optimale Kapazität für die Anzahl der zu startenden Instances verfügt und gleichzeitig den günstigsten Pool auszuwählen.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "OnDemandAllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111111111111:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "lt-0123456789example",
                    "Version": "1"
                },
                "Overrides": [
                     {
                           "InstanceType": "r4.2xlarge",
                           "AvailabilityZone": "us-west-2a"
                      },
                      {
                           "InstanceType": "m4.2xlarge",
                           "AvailabilityZone": "us-west-2b"
                      },
                      {
                           "InstanceType": "c5.2xlarge",
                           "AvailabilityZone": "us-west-2b"
```

```
                    }
                ]
            }
        ],
        "TargetCapacity": 50,
        "Type": "request"
    }
}
```

Beispiel 12: Konfigurieren von attributbasierter Auswahl von Instance-Typen

Im folgenden Beispiel wird veranschaulicht, wie eine Spot-Flotte so konfiguriert wird, dass sie die attributbasierte Instance-Typauswahl zur Identifizierung von Instance-Typen verwendet. Um die erforderlichen Instance-Attribute anzugeben, geben Sie die Attribute in der `InstanceRequirements`-Struktur an.

Im folgenden Beispiel werden zwei Instance-Attribute angegeben:

- `VCpuCount`— Ein Mindestwert von 2 V CPUs ist angegeben. Da kein Maximum angegeben ist, gibt es keine Höchstgrenze.
- `MemoryMiB` – Es werden mindestens 4 MiB Arbeitsspeicher angegeben. Da kein Maximum angegeben ist, gibt es keine Höchstgrenze.

Alle Instance-Typen mit 2 oder mehr v CPUs und 4 MiB oder mehr Speicher werden identifiziert. Der Preisschutz und die Zuweisungsstrategie könnten jedoch einige Instance-Typen ausschließen, wenn die Spot-Flotte die Flotte bereitstellt.

Eine Liste und Beschreibungen aller möglichen Attribute, die Sie angeben können, finden Sie InstanceRequirementsin der Amazon EC2 API-Referenz.

```
{
 "AllocationStrategy": "priceCapacityOptimized",
 "TargetCapacity": 20,
 "Type": "request",
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
```

```
    "InstanceRequirements": {
     "VCpuCount": {
      "Min": 2
     },
     "MemoryMiB": {
      "Min": 4
     }
    }
   }]
  }]
}
```

Kontingente für EC2 Fleet und Spot-Flotte

Ihr AWS-Konto hat Standardkontingente, früher als Limits bezeichnet, für jeden AWS Service. Sofern nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region.

Die üblichen EC2 Amazon-Kontingente gelten für Instances, die von einer EC2 Flotte oder einer Spot-Flotte gestartet werden, wie z. B. Spot-Instance-Limits und Volumenlimits.

Darüber hinaus gelten für Ihre AWS-Konto EC2 Flotte und Spot-Flotte die folgenden Kontingente:

Quota-Beschreibung	Kontingent
Die Anzahl der EC2 Flotten und Spot-Flotten pro Typregion `maintain` und `request` in den Bundesstaaten `activedeleted_running` , und `cancelled_running`	1 000 [1] [2] [3]
Die Anzahl der EC2 Flotten des Typs `instant`	Unbegrenzt
Die Anzahl der Spot-Kapazitätspools (eindeutige Kombination aus Instance-Typ und Subnetz) für EC2 Flotten und Spot-Flotten des Typs und `maintain` `request`	300 [1]
Die Anzahl der Spot-Kapazitätspools (eindeutige Kombination aus Instance-Typ und Subnetz) für Flotten des Typs EC2 `instant`	Unbegrenzt

Quota-Beschreibung	Kontingent
Größe der Benutzerdaten in einer Startspezifikation	16 KB [2]
Die Zielkapazität pro EC2 Flotte oder Spot-Flotte	10.000
Die Zielkapazität für alle EC2 Flotten und Spot-Flotten in einer Region	100 000 [1]
Eine EC2 Flottenanfrage oder eine Spot-Flottenanfrage kann sich nicht über mehrere Regionen erstrecken.	
Eine EC2 Flotte-Anfrage oder eine Spot-Flotte-Anfrage kann sich nicht über verschiedene Subnetze derselben Availability Zone erstrecken.	

[1] Diese Kontingente gelten sowohl für Ihre EC2 Flotten als auch für Ihre Spot-Flotten.

[2] Dabei handelt es sich um feste Quotas. Sie können keine Erhöhung einiger dieser Quotas beantragen.

[3] Nachdem Sie eine EC2 Flotte gelöscht oder eine Spot-Flotte-Anfrage storniert haben und Sie beim Löschen oder Stornieren der Anfrage angegeben haben, dass die Flotte ihre Spot-Instances nicht beenden soll, wechselt die Flottenanforderung in den Status `deleted_running` (EC2 Fleet) oder `cancelled_running` (Spot-Flotte) und die Instances laufen weiter, bis sie unterbrochen werden oder Sie sie manuell beenden. Wenn Sie die Instances beenden, wechselt die Flottenanforderung in den Status `deleted_terminating` (EC2 Fleet) oder `cancelled_terminating` (Spot-Flotte) und wird nicht auf dieses Kontingent angerechnet. Weitere Informationen erhalten Sie unter Löschen Sie eine EC2 Flottenanfrage und die Instances in der Flotte und Spot-Flotten-Anforderung abbrechen (löschen).

Anfordern einer Quota-Erhöhung für die Zielkapazität

Wenn Sie mehr als diese Standard-Quota für die Zielkapazität benötigen, können Sie eine Quota-Erhöhung anfordern.

So fordern Sie eine Quota-Erhöhung für die Zielkapazität an

1. Öffnen Sie das Formular Support Center Create Case.
2. Wählen Sie Service Limit increase (Erhöhung des Servicelimits).
3. Wählen Sie als Limittyp die Option EC2Flotte aus.
4. Wählen Sie unter Region die AWS Region aus, für die Sie die Erhöhung des Kontingents beantragen möchten.
5. Bei Limit (Limit) wählen Sie Target Fleet Capacity per Fleet (in units) (Zielflottenkapazität pro Flotte (in Einheiten)) oder Target Fleet Capacity per Region (in units) (Zielflottenkapazität pro Region (in Einheiten)) aus, abhängig davon, welche Quota Sie erhöhen möchten.
6. Geben Sie unter New limit value (Neuer Limit-Wert) den neuen Wert ein.
7. Um eine Erhöhung für eine andere Quota anzufordern, wählen Sie Add another request (Weitere Anforderung hinzufügen) aus und wiederholen Sie die Schritte 4 bis 6.
8. Bei Use case description (Beschreibung des Anwendungsfalls) geben Sie Ihren Grund für die Anforderung einer Quota-Erhöhung an.
9. Unter Contact options (Kontakt-Optionen) geben Sie Ihre bevorzugte Kontaktsprache und Kontaktmethode an.
10. Wählen Sie Absenden aus.

Netzwerk in Amazon EC2

Amazon VPC ermöglicht es Ihnen, AWS-Ressourcen wie Amazon EC2-Instances in einem virtuellen Netzwerk für Ihr AWS-Konto zu starten, das als Virtual Private Cloud (VPC) bezeichnet wird. Wenn Sie eine Instance starten, können Sie ein Subnetz aus der VPC auswählen. Die Instance ist mit einer primären Netzwerkschnittstelle konfiguriert, bei der es sich um eine logische virtuelle Netzwerkkarte handelt. Die Instance erhält eine primäre private IP-Adresse von der IPv4-Adresse des Subnetzes und wird der primären Netzwerkschnittstelle zugewiesen.

Sie können steuern, ob die Instance eine öffentliche IP-Adresse aus dem Pool öffentlicher IP-Adressen von Amazon erhält. Die öffentliche IP-Adresse einer Instance wird Ihrer Instance nur zugeordnet, bis sie gestoppt oder beendet wird. Wenn Sie eine dauerhafte öffentliche IP-Adresse benötigen, können Sie Ihrem AWS-Konto eine Elastic IP-Adresse zuweisen und diese mit einer Instance oder einer Netzwerkschnittstelle verknüpfen. Eine Elastic IP-Adresse bleibt mit Ihrem AWS-Konto verknüpft, bis Sie es freigeben. Sie können es bei Bedarf von einer Instance auf eine andere verschieben. Sie können Ihren eigenen IP-Adressbereich in Ihr AWS-Konto bringen, wo er als Adresspool angezeigt wird, und dann Elastic IP-Adressen aus Ihrem Adresspool zuweisen.

Um die Netzwerkleistung zu erhöhen und die Latenz zu reduzieren, können Sie Instances in einer Placement-Gruppe starten. Mithilfe von Enhanced Networking können Sie eine deutlich höhere Paketleistung pro Sekunde (PPS) erzielen. Sie können High-Performance-Computing- und Machine-Learning-Anwendungen mit einem Elastic Fabric Adapter (EFA) beschleunigen. Dies ist ein Netzwerkgerät, das Sie an einen unterstützten Instance-Typ anschließen können.

Feature

- Regionen und Zonen
- IP-Adressierung von Amazon EC2-Instances
- Hostnamen und Domains der EC2-Instance
- Bringen Sie Ihre eigenen IP-Adressen (BYOIP) zu Amazon EC2
- Elastic-IP-Adressen
- Elastic-Network-Schnittstelle
- Netzwerkbandbreite der EC2 Amazon-Instance
- Erweitertes Netzwerk in Amazon-EC2-Instances
- Elastic Fabric Adapter für AI/ML und HPC-Workloads bei Amazon EC2

- EC2 Amazon-Topologie
- Platzierungsgruppen für Ihre Amazon-EC2-Instances
- Netzwerk-MTU (Maximum Transmission Unit) für Ihre EC2-Instance
- Virtual Private Clouds für Ihre EC2-Instances

Regionen und Zonen

Amazon EC2 wird an mehreren Standorten weltweit gehostet. Diese Standorte bestehen aus AWS-Regionen, Availability Zones, Local Zones, AWS Outposts und Wavelength Zones.

- Regionen sind separate geografische Gebiete.
- Availability Zones sind mehrere isolierte Standorte innerhalb jeder Region.
- Local Zones bieten Ihnen die Möglichkeit, Ressourcen wie Rechenleistung und Speicher an mehreren Standorten zu platzieren, die näher an Ihren Endbenutzern liegen.
- Wavelength Zones ermöglichen es, Anwendungen zu erstellen, die extrem niedrige Latenzen für 5G-Geräte und Endbenutzer bereitstellen. Wavelength stellt standardmäßige AWS-Datenverarbeitungs- und -Speicherservices am Edge der 5G-Netze von Telekommunikationsanbietern bereit.
- AWS Outposts bietet native AWS-Services, Infrastruktur und Betriebsmodelle für praktisch jedes Rechenzentrum, jeden Co-Location-Bereich oder jede On-Premises-Einrichtung.

AWS betreibt hochmoderne, hoch verfügbare Rechenzentren. In seltenen Fällen kann es aber zu Ausfällen kommen, die die Verfügbarkeit von Instances desselben Standorts beeinträchtigen. Wenn Sie alle Ihre Instances an einem einzigen Standort hosten, der von einem Ausfall dieser Art betroffen ist, ist keine Ihrer Instances verfügbar.

Weitere Informationen finden Sie unter AWS-Globale Infrastruktur.

Inhalt

- Regionen
- Availability Zones
- Local Zones
- Wavelength-Zones
- AWS Outposts

Regionen

Jede -Region ist darauf ausgelegt, vollständig von den anderen -Regionen getrennt zu sein. Dies sorgt für die größtmögliche Fehlertoleranz und Stabilität.

Wählen Sie beim Starten einer Instance eine Region aus, in der Instances nah an bestimmten Kunden platziert werden oder mit der rechtliche oder andere Anforderungen erfüllt werden. Sie können Instances in mehreren Regionen starten.

Wenn Sie sich Ihre Ressourcen anzeigen lassen, werden nur die Ressourcen angezeigt, die mit der von Ihnen angegebenen Region verknüpft sind. Der Grund hierfür ist, dass die Regionen voneinander isoliert sind und Ressourcen nicht automatisch über unterschiedliche Regionen repliziert werden.

Verfügbare Regionen

Eine Liste der verfügbaren Regionen finden Sie unter AWS-Regionen.

Regionale Endpunkte für Amazon EC2

Wenn Sie über die Befehlszeilenschnittstelle oder über API-Aktionen mit einer Instance arbeiten, müssen Sie ihren regionalen Endpunkt angeben. Weitere Informationen über Regionen und Endpunkte für Amazon EC2 finden Sie unter Amazon-EC2-Service-Endpunkte im Entwicklerhandbuch für Amazon EC2.

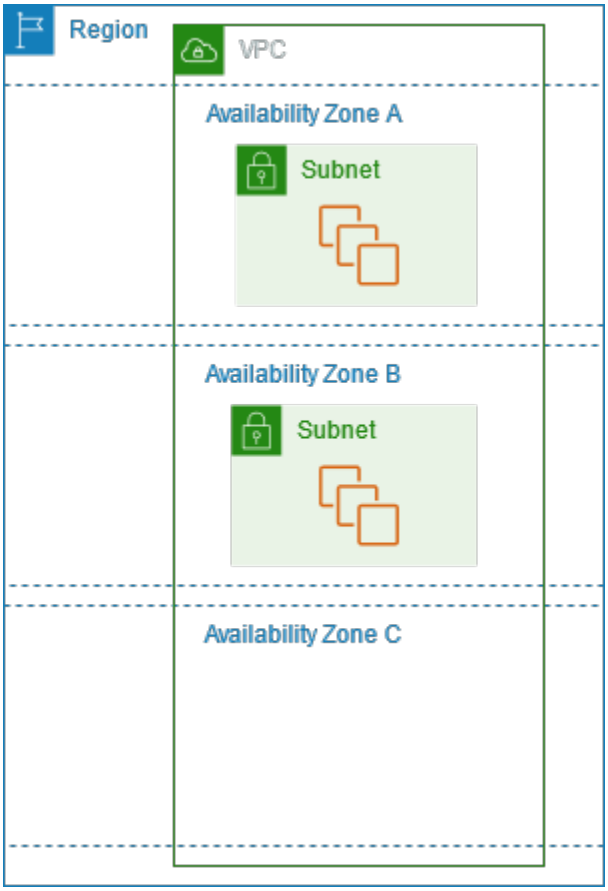
Weitere Informationen finden Sie unter AWS-Regionen im Benutzerhandbuch für AWS-Regionen und Availability Zones.

Availability Zones

Jede Region verfügt über mehrere isolierte Standorte, die als Availability Zones bezeichnet werden. Der Code für eine Availability Zone ist der Regionscode gefolgt von einem Buchstaben als Bezeichner. Beispiel, `us-east-1a`.

Indem Sie EC2-Instances in mehreren Availability Zones starten, können Sie Ihre Anwendungen vor dem Ausfall eines einzelnen Standorts in der Region schützen.

Das folgende Diagramm veranschaulicht mehrere Availability Zones in einer AWS-Region. Availability Zone A und Availability Zone B haben jeweils ein Subnetz, und jedes Subnetz verfügt über EC2-Instances. Availability Zone C hat keine Subnetze, daher können Sie keine Instances in diese Availability Zone starten.



Weitere Informationen finden Sie unter Virtual Private Clouds für Ihre EC2-Instances.

Availability Zones nach Region

Eine Liste der Availability Zones nach Regionen finden Sie unter AWS Availability Zones.

Instances in Availability Zones

Wenn Sie eine Instance starten, wählen Sie eine Region und eine Virtual Private Cloud (VPC) aus. Dann können Sie entweder ein Subnetz aus einer der Availability Zones auswählen oder uns eines für Sie auswählen lassen. Beim Starten Ihrer ersten Instances empfehlen wir, dass Sie uns die beste Availability Zone basierend auf dem Systemzustand und der verfügbaren Kapazität für Sie auswählen lassen. Geben Sie beim Starten weiterer Instances nur dann eine Availability Zone an, wenn die neuen Instances entweder nah bei Ihren laufenden Instances oder getrennt davon sein müssen.

Wenn Sie Instances auf mehrere Availability Zones verteilen, ist es sinnvoll, Ihre Anwendung so zu entwerfen, dass bei einem Ausfall einer Instance die Anforderungen von einer Instance in einer anderen Availability Zone verarbeitet werden können.

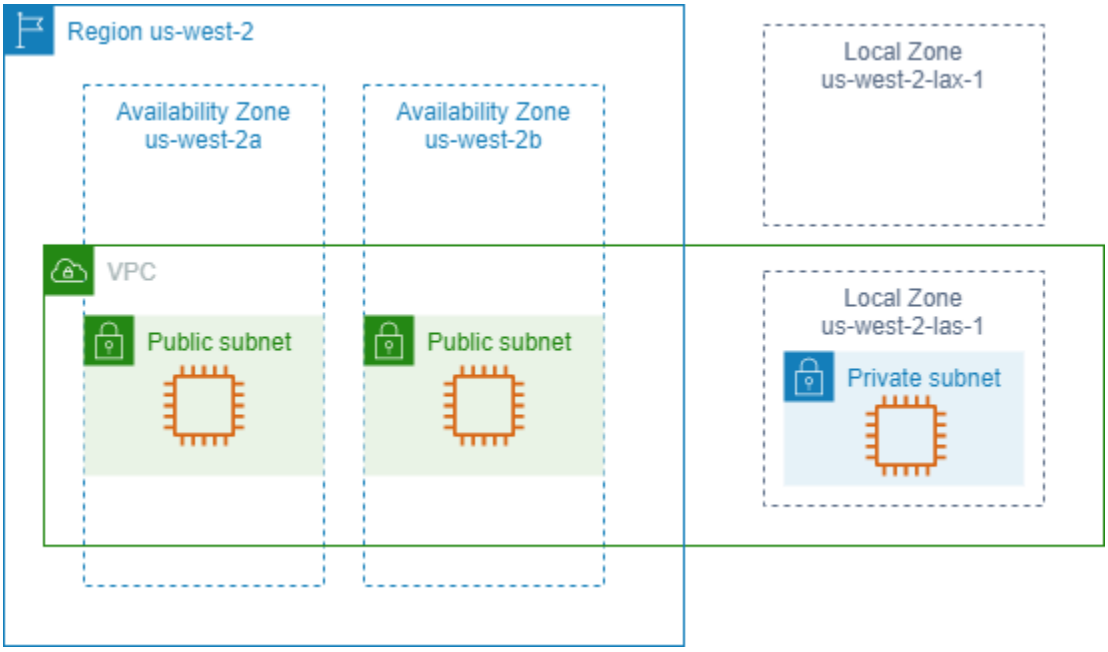
Weitere Informationen finden Sie unter AWS Availability Zones im Benutzerhandbuch für AWS-Regionen und Availability Zones.

Local Zones

Eine Local Zone ist eine Erweiterung einer AWS-Region in geografischer Nähe zu Ihren Benutzern. Local Zones haben ihre eigenen Internetverbindungen und unterstützen Direct Connect. Ressourcen, die in einer lokalen Zone erstellt wurden, können so von lokalen Benutzern mit Netzwerkverbindungen mit geringer Latenz genutzt werden. Weitere Informationen finden Sie unter Was sind AWS Local Zones? im AWS-Benutzerhandbuch zu Local Zones.

Der Code für die lokale Zone wird durch einen Regionscode dargestellt, gefolgt von einer ID, die den physischen Standort angibt. Beispiel: `us-west-2-lax-1` in Los Angeles.

Das folgende Diagramm veranschaulicht die AWS-Region `us-west-2`, zwei ihrer Availability Zones und zwei ihrer lokalen Zonen. Die VPC erstreckt sich über die Availability Zones und eine der lokalen Zonen. Jede Zone in der VPC hat ein Subnetz und jedes Subnetz eine Instance.



Verfügbare Local Zones

Eine Liste der verfügbaren lokalen Zonen finden Sie unter Verfügbare Local Zones im AWS-Benutzerhandbuch für Local Zones. Eine Liste der angekündigten Local Zones finden Sie unter AWS-Local-Zones-Standorte.

Instances in Local Zones

Um eine Local Zone verwenden zu können, müssen Sie diese zunächst aktivieren. Dann erstellen Sie ein Subnetz in der Local Zone. Sie können das Subnetz der Local Zone angeben, wenn Sie Instances starten, wodurch es im Subnetz der Local Zone in der lokalen Zone platziert wird.

Wenn Sie eine Instance in einer Local Zone starten, weisen Sie auch eine IP-Adresse aus einer Netzwerkgrenzgruppe zu. Eine Netzwerkgrenzgruppe ist ein eindeutiger Satz von Availability Zones, Local Zones oder Wavelength Zones, aus denen AWS IP-Adressen ankündigt, zum Beispiel `us-west-2-lax-1a`. Sie können die folgenden IP-Adressen aus einer Netzwerkgrenzgruppe zuweisen:

- Elastische IPv4-Adressen, die von Amazon bereitgestellt werden
- Von Amazon bereitgestellte IPv6-VPC-Adressen (nur in den Zonen von Los Angeles verfügbar)

Weitere Informationen zum Starten einer Instance in einer Local Zone finden Sie unter Erste Schritte mit AWS Local Zones im Benutzerhandbuch zu AWS Local Zones.

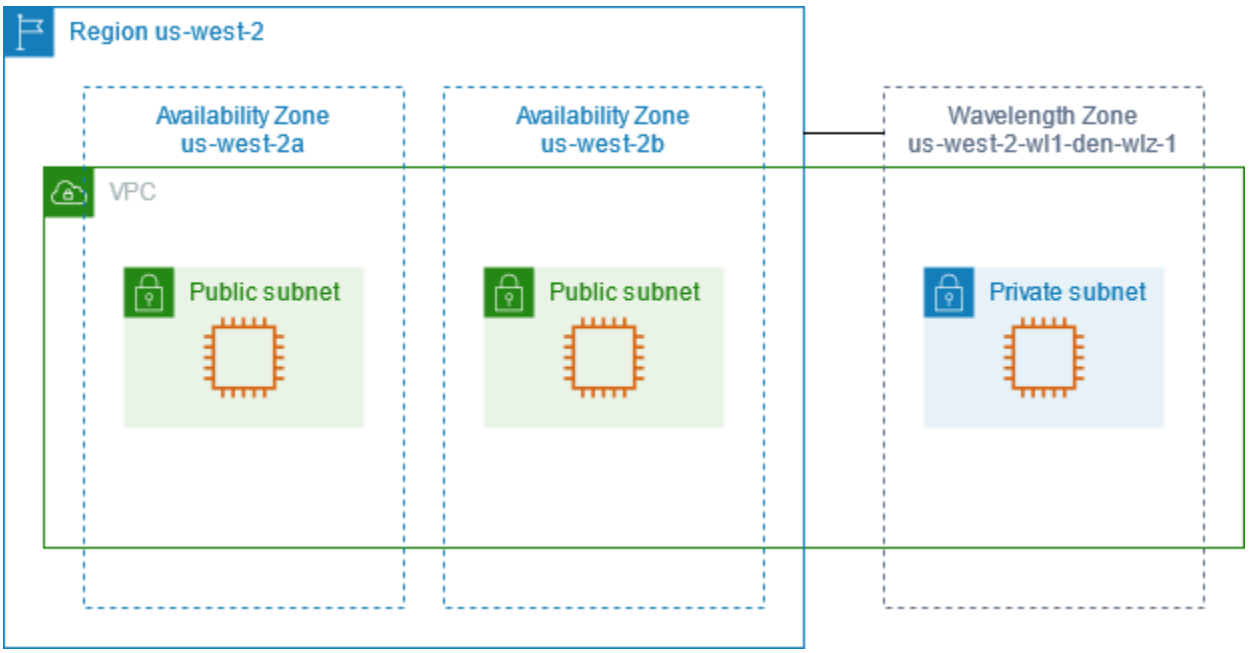
Wavelength-Zones

AWS WavelengthMit können Developer Anwendungen mit ultra-niedriger Latenz für Mobilgeräte und Endbenutzer erstellen. Wavelength stellt standardmäßige AWS-Datenverarbeitungs- und Speicher-Services für die Grenze der 5G-Netze von Telekommunikationsanbietern bereit. Entwickler können eine Virtual Private Cloud (VPC) auf eine oder mehrere Wavelength-Zonen ausweiten und dann AWS-Ressourcen wie Amazon-EC2-Instances verwenden, um Anwendungen auszuführen, die eine extrem niedrige Latenz und eine Verbindung zu AWS-Services in der Region erfordern.

Eine Wavelength-Zone ist eine isolierte Zone am Standort des Carriers, an dem die Wavelength-Infrastruktur bereitgestellt wird. Wavelength Zones sind an eine Region gebunden. Eine Wavelength-Zone ist eine logische Erweiterung einer Region und wird von der Steuerungsebene in der Region verwaltet.

Der Code für die Wavelength-Zone wird durch einen Regionscode dargestellt, gefolgt von einer ID, die den physischen Standort angibt. Beispiel: `us-east-1-wl1-bos-wlz-1` in Boston.

Das folgende Diagramm veranschaulicht die AWS-Region `us-west-2`, zwei ihrer Availability Zones und eine Wavelength-Zone. Die VPC erstreckt sich über die Availability Zones und die Wavelength-Zone. Jede Zone in der VPC hat ein Subnetz und jedes Subnetz eine Instance.



Wavelength Zones sind nicht in jeder Region verfügbar. Weitere Informationen zu den Regionen, die Wavelength Zones unterstützen, finden Sie unter Verfügbare Wavelength Zones im AWS Wavelength Developerhandbuch.

Verfügbare Wavelength Zones

Weitere Informationen zu verfügbaren Wavelength Zones finden Sie unter Verfügbare Wavelength Zones im AWS Wavelength-Entwicklerhandbuch.

Instances in Wavelength Zones

Um eine Wavelength-Zone zu verwenden, müssen Sie sich zunächst für die Zone anmelden. Dann erstellen Sie ein Subnetz in der Wavelength Zone. Sie können das Wavelength-Subnetz angeben, wenn Sie Instances starten. Sie weisen auch eine Carrier-IP-Adresse aus einer Netzwerkgrenzgruppe zu, bei der es sich um einen eindeutigen Satz von Availability Zones, Local Zones oder Wavelength Zones handelt, von denen AWS IP-Adressen präsentiert, zum Beispiel `us-east-1-wl1-bos-wlz-1`.

Weitere Informationen zum Starten einer Instance in einer Wavelength-Zone finden Sie unter Erste Schritte mit AWS Wavelength im AWS Wavelength-Entwicklerhandbuch.

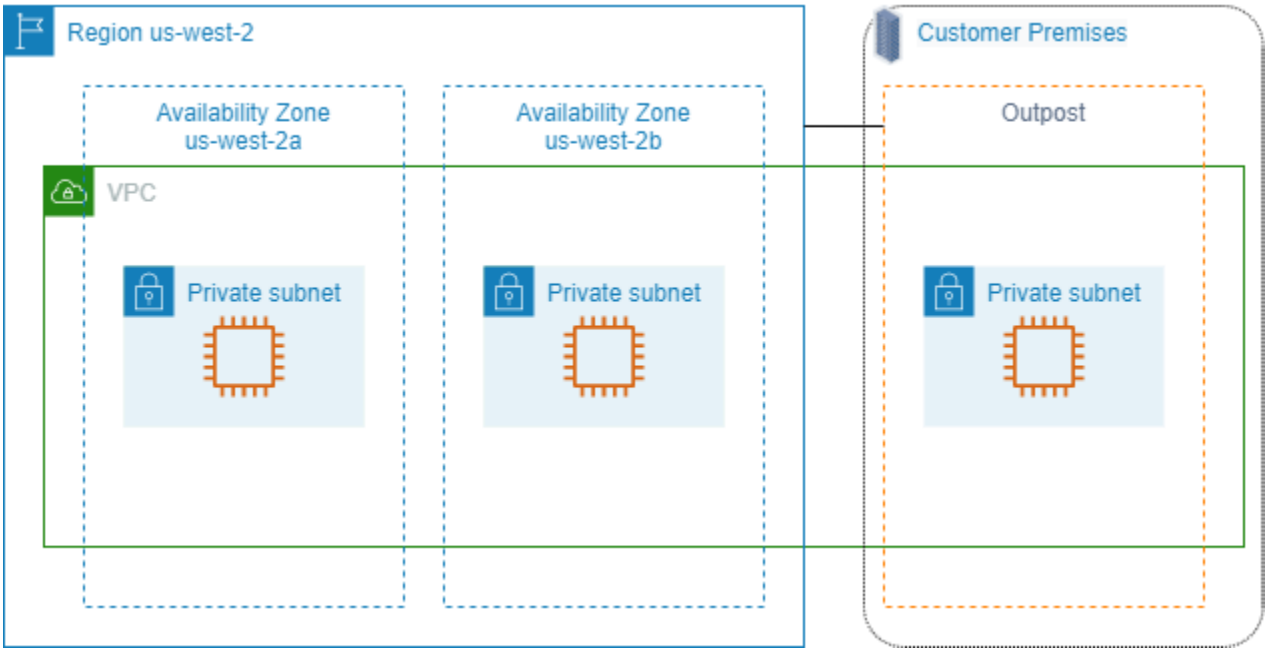
AWS Outposts

AWS Outposts ist ein vollständig verwalteter Service, der AWS-Infrastruktur, Services, APIs und Tools auf Kundenstandorte ausweitet. Durch die Bereitstellung des lokalen Zugriffs auf die von

AWS verwaltete Infrastruktur ermöglicht AWS Outposts Kunden, Anwendungen On-Premises mit denselben Programmierschnittstellen wie in AWS-Regionen zu erstellen und auszuführen, während lokale Datenverarbeitungs- und Speicherressourcen für geringere Latenz und lokale Datenverarbeitungsanforderungen verwendet werden.

Ein Outpost ist ein Pool von AWS-Rechen- und Speicherkapazitäten, die an einem Kundenstandort bereitgestellt werden. AWS betreibt, überwacht und verwaltet diese Kapazität als Teil einer AWS-Region. Sie können Subnetze in Ihrem Outpost erstellen und diese angeben, wenn Sie AWS-Ressourcen erstellen. Instances in Outpost-Subnetzen kommunizieren mit anderen Instances in der AWS-Region mithilfe privater IP-Adressen, sämtlich innerhalb derselben VPC.

Das folgende Diagramm veranschaulicht die AWS-Region `us-west-2`, zwei ihrer Availability Zones und einen Outpost. Die VPC erstreckt sich über die Availability Zones und den Outpost. Der Outpost befindet sich in einem On-Premises Kundenrechenzentrum. Jede Zone in der VPC hat ein Subnetz und jedes Subnetz eine Instance.



Starten von Instances in einem Outpost

Um mit der Verwendung von AWS Outposts zu beginnen, müssen Sie einen Outpost erstellen und die Outpost-Kapazität bestellen. AWS Outposts bietet zwei Formfaktoren: Outposts-Racks und Outposts-Server. Weitere Informationen zu Outpost-Konfigurationen finden Sie in AWS Outposts-Familie. Nach der Installation Ihres Outpost-Equipments steht Ihnen die Datenverarbeitungs- und Speicherkapazität zur Verfügung, wenn Sie Amazon-EC2-Instances in Ihrem Outpost starten.

Um EC2-Instances zu starten, müssen Sie ein Outpost-Subnetz erstellen. Sicherheitsgruppen steuern den eingehenden und ausgehenden VPC-Datenverkehr für Instances in einem Outpost-Subnetz genauso wie für Instances in einem Availability-Zone-Subnetz. Um eine Verbindung zu Instances in Outpost-Subnetzen mit SSH herzustellen, geben Sie beim Starten der Instance ein Schlüsselpaar an, genauso wie bei Instances in einem Availability-Zone-Subnetz.

Weitere Informationen finden Sie unter Erste Schritte mit Outposts-Racks oder Erste Schritte mit Outposts-Servern.

Volumes in einem Outposts-Rack

Wenn sich Ihre Dantenverabeitungskapazität in einem Outpost-Rack befindet, können Sie EBS-Volumes in dem Outpost-Subnetz erstellen, das Sie erstellt haben. Wenn Sie das Volume erstellen, geben Sie den Amazon-Ressourcennamen (ARN) des Outposts an.

Der folgende Befehl create-volume erstellt ein leeres 50 GB-Volume auf dem angegebenen Outpost.

```
aws ec2 create-volume --availability-zone us-east-2a --outpost-arn arn:aws:outposts:us-east-2:123456789012:outpost/op-03e6fecad652a6138 --size 50
```

Sie können die Größe Ihres Amazon EBS gp2-Volumes dynamisch ändern, ohne sie zu trennen. Weitere Informationen zum Ändern eines Volumes ohne es abzuhängen finden Sie unter Anfordern von Änderungen an Ihren EBS-Volumes im Amazon-EBS-Benutzerhandbuch.

Wir empfehlen, das Root-Volume für eine Instance in einem Outpost-Rack auf 30 GiB oder kleiner zu beschränken. Sie können Daten-Volumes in der Blockgeräte-Zuweisung des AMI oder der Instance angeben, um zusätzlichen Speicher bereitzustellen. Informationen zum Begrenzen nicht verwendeter Blöcke vom Boot-Volume finden Sie unter So erstellen Sie Sparse-EBS-Volumes im AWS-Partner-Netzwerk-Blog.

Es wird empfohlen, das NVMe-Timeout für das Root-Volume zu erhöhen. Weitere Informationen finden Sie unter E/A-Betriebs-Timeout im Amazon-EBS-Benutzerhandbuch.

Volumes in einem Outposts-Server

Instances in Outposts-Servern enthalten Instance-Speicher-Volumes, unterstützen jedoch keine EBS-Volumes. Wählen Sie ein Amazon-EBS-gestütztes AMI mit nur einem EBS-Snapshot. Wählen Sie eine ausreichende Instance-Speicher-Größe, um die Anforderungen Ihrer Anwendung zu erfüllen. Weitere Informationen finden Sie unter Limits für Instance-Speicher-Volumes.

IP-Adressierung von Amazon EC2-Instances

Amazon EC2 und Amazon VPC unterstützen sowohl die IPv4- als auch IPv6-Adressierungsprotokolle. Standardmäßig verwendet Amazon VPC das IPv4-Adressierungsprotokoll; dieses Verhalten lässt sich nicht deaktivieren. Wenn Sie eine VPC erstellen, müssen Sie einen IPv4 CIDR-Block (einen privaten IPv4-Adressenbereich) angeben. Optional können Sie Ihrer VPC und einen IPv6-CIDR-Block zuordnen und den Instances in Ihrem Subnetz IPv6-Adressen von diesem Block zuweisen.

Wenn Sie eine EC2-Instance starten, können Sie eine VPC und ein Subnetz angeben. Die Instance erhält eine private IPv4-Adresse aus dem CIDR-Bereich des Subnetzes. Sie können Ihre Instances optional mit öffentlichen IPv4-Adressen und IPv6-Adressen konfigurieren. Wenn EC2-Instances in verschiedenen VPCs über öffentliche IP-Adressen kommunizieren, bleibt der Datenverkehr im AWS privaten globalen Netzwerk und durchquert nicht das öffentliche Internet.

Inhalt

- Private IPv4-Adressen
- Öffentliche IPv4-Adressen
- Optimierung von öffentlichen IPv4-Adressen
- IPv6-Adressen
- Mehrere IP-Adressen
- Hostnamen der EC2-Instance
- Link-lokale Adressen
- Arbeiten mit den IPv4-Adressen für Ihre EC2-Instances
- Die IPv6-Adressen für Ihre EC2-Instances verwalten
- Sekundäre IP-Adressen für Ihre EC2-Instances
- Sekundäre private IPv4-Adresse für Windows-Instance konfigurieren

Private IPv4-Adressen

Eine private IPv4-Adresse ist eine IP-Adresse, die nicht über das Internet erreichbar ist. Sie können private IPv4-Adressen zur Kommunikation zwischen Instances im selben VPC verwenden. Weitere Informationen über die Standards und Spezifikationen vom privaten IPv4-Adressen finden Sie unter RFC 1918. Wir reservieren mit DHCP private IPv4-Adressen für Instances.

> **Note**
>
> Sie können eine VPC mit einem öffentlich routingfähigen CIDR-Block erstellen, der außerhalb der privaten, in RFC 1918 angegebenen IPv4-Adressbereiche fällt. Für die Zwecke dieser Dokumentation bezeichnen wir als private IPv4-Adressen (oder „private IP-Adressen“) die IP-Adressen, die innerhalb des IPv4 CIDR-Bereichs Ihrer VPC liegen.

VPC-Subnetze können einen der folgenden Typen haben:

- Nur-IPv4-Subnetze – Sie können nur Ressourcen in diesen Subnetzen erstellen, denen IPv4-Adressen zugewiesen sind.
- Nur-IPv6-Subnetze – Sie können nur Ressourcen in diesen Subnetzen erstellen, denen IPv6-Adressen zugewiesen sind.
- IPv4- und IPv6-Subnetze – Sie können Ressourcen in diesen Subnetzen erstellen, denen IPv4- oder IPv6-Adressen zugewiesen sind.

Wenn Sie eine EC2-Instance in einem reinen IPv4-oder Dual-Stack-Subnetz (IPv4 und IPv6) starten, erhält die Instance eine primäre private IP-Adresse vom IPv4-Adressbereich des Subnetzes. Weitere Informationen finden Sie unter IP-Adresse im Amazon-VPC-Benutzerhandbuch. Wenn Sie beim Start der Instance keine primäre private IP-Adresse angeben, wählen wir eine verfügbare IP-Adresse im IPv4-Bereich des Subnetzes für Sie aus. Jede Instance hat eine standardmäßige Netzwerkschnittstelle (Index 0), die der primären privaten IPv4-Adresse zugeordnet ist. Sie können auch zusätzliche private IPv4-Adressen angeben, die auch als sekundäre private IPv4-Adressen bezeichnet werden. Im Gegensatz zu privaten IP-Adressen können sekundäre private IP-Adressen von einer Instance zur anderen erneut zugewiesen werden. Weitere Informationen finden Sie unter Mehrere IP-Adressen.

Eine private IPv4-Adresse, unabhängig davon, ob es sich um eine primäre oder sekundäre Adresse handelt, bleibt der Netzwerkschnittstelle zugeordnet, wenn die Instance angehalten und neu gestartet oder in den Ruhezustand versetzt und gestartet wird, und wird freigegeben, wenn die Instance beendet wird.

Öffentliche IPv4-Adressen

Eine öffentliche IP-Adresse ist eine IPv4-Adresse, die über das Internet erreichbar ist. Sie können öffentliche Adressen zur Kommunikation zwischen Ihren Instances und dem Internet verwenden.

Wenn Sie eine Instance in einer Standard-VPC starten, weisen wir ihr standardmäßig eine öffentliche IP-Adresse zu. Wenn Sie eine Instance in einer nicht standardmäßigen VPC starten, hat Ihr Subnetz ein Attribut, durch das festgelegt wird, ob in diesem Subnetz gestartete Instances eine öffentliche IP-Adresse aus dem Pool öffentlicher IPv4-Adressen erhalten. Standardmäßig weisen wir Instances, die in einem nicht standardmäßigen Subnetz gestartet wurden, keine öffentliche IP-Adresse zu.

Anhand der folgenden Schritte können Sie kontrollieren, ob Ihre Instance eine öffentliche IP-Adresse erhält:

- Ändern Sie das öffentliche IP-Adressierungsattributs Ihres Subnetzes. Weitere Informationen finden Sie unter Ändern des öffentlichen IPv4-Adressierungsattributs für Ihr Subnetz im Amazon-VPC-Benutzerhandbuch.
- Aktivieren oder deaktivieren Sie das Adressierungs-Feature für öffentliche IP-Adressen während dem Start. Dadurch wird das öffentliche IP-Adressierungsattribut des Subnetzes überschrieben. Weitere Informationen finden Sie unter Eine öffentliche IPv4-Adresse beim Start zuweisen.
- Heben Sie nach dem Start die Zuweisung einer öffentlichen IP-Adresse an Ihre Instance auf. Weitere Informationen finden Sie unter the section called “Verwalten von IP-Adressen”.

Eine öffentliche IP-Adresse wird Ihrer Instance aus dem Pool öffentlicher IPv4-Adressen von Amazon zugewiesen. Diese Adresse ist nicht mit Ihrem AWS-Konto verknüpft. Wenn eine öffentliche IP-Adresse von Ihrer Instance getrennt wurde, wird sie an den Pool öffentlicher IPv4-Adressen zurückgegeben, und Sie können sie nicht erneut verwenden.

Wir geben die öffentliche IP-Adresse Ihrer Instance frei und weisen ihr eine neue zu, wenn einer der folgenden Fälle eintritt:

- Wir geben die öffentliche IP-Adresse für frei, wenn die Instance angehalten ist, in den Ruhezustand versetzt wurde oder beendet wird. Wir weisen eine neue öffentliche IP-Adresse zu, wenn Sie Ihre angehaltene oder den Ruhezustand versetzte Instance starten.
- Wir geben die öffentliche IP-Adresse frei, wenn Sie der Instance eine Elastic-IP-Adresse zuordnen. Wir weisen eine neue öffentliche IP-Adresse zu, wenn Sie die Elastic-IP-Adresse von der Instance trennen.
- Wenn wir die öffentliche IP-Adresse Ihrer Instance freigeben und sie über eine sekundäre Netzwerkschnittstelle verfügt, weisen wir keine neue öffentliche IP-Adresse zu.
- Wenn wir die öffentliche IP-Adresse Ihrer Instance freigeben und sie über eine sekundäre private IP-Adresse verfügt, die einer Elastic-IP-Adresse zugeordnet ist, weisen wir keine neue öffentliche IP-Adresse zu.

Wenn Sie eine persistente öffentliche IP-Adresse benötigen, die Instances nach Bedarf zugeordnet werden kann, verwenden Sie eine Elastic IP-Adresse.

Wenn Sie dynamisches DNS verwenden, um einen existierenden DNS-Namen der öffentlichen IP-Adresse einer neuen Instance zuzuordnen, kann es bis zu 24 Stunden dauern, bis die IP-Adresse im Internet übernommen wird. Infolgedessen erhalten neue Instances möglicherweise keinen Datenverkehr, während beendete Instances weiterhin Anfragen erhalten. Verwenden Sie eine Elastic IP-Adresse, um dieses Problem zu lösen. Sie können Ihre eigene Elastic IP-Adresse zuweisen und sie mit Ihrer Instance verknüpfen. Weitere Informationen finden Sie unter Elastic-IP-Adressen.

Wenn Sie Amazon VPC IP Address Manager (IPAM) verwenden, können Sie einen zusammenhängenden Block von öffentlichen IPv4-Adressen von AWS abrufen und ihn verwenden, um AWS-Ressourcen Elastic-IP-Adressen zuzuweisen. Die Verwendung von zusammenhängenden IPv4-Adressblöcken kann den Verwaltungsaufwand für Sicherheitszugriffskontrolllisten erheblich reduzieren und die Zuweisung und Verfolgung von IP-Adressen für Unternehmen, die auf AWS skalieren, vereinfachen. Weitere Informationen finden Sie unter Zuweisen sequenzieller Elastic IP-Adressen aus einem IPAM-Pool im Amazon VPC IPAM-Benutzerhandbuch.

Überlegungen

- AWS berechnet Gebühren für alle öffentlichen IPv4-Adressen, einschließlich öffentlicher IPv4-Adressen, die mit laufenden Instances verknüpft sind, und Elastic-IP-Adressen. Weitere Informationen finden Sie auf der Registerkarte Öffentliche IPv4-Adresse auf der Seite Preise für Amazon VPC.
- Für Instances, die auf andere Instances über ihre öffentliche NAT-IP-Adresse zugreifen, werden Gebühren für regionale oder Internet-Datenübertragung berechnet, je nachdem, ob sich die Instances in derselben Region befinden.

Optimierung von öffentlichen IPv4-Adressen

AWS berechnet Gebühren für alle öffentlichen IPv4-Adressen, einschließlich öffentlicher IPv4-Adressen, die mit laufenden Instances verknüpft sind, und Elastic-IP-Adressen. Weitere Informationen finden Sie auf der Registerkarte Öffentliche IPv4-Adresse auf der Seite Preise für Amazon VPC.

Die folgende Liste enthält Maßnahmen, die Sie ergreifen können, um die Anzahl der von Ihnen verwendeten öffentlichen IPv4-Adressen zu optimieren:

- Verwenden Sie einen Elastic Load Balancer, um den Datenverkehr zu Ihren EC2-Instances zu verteilen, und deaktivieren Sie die automatische Zuweisung öffentlicher IP-Adressen auf der primären ENI, die den Instances zugewiesen ist. Load Balancer verwenden eine einzige öffentliche IPv4-Adresse. Dadurch wird die Anzahl Ihrer öffentlichen IPv4-Adressen reduziert. Möglicherweise möchten Sie auch vorhandene Load Balancer konsolidieren, um die Anzahl der öffentlichen IPv4-Adressen weiter zu reduzieren.
- Wenn der einzige Grund für die Verwendung eines NAT-Gateways die SSH-Verbindung zu einer EC2-Instance in einem privaten Subnetz für Wartungs- oder Notfälle ist, sollten Sie stattdessen EC2-Instance-Connect-Endpunkt verwenden. Mit dem EC2-Instance-Connect-Endpunkt können Sie eine Verbindung zu einer Instance herstellen, ohne dass die Instance eine öffentliche IPv4-Adresse haben muss.
- Wenn sich Ihre EC2-Instances in einem öffentlichen Subnetz befinden, dem öffentliche IP-Adressen zugewiesen sind, sollten Sie erwägen, die Instances in ein privates Subnetz zu verschieben, die öffentlichen IP-Adressen zu entfernen und ein öffentliches NAT-Gateway zu verwenden, um den Zugriff auf und von Ihren EC2-Instances zu ermöglichen. Bei der Verwendung von NAT-Gateways gibt es Kostenüberlegungen. Verwenden Sie diese Berechnungsmethode, um zu entscheiden, ob NAT-Gateways kosteneffektiv sind. Sie können die für diese Berechnung erforderlichen `Number of public IPv4 addresses` abrufen, indem Sie einen Bericht zu AWS-Abrechnungskosten und -nutzung erstellen.

  ```
  NAT gateway per hour + NAT gateway public IPs + NAT gateway transfer / Existing
   public IP cost
  ```

  Wobei Folgendes gilt:

  - `NAT gateway per hour = $0.045 * 730 hours in a month * Number of Availability Zones the NAT gateways are in`
  - `NAT gateway public IPs = $0.005 * 730 hours in a month * Number of IPs associated with your NAT gateways`
  - `NAT gateway transfer = $0.045 * Number of GBs that will go through the NAT gateway in a month`
  - `Existing public IP cost = $0.005 * 730 hours in a month * Number of public IPv4 addresses`

  Wenn die Summe weniger als 1 ist, sind NAT-Gateways günstiger als öffentliche IPv4-Adressen.

- Verwenden Sie AWS PrivateLink, um private Verbindungen zu AWS-Services oder Services herzustellen, die von anderen AWS-Konten gehostet werden, anstatt öffentliche IPv4-Adressen und Internet-Gateways zu verwenden.
- Bringen Sie Ihren eigenen IP-Adressbereich (BYOIP) zu AWS und verwenden Sie den Bereich für öffentliche IPv4-Adressen, anstatt öffentliche IPv4-Adressen im Besitz von Amazon zu verwenden.
- Schalten Sie Automatische Zuordnung der öffentlichen IPv4-Adresse zur Instance, die in Subnetzen gestartet wird aus. Diese Option ist in der Regel standardmäßig für VPCs deaktiviert, wenn Sie ein Subnetz erstellen. Sie sollten jedoch Ihre vorhandenen Subnetze überprüfen, um sicherzustellen, dass sie deaktiviert ist.
- Wenn Sie über EC2-Instances verfügen, die keine öffentlichen IPv4-Adressen benötigen, überprüfen Sie, ob für die Netzwerkschnittstellen, die an Ihre Instances angeschlossen sind, die automatische Zuweisung öffentlicher IP-Adressen deaktiviert ist.
- Konfigurieren Sie Accelerator-Endpunkte in AWS Global Accelerator für EC2-Instances in privaten Subnetzen, damit der Internetverkehr direkt zu den Endpunkten in Ihren VPCs fließen kann, ohne dass öffentliche IP-Adressen erforderlich sind. Sie können auch Ihre eigenen Adressen zu AWS Global Accelerator bringen und Ihre eigenen IPv4-Adressen für die statischen IP-Adressen Ihres Accelerators verwenden.

IPv6-Adressen

IPv6-Adressen sind global eindeutig und können so konfiguriert werden, dass sie privat oder über das Internet erreichbar sind. Sowohl öffentliche als auch private IPv6-Adressierung ist verfügbar in AWS:

- Private IPv6: Als private IPv6-Adressen werden solche Adressen von AWS betrachtet, für die keine Werbung im Internet gemacht wurde und von denen aus auch nicht im Internet Werbung gemacht werden kann von AWS.
- Öffentliches IPv6: AWS berücksichtigt öffentliche IPv6-Adressen, von denen aus im Internet Werbung gemacht wird von AWS.

Weitere Informationen zu IPv6-Adressen finden Sie unter IPv6-Adressen im Amazon-VPC-Benutzerhandbuch.

Alle Instance-Typen unterstützen IPv6-Adressen, außer den folgenden: C1, M1, M2, M3 und T1.

Ihre EC-2 Instance erhält eine IPv6-Adresse, wenn Ihrer VPC und Ihrem Subnetz ein IPv6 CIDR-Block zugewiesen ist und eines der Folgenden zutrifft:

- Ihr Subnetz ist so konfiguriert, dass einer Instance beim Start automatisch eine IPv6-Adresse zugewiesen wird. Weitere Informationen finden Sie unter Ändern des öffentlichen IP-Adressierungsattributs Ihres Subnetzes.
- Sie weisen Ihrer Instance beim Start manuell eine IPv6-Adresse zu.
- Sie weisen der primären Netzwerkschnittstelle Ihrer Instance nach dem Start eine IPv6-Adresse zu.
- Sie weisen einer Netzwerkschnittstelle eine IPv6-Adresse im gleichen Subnetz zu und fügen die Netzwerkschnittstelle nach dem Start Ihrer Instance hinzu.

Wenn Ihre Instance beim Start eine IPv6-Adresse erhält, wird die Adresse mit der primären Netzwerkschnittstelle (Index 0) der Instance verknüpft. Sie können die IPv6-Adressen der primären Netzwerkschnittstelle Ihrer Instance auf folgende Weise verwalten:

- Zuweisung und Aufhebung der Zuweisung von IPv6-Adressen an der Netzwerkschnittstelle. Die Anzahl der IPv6-Adressen, die Sie einer Netzwerkschnittstelle zuweisen können, und die Anzahl der Netzwerkschnittstellen, die Sie einer Instance zuweisen können, ist abhängig vom Instance-Typ. Weitere Informationen finden Sie unter Maximale IP-Adressen pro Netzwerkschnittstelle.
- Aktivieren Sie eine primäre IPv6-Adresse. Mit einer primären IPv6-Adresse können Sie eine Unterbrechung des Datenverkehrs zu Instances oder ENIs vermeiden. Weitere Informationen finden Sie unter Erstellen Sie eine Netzwerkschnittstelle für Ihre EC2 Instance oder Die IP-Adressen für Ihre Netzwerkschnittstellen verwalten.

Eine IPv6-Adresse bleibt beim Anhalten und Starten oder beim Versetzen in den Ruhezustand und Starten Ihrer Instance bestehen und wird beim Beenden Ihrer Instance freigegeben. Solange eine IPv6-Adresse einer anderen Netzwerkschnittstelle zugewiesen ist, können Sie sie nicht erneut zuordnen – Sie müssen die Zuweisung zunächst aufheben.

Sie können kontrollieren, ob Instances über ihre IPv6-Adressen erreichbar sind, indem Sie entweder das Routing Ihres Subnetzes steuern oder Sicherheitsgruppen und Netzwerk-ACL-Regeln verwenden. Weitere Informationen finden Sie unter Datenschutz im Internet-Netzwerk im Amazon VPC-Benutzerhandbuch.

Weitere Informationen über reservierte IPv6-Adressbereiche finden Sie unter IANA IPv6 Special-Purpose Address Registry und RFC4291.

Mehrere IP-Adressen

Sie können Sie mehrere private IPv4- und IPv6-Adressen für Ihre Instances angeben. Die Anzahl von Netzwerkschnittstellen und privaten IPv4- und IPv6-Adressen, die Sie für eine Instance angeben können, hängt vom Instance-Typ ab. Weitere Informationen finden Sie unter Maximale IP-Adressen pro Netzwerkschnittstelle.

Anwendungsfälle

- Hosten mehrerer Websites auf einem einzelnen Server, indem mehrere SSL-Zertifikate auf einem einzelnen Server verwendet werden und jedem Zertifikat eine spezifische IP-Adresse zugeordnet wird.
- Betreiben von Netzwerkgeräten, beispielsweise Firewalls oder Load Balancers, die über mehrere IP-Adressen für jede Netzwerkschnittstelle verfügen.
- Umleiten von internem Datenverkehr zu einer Standby-Instance für den Fall, dass Ihre Instance ausfällt, wobei die sekundäre IP-Adresse der Standby-Instance zugewiesen wird.

So funktionieren mehrere IP-Adressen

- Sie können jeder Netzwerkschnittstelle eine sekundäre private IPv4-Adresse zuweisen.
- Sie können mehrere IPv6-Adressen einer Netzwerkschnittstelle in einem Subnetz zuweisen, dem ein IPv6 CIDR-Block zugeordnet ist.
- Sie müssen die sekundäre IPv4-Adresse für die Netzwerkschnittstelle aus dem IPv4 CIDR-Blockbereich des Subnetzes auswählen.
- Sie müssen IPv6-Adressen für die Netzwerkschnittstelle aus dem IPv6 CIDR-Blockbereich des Subnetzes auswählen.
- Sie weisen den Netzwerkschnittstellen Sicherheitsgruppen und keine einzelnen IP-Adressen zu. Daher unterliegt jede IP-Adresse, die Sie in einer Netzwerkschnittstelle angeben, der Sicherheitsgruppe dieser Netzwerkschnittstelle.
- Es kann eine Zuweisung mehrerer IP-Adressen zu Netzwerkschnittstellen erfolgen oder aufgehoben werden, die an laufende oder angehaltene Instances angefügt sind.
- Sekundäre private IPv4-Adressen, die einer Netzwerkschnittstelle zugewiesen sind, können einer anderen Schnittstelle erneut zugewiesen werden, wenn Sie dies ausdrücklich erlauben.
- Eine IPv6-Adresse kann einer anderen Netzwerkschnittstelle nicht erneut zugewiesen werden; Sie müssen zuerst die Zuordnung der IPv6-Adresse zu der bestehenden Netzwerkschnittstelle aufheben.

- Wenn Sie einer Netzwerkschnittstelle mit den Befehlszeilen-Tools oder der API mehrere IP-Adressen zuweisen, schlägt die gesamte Operation fehl, wenn eine der IP-Adressen nicht zugewiesen werden kann.
- Primäre private IPv4-, sekundäre private IPv4-, Elastic IP- und IPv6-Adressen bleiben mit einer sekundären Netzwerkschnittstelle verknüpft, wenn sie von einer Instance getrennt oder an eine Instance angefügt wird.
- Obwohl es nicht möglich ist, die primäre Netzwerkschnittstelle von einer Instance zu trennen, können Sie die sekundäre private IPv4-Adresse der primären Netzwerkschnittstelle einer anderen Netzwerkschnittstelle zuweisen.

Weitere Informationen finden Sie unter the section called “Sekundäre IP-Adressen”.

Hostnamen der EC2-Instance

Wenn Sie eine EC2-Instance erstellen, erstellt AWS einen Hostnamen für diese Instance. Weitere Informationen über die Typen von Hostnamen und wie diese von AWS bereitgestellt werden, finden Sie unter Hostnamen und Domains der EC2-Instance. Amazon bietet einen DNS-Server, der von Amazon bereitgestellten Hostnamen zu IPv4- und IPv6-Adressen auflöst. Der Amazon DNS-Server befindet sich an der Basis Ihres VPC-Netzwerkbereichs plus zwei. Weitere Infomationen finden Sie unter DNS-Attribute für Ihre VPC im Amazon VPC-Benutzerhandbuch.

Link-lokale Adressen

Link-Local-Adressen sind bekannte, nicht weiterleitbare IP-Adressen. Amazon EC2 verwendet Adressen aus dem Link-lokalen Adressraum, um Services bereitzustellen, auf die nur von einer EC2-Instance aus zugegriffen werden kann. Diese Services werden nicht auf der Instance ausgeführt, sondern auf dem zugrunde liegenden Host. Wenn Sie auf die Link-lokalen Adressen für diese Services zugreifen, kommunizieren Sie entweder mit dem Xen-Hypervisor oder dem Nitro-Controller.

Link-lokale Adressbereiche

- IPv4 – 169.254.0.0/16 (169.254.0.0 bis 169.254.255.255)
- IPv6 – fe80::/10

Services, auf die Sie über Link-lokale Adressen zugreifen

- Instance-Metadatenservice

- Amazon Route 53 Resolver (auch bekannt als Amazon DNS-Server)
- Amazon Time Sync Service
- AWS KMS-Server

Arbeiten mit den IPv4-Adressen für Ihre EC2-Instances

Sie können Ihrer Instance beim Start eine öffentliche IPv4-Adresse zuweisen. Sie können die IPv4-Adressen für Ihre Instance in der Konsole über die Seite Instances oder die Seite Network Interfaces (Netzwerkschnittstellen) anzeigen.

Aufgaben

- Eine öffentliche IPv4-Adresse beim Start zuweisen
- Eine private IPv4-Adresse beim Start zuweisen
- Die primäre IPv4-Adresse anzeigen
- Die IPv4-Adressen mithilfe der Instance-Metadaten anzeigen

Eine öffentliche IPv4-Adresse beim Start zuweisen

Alle Subnetze haben ein Attribut, das bestimmt, ob den Instances, die in diesem Subnetz gestartet werden, eine öffentliche IP-Adresse zugewiesen wird. Standardmäßig ist dieses Attribut bei nicht standardmäßigen Subnetzen auf „false“ eingestellt. Bei standardmäßigen Subnetzen ist es auf „true“ eingestellt. Wenn Sie eine Instance starten, steht Ihnen auch ein öffentliches IPv4-Adressierungsfeature zur Verfügung, um zu kontrollieren, ob Ihrer Instance eine öffentliche IPv4-Adresse zugewiesen wurde. Sie können das Standardverhalten des IP-Adressierungsattributs des Subnetzes außer Kraft setzen. Die öffentliche IPv4-Adresse wird aus dem Pool öffentlicher IPv4-Adressen von Amazon zugeordnet. Sie wird der Netzwerkschnittstelle mit dem Geräteindex 0 zugewiesen. Dieses Feature ist von bestimmten Bedingungen zum Zeitpunkt des Starts Ihrer Instance abhängig.

Überlegungen

- Sie können die Zuweisung der öffentlichen IP-Adresse zu Ihrer Instance nach dem Start aufheben, indem Sie die IP-Adressen verwalten, die einer Netzwerkschnittstelle zugeordnet sind. Weitere Informationen über öffentliche IPv4-Adressen finden Sie unter Öffentliche IPv4-Adressen.
- Sie können eine öffentliche IP-Adresse nicht automatisch zuweisen, wenn Sie mehr als eine Netzwerkschnittstelle angeben. Außerdem können Sie die Subnetz-Einstellung nicht mit dem

Feature „Öffentliche IP automatisch zuweisen“ außer Kraft setzen, wenn Sie eine vorhandene Netzwerkschnittstelle für Geräteindex 0 angeben.

- Unabhängig davon, ob Sie Ihrer Instance beim Start eine öffentliche IP-Adresse zugewiesen haben oder nicht, können Sie Ihrer Instance auch noch nach dem Start eine Elastic-IP-Adresse zuordnen. Weitere Informationen finden Sie unter Elastic-IP-Adressen. Sie können auch das Adressierungsverhaltens Ihres Subnetzes für öffentliche IPv4-Adressen ändern. Weitere Informationen finden Sie unter Ändern des öffentlichen IPv4-Adressierungsattributs für Ihr Subnetz.

Console

So können Sie eine öffentliche IPv4-Adresse beim Start zuweisen

Folgen Sie dem Verfahren unter Eine Instance starten und wenn Sie dabei sind, die Netzwerk-Einstellungen zu konfigurieren, wählen Sie die Option Auto-assign Public IP (Öffentliche IP-Adresse automatisch zuweisen).

AWS CLI

So können Sie eine öffentliche IPv4-Adresse beim Start zuweisen

Verwenden den Befehl run-instances mit der Option `--associate-public-ip-address`.

```
--associate-public-ip-address
```

PowerShell

So können Sie eine öffentliche IPv4-Adresse beim Start zuweisen

Verwenden Sie das Cmdlet New-EC2Instance mit dem `-AssociatePublicIp`-Parameter.

```
-AssociatePublicIp $true
```

Eine private IPv4-Adresse beim Start zuweisen

Sie können eine private IPv4-Adresse aus dem IPv4-Adressenbereich des Subnetzes angeben oder Amazon EC2 eine für Sie auswählen lassen. Diese Adresse ist der primären Netzwerkschnittstelle zugewiesen.

Informationen dazu, wie Sie nach IPv4-Adressen nach dem Start zuweisen, finden Sie unter the section called “Einer Instance sekundäre IP-Adressen zuweisen”.

Console

So können Sie eine private IPv4-Adresse beim Start zuweisen

Befolgen Sie das Verfahren zum Starten einer Instance. Wenn Sie Netzwerkeinstellungen konfigurieren, erweitern Sie Erweiterte Netzwerkkonfiguration und geben Sie einen Wert für Primäre IP ein.

AWS CLI

So können Sie eine private IPv4-Adresse beim Start zuweisen

Verwenden den Befehl run-instances mit der Option `--private-ip-address`.

```
--private-ip-addresses 10.251.50.12
```

Lassen Sie diese Option weg, damit Amazon EC2 die IP-Adresse wählen kann.

PowerShell

So können Sie eine private IPv4-Adresse beim Start zuweisen

Verwenden Sie das Cmdlet New-EC2Instance mit dem `-PrivateIpAddress`-Parameter.

```
-PrivateIpAddress 10.251.50.12
```

Lassen Sie diesen Parameter weg, damit Amazon EC2 die IP-Adresse wählen kann.

Die primäre IPv4-Adresse anzeigen

Die öffentliche IPv4-Adresse wird als Eigenschaft der Netzwerkschnittstelle auf der Konsole angezeigt, jedoch ist sie mit der primären privaten IPv4-Adresse über NAT verknüpft. Daher wird die öffentliche IPv4-Adresse bei einer Überprüfung der Eigenschaften Ihrer Netzwerkschnittstelle auf Ihrer Instance, beispielsweise über `ifconfig` (Linux) oder `ipconfig` (Windows), nicht angezeigt.

Console

So können Sie die IPv4-Adressen für eine Instance anzeigen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.

4. Suchen Sie auf der Registerkarte Netzwerk nach Öffentliche IPv4-Adresse und Private IPv4-Adressen.
5. (Optional) Die Registerkarte Netzwerk enthält auch die Netzwerkschnittstellen und Elastic-IP-Adressen für die Instance.

AWS CLI

So können Sie die primäre IPv4-Adresse für eine Instance anzeigen

Verwenden Sie den Befehl describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[].Instances[].PrivateIpAddress" \
    --output text
```

Es folgt eine Beispielausgabe.

```
10.251.50.12
```

PowerShell

So können Sie die primäre IPv4-Adresse für eine Instance anzeigen

Verwenden Sie das cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.PrivateIpAddress
```

Es folgt eine Beispielausgabe.

```
10.251.50.12
```

Die IPv4-Adressen mithilfe der Instance-Metadaten anzeigen

Sie können die IPv4-Adressen für Ihre Instance abrufen, indem Sie Instance-Metadaten abrufen. Weitere Informationen finden Sie unter Verwenden Sie Instanz-Metadaten, um Ihre EC2 Instanz zu verwalten.

So können Sie die IPv4-Adressen mithilfe der Instance-Metadaten anzeigen

1. Verbinden Sie sich mit der Instance. Weitere Informationen finden Sie unter Connect zu Ihrer EC2 Instance her.
2. Führen Sie einen der folgenden Befehle aus.

   IMDSv2

   Linux

   Führen Sie den folgenden Befehl in Ihrer Linux-Instance aus.

   ```
   TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/local-ipv4
   ```

   Windows

   Führen Sie den folgenden Befehl in Ihrer Windows-Instance aus.

   ```
   [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
       -Method PUT -Uri http://169.254.169.254/latest/api/token
   ```

   ```
   Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
       -Method GET -Uri http://169.254.169.254/latest/meta-data/local-ipv4
   ```

   IMDSv1

   Linux

   Führen Sie den folgenden Befehl in Ihrer Linux-Instance aus.

   ```
   curl http://169.254.169.254/latest/meta-data/local-ipv4
   ```

   Windows

   Führen Sie den folgenden Befehl in Ihrer Windows-Instance aus.

```
Invoke-RestMethod http://169.254.169.254/latest/meta-data/local-ipv4
```

3. Verwenden Sie einen der folgenden Befehle, um auf die öffentliche IP-Adresse zuzugreifen. Wenn eine Elastic-IP-Adresse der Instance zugeordnet ist, gibt der Befehl die Elastic-IP-Adresse zurück.

   IMDSv2

   Linux

   Führen Sie den folgenden Befehl in Ihrer Linux-Instance aus.

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/public-ipv4
   ```

   Windows

   Führen Sie den folgenden Befehl in Ihrer Windows-Instance aus.

   ```
   [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
   seconds" = "21600"} `
       -Method PUT -Uri http://169.254.169.254/latest/api/token
   ```

   ```
   Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
       -Method GET -Uri http://169.254.169.254/latest/meta-data/public-ipv4
   ```

   IMDSv1

   Linux

   Führen Sie den folgenden Befehl in Ihrer Linux-Instance aus.

   ```
   curl http://169.254.169.254/latest/meta-data/public-ipv4
   ```

   Windows

   Führen Sie den folgenden Befehl in Ihrer Windows-Instance aus.

```
Invoke-RestMethod http://169.254.169.254/latest/meta-data/public-ipv4
```

Die IPv6-Adressen für Ihre EC2-Instances verwalten

Wenn Ihrer VPC und dem Subnetz IPv6 CIDR-Blöcke zugeordnet sind, können Sie Ihrer Instance während oder nach dem Start eine IPv6-Adresse zuweisen. Sie können auf die IPv6-Adressen für Ihre Instance in der Konsole über die Seite Instances oder die Seite Netzwerkschnittstellen zugreifen. Mit den folgenden Aufgaben werden IP-Adressen für Ihre Instances konfiguriert. Informationen dazu, stattdessen IP-Adressen für Ihre Netzwerkschnittstellen zu konfigurieren, finden Sie unter the section called “Verwalten von IP-Adressen”.

Aufgaben

- Zuweisen einer IPv6-Adresse zu einer Instance
- IPv6-Adressen für eine Instance anzeigen
- Die IPv6-Adressen mithilfe der Instance-Metadaten anzeigen
- Aufheben der Zuweisung einer IPv6-Adresse zu einer Instance

Zuweisen einer IPv6-Adresse zu einer Instance

Sie können eine IPv6-Adresse aus dem IPv6-Adressenbereich des Subnetzes angeben oder Amazon EC2 eine für Sie auswählen lassen. Diese Adresse ist der primären Netzwerkschnittstelle zugewiesen. Beachten Sie, dass die folgenden Instance-Typen keine IPv6-Adressen unterstützen: C1, M1, M2, M3 und T1.

Console

So weisen Sie beim Start eine IPv6-Adresse zu

Befolgen Sie das Verfahren zum Starten einer Instance. Wählen Sie bei der Konfiguration der Netzwerkeinstellungen die Option zur automatischen Zuweisung von IPv6-IP. Wenn Sie diese Option nicht sehen, wurde dem ausgewählten Subnetz kein IPv6-CIDR-Block zugeordnet.

So weisen Sie nach dem Start eine IPv6-Adresse zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.

3. Wählen Sie Ihre Instance und anschließend Aktionen, Netzwerk, IP-Adressen verwalten aus.
4. Erweitern Sie die Netzwerkschnittstelle. Wählen Sie unter IPv6-Adressen die Option Neue IP-Adresse zuweisen aus.
5. Geben Sie eine IPv6-Adresse aus dem Bereich des Subnetzes ein oder lassen Sie das Feld leer, damit Amazon EC2 die IPv6-Adresse für Sie auswählen kann. Wenn Sie diese Option nicht sehen, wurde dem Instance-Subnetz kein IPv6-CIDR-Block zugeordnet.
6. Wählen Sie Speichern.

AWS CLI

So weisen Sie beim Start eine IPv6-Adresse zu

Verwenden den Befehl run-instances mit der Option `--ipv6-addresses`. Im folgenden Beispiel werden zwei IPv6-Adressen zugewiesen.

```
--ipv6-addresses Ipv6Address=2001:db8::1234:5678:1.2.3.4
 Ipv6Address=2001:db8::1234:5678:5.6.7.8
```

Verwenden Sie stattdessen die Option `--ipv6-address-count`, damit Amazon EC2 die IPv6-Adressen auswählen kann. Im folgenden Beispiel werden zwei IPv6-Adressen zugewiesen.

```
--ipv6-address-count 2
```

So weisen Sie nach dem Start eine IPv6-Adresse zu

Verwenden Sie den Befehl assign-ipv6-addresses. Im folgenden Beispiel werden zwei IPv6-Adressen zugewiesen.

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-addresses 2001:db8::1234:5678:1.2.3.4 2001:db8::1234:5678:5.6.7.8
```

Verwenden Sie stattdessen die Option `--ipv6-address-count`, damit Amazon EC2 die IPv6-Adressen auswählen kann. Im folgenden Beispiel werden zwei IPv6-Adressen zugewiesen.

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
```

```
    --ipv6-address-count 2
```

PowerShell

So weisen Sie beim Start eine IPv6-Adresse zu

Verwenden Sie das Cmdlet New-EC2Instance mit dem `-Ipv6Address`-Parameter. Im folgenden Beispiel werden zwei IPv6-Adressen zugewiesen.

```
-Ipv6Address $ipv6addr1,$ipv6addr2
```

Definieren Sie die IPv6-Adressen wie folgt.

```
$ipv6addr1 = New-Object Amazon.EC2.Model.InstanceIpv6Address
$ipv6addr1.Ipv6Address = "2001:db8::1234:5678:1.2.3.4"
$ipv6addr2 = New-Object Amazon.EC2.Model.InstanceIpv6Address
$ipv6addr2.Ipv6Address = "2001:db8::1234:5678:5.6.7.8"
```

Verwenden Sie stattdessen den Parameter `-Ipv6AddressCount`, damit Amazon EC2 die IPv6-Adressen auswählen kann. Im folgenden Beispiel werden zwei IPv6-Adressen zugewiesen.

```
-Ipv6AddressCount 2
```

So weisen Sie nach dem Start eine IPv6-Adresse zu

Verwenden Sie das cmdlet Register-EC2Ipv6AddressList. Im folgenden Beispiel werden zwei IPv6-Adressen zugewiesen.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6Address "2001:db8::1234:5678:1.2.3.4","2001:db8::1234:5678:5.6.7.8"
```

Verwenden Sie stattdessen den Parameter `-Ipv6AddressCount`, damit Amazon EC2 die IPv6-Adressen auswählen kann. Im folgenden Beispiel werden zwei IPv6-Adressen zugewiesen.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6AddressCount 2
```

IPv6-Adressen für eine Instance anzeigen

Sie können die IPv6-Adressen für Ihre Instances anzeigen.

Console

So können Sie die IPv6-Adressen für eine Instance anzeigen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.
4. Suchen Sie auf der Registerkarte Netzwerk die Option IPv6-Adressen.

AWS CLI

So können Sie die IPv6-Adresse für eine Instance anzeigen

Verwenden Sie den Befehl describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[*].Instances[].Ipv6Address" \
    --output text
```

Es folgt eine Beispielausgabe.

```
2001:db8::1234:5678:1.2.3.4
```

PowerShell

So können Sie die IPv6-Adresse für eine Instance anzeigen

Verwenden Sie das cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.Ipv6Address
```

Es folgt eine Beispielausgabe.

```
2001:db8::1234:5678:1.2.3.4
```

Die IPv6-Adressen mithilfe der Instance-Metadaten anzeigen

Nachdem Sie eine Verbindung zu Ihrer Instance hergestellt haben, können Sie die IPv6-Adressen mithilfe von Instance-Metadaten abrufen. Rufen Sie zunächst die MAC-Adresse der Instance von `http://169.254.169.254/latest/meta-data/network/interfaces/macs/` ab.

IMDSv2

Linux

Führen Sie den folgenden Befehl in Ihrer Linux-Instance aus.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/network/interfaces/macs/mac-address/ipv6s
```

Windows

Führen Sie die folgenden cmdlets in Ihrer Windows-Instance aus.

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/network/interfaces/
macs/mac-address/ipv6s
```

IMDSv1

Linux

Führen Sie den folgenden Befehl in Ihrer Linux-Instance aus.

```
curl http://169.254.169.254/latest/meta-data/network/interfaces/macs/mac-address/
ipv6s
```

Windows

Führen Sie das folgende cmdlet in Ihrer Windows-Instance aus.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/network/interfaces/
macs/mac-address/ipv6s
```

Aufheben der Zuweisung einer IPv6-Adresse zu einer Instance

Sie können die Zuweisung einer IPv6-Adresse zu einer Instance jederzeit aufheben.

Console

So heben Sie die Zuweisung einer IPv6-Adresse zu einer Instance auf

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie Ihre Instance und anschließend Aktionen, Netzwerk, IP-Adressen verwalten aus.
4. Erweitern Sie die Netzwerkschnittstelle. Wählen Sie unter IPv6-Adressen die Option Zuweisung aufheben neben der IPv6-Adresse aus.
5. Wählen Sie Speichern.

AWS CLI

So heben Sie die Zuweisung einer IPv6-Adresse zu einer Instance auf

Verwenden Sie den Befehl unassign-ipv6-addresses.

```
aws ec2 unassign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-addresses 2001:db8::1234:5678:1.2.3.4
```

PowerShell

So heben Sie die Zuweisung einer IPv6-Adresse zu einer Instance auf

Verwenden Sie das cmdlet Unregister-EC2Ipv6AddressList.

```
Unregister-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6Address 2001:db8::1234:5678:1.2.3.4
```

Sekundäre IP-Adressen für Ihre EC2-Instances

Die erste IPv4-Adresse, die einer Netzwerkschnittstelle zugewiesen ist, wird als primäre IP-Adresse bezeichnet. Sekundäre IP-Adressen sind zusätzliche IPv4-Adressen, die einer Netzwerkschnittstelle zugewiesen sind. Weitere Informationen finden Sie unter the section called “Mehrere IP-Adressen”.

Sie können einer Instance auch mehrere IPv6-Adressen zuweisen. Weitere Informationen finden Sie unter the section called “IPv6-Adressen”.

Aufgaben

- Einer Instance sekundäre IP-Adressen zuweisen
- Das Betriebssystem zur Verwendung von sekundären IP-Adressen konfigurieren
- Die Zuweisung einer sekundären IP-Adresse zu einer Instance aufheben

Einer Instance sekundäre IP-Adressen zuweisen

Sie können der Netzwerkschnittstelle für eine Instance sekundäre IP-Adressen zuweisen, während Sie die Instance starten oder wenn die Instance ausgeführt wird.

Console

So können Sie eine sekundäre IP-Adresse beim Start zuweisen

1. Befolgen Sie das Verfahren zum Starten einer Instance. Wenn Sie Netzwerkeinstellungen konfigurieren, erweitern Sie Erweiterte Netzwerkkonfiguration.
2. Wählen Sie für Sekundäre IP die Option Automatisch zuweisen und geben Sie die Anzahl der IP-Adressen ein, die Amazon EC2 zuweisen soll. Wählen Sie alternativ Manuell zuweisen und geben Sie die IPv4-Adressen ein.
3. Führen Sie die verbleibenden Schritte zum Starten der Instance aus.

So können Sie eine sekundäre IP-Adresse nach dem Start zuweisen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie Ihre Instance und anschließend Aktionen, Netzwerk, IP-Adressen verwalten aus.
4. Erweitern Sie die Netzwerkschnittstelle.

5. Um eine IPv4-Adresse hinzuzufügen, wählen Sie unter IPv4-Adressen die Option Neue IP-Adresse zuweisen aus. Geben Sie eine IPv4-Adresse aus dem Bereich des Subnetzes ein oder lassen Sie das Feld leer, um Amazon EC2 eine Adresse für Sie auswählen zu lassen.
6. Wählen Sie Speichern.

AWS CLI

So können Sie eine sekundäre IP-Adresse beim Start zuweisen

Verwenden den Befehl run-instances mit der Option `--secondary-private-ip-addresses`.

```
--secondary-private-ip-addresses 10.251.50.12
```

Verwenden Sie stattdessen die Option `--secondary-private-ip-address-count`, damit Amazon EC2 die IP-Adresse auswählen kann. Im folgenden Beispiel wird eine sekundäre IP-Adresse zugewiesen.

```
--secondary-private-ip-address-count 1
```

Alternativ können Sie auch eine Netzwerkschnittstelle erstellen. Weitere Informationen finden Sie unter the section called “Erstellen einer Netzwerkschnittstelle”.

So können Sie eine sekundäre IP-Adresse nach dem Start zuweisen

Verwenden Sie den Befehl assign-private-ip-addresses mit der Option `--private-ip-addresses`.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-ids eni-1234567890abcdef0 \
    --private-ip-addresses 10.251.50.12
```

Verwenden Sie stattdessen den Parameter `--secondary-private-ip-address-count`, damit Amazon EC2 die IPv4-Adressen auswählen kann. Im folgenden Beispiel wird eine IPv4-Adresse zugewiesen.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-ids eni-1234567890abcdef0 \
    --secondary-private-ip-address-count 1
```

PowerShell

So können Sie eine sekundäre IP-Adresse beim Start zuweisen

Siemüssen eine Netzwerkschnittstelle erstellen. Weitere Informationen finden Sie unter the section called “Erstellen einer Netzwerkschnittstelle”.

So können Sie eine sekundäre IP-Adresse nach dem Start zuweisen

Verwenden Sie das cmdlet Register-EC2PrivateIpAddress mit dem Parameter `-PrivateIpAddress`.

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -PrivateIpAddress 10.251.50.12
```

Verwenden Sie stattdessen den Parameter `-SecondaryPrivateIpAddressCount`, damit Amazon EC2 die IPv4-Adressen auswählen kann. Im folgenden Beispiel wird eine IPv4-Adresse zugewiesen.

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -SecondaryPrivateIpAddressCount 1
```

Das Betriebssystem zur Verwendung von sekundären IP-Adressen konfigurieren

Nachdem Sie Ihrer Instance eine sekundäre IP-Adresse zugewiesen haben, müssen Sie das Betriebssystem auf der Instance so konfigurieren, dass es die zusätzliche private IPv4-Adresse erkennt.

Linux-Instances

- Wenn Sie Amazon Linux verwenden, kann das Paket ec2-net-utils diesen Schritt für Sie übernehmen. Es konfiguriert zusätzliche Netzwerkschnittstellen, die Sie anfügen, während die Instance ausgeführt wird, aktualisiert sekundäre IPv4-Adressen während der Erneuerung der DHCP-Lease und aktualisiert die zugehörigen Routing-Regeln. Sie können die Liste der Schnittstellen sofort aktualisieren, indem Sie je nach Ihrem System einen der folgenden Befehle verwenden: `sudo systemctl restart systemd-networkd` (AL2023) oder `sudo service network restart` (Amazon Linux 2). Sie können die aktuelle Liste mit dem folgenden Befehl anzeigen: `ip addr li`. Wenn Sie eine manuelle Kontrolle über Ihre Netzwerkkonfiguration

benötigen, können Sie das Paket ec2-net-utils entfernen. Weitere Informationen finden Sie unter Konfigurieren Ihrer Netzwerkschnittstelle mit ec2-net-utils.

- Wenn Sie eine andere Linux-Verteilung verwenden, ziehen Sie die Dokumentation für Ihre Linux-Distribution zurate. Suchen Sie nach Informationen zum Konfigurieren zusätzlicher Netzwerkschnittstellen und sekundärer IPv4-Adressen. Wenn die Instance zwei oder mehr Schnittstellen in demselben Subnetz hat, suchen Sie nach Informationen zur Verwendung von Routing-Regeln, um asymmetrisches Routing zu umgehen.

Windows-Instances

Weitere Informationen finden Sie unter Sekundäre private IPv4-Adresse für Windows-Instance konfigurieren.

Die Zuweisung einer sekundären IP-Adresse zu einer Instance aufheben

Wenn Sie eine sekundäre IP-Adresse nicht länger benötigen, können Sie die Zuweisung zu der Instance oder der Netzwerkschnittstelle aufheben. Wird die Zuweisung einer sekundären privaten IPv4-Adresse zu einer Netzwerkschnittstelle aufgehoben, wird die Zuordnung der Elastic IP-Adresse (falls vorhanden) ebenfalls getrennt.

Console

So heben Sie die Zuweisung einer sekundären privaten IPv4-Adresse zu einer Instance auf

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie eine Instance und anschließend Aktionen, Netzwerk, IP-Adressen verwalten aus.
4. Erweitern Sie die Netzwerkschnittstelle. Wählen Sie unter IPv4-Addressen die Option Zuweisung aufheben zum Aufheben der Zuweisung der IPv4-Adresse aus.
5. Wählen Sie Speichern.

AWS CLI

So heben Sie die Zuweisung einer sekundären privaten IP-Adresse auf

Verwenden Sie den Befehl unassign-private-ip-addresses.

```
aws ec2 unassign-private-ip-addresses \
```

```
    --network-interface eni-1234567890abcdef0\
    --private-ip-addresses 10.251.50.12
```

PowerShell

So heben Sie die Zuweisung einer sekundären privaten IP-Adresse auf

Verwenden Sie das cmdlet Unregister-EC2PrivateIpAddress.

```
Unregister-EC2PrivateIpAddress `
    -NetworkInterface eni-1234567890abcdef0 `
    -PrivateIpAddress 10.251.50.12
```

Sekundäre private IPv4-Adresse für Windows-Instance konfigurieren

Sie können Sie mehrere private IPv4-Adressen für Ihre Instances angeben. Nachdem Sie einer Instance eine sekundäre private IPv4-Adresse zugewiesen haben, müssen Sie das Betriebssystem auf der Instance so konfigurieren, dass es die sekundäre private IPv4-Adresse erkennt.

> **Note**
>
> Diese Anweisungen basieren auf Windows Server 2022. Die Implementierung dieser Schritte kann je nach dem auf der Windows-Instance installierten Betriebssystem variieren.

Aufgaben

- Voraussetzungen
- Schritt 1: Statische IP-Adresszuweisung auf Ihrer Instance konfigurieren
- Schritt 2: Konfigurieren einer sekundären privaten IP-Adresse für Ihre Instance
- Schritt 3: Konfigurieren von Anwendungen für die Verwendung der sekundären privaten IP-Adresse

Voraussetzungen

- Weisen Sie der Netzwerkschnittstelle für die Instance die sekundäre private IPv4-Adresse zu. Sie können die sekundäre private IPv4-Adresse zuweisen, wenn Sie die Instance starten oder nachdem die Instance ausgeführt wird. Weitere Informationen finden Sie unter Einer Instance sekundäre IP-Adressen zuweisen.

Schritt 1: Statische IP-Adresszuweisung auf Ihrer Instance konfigurieren

Um für Ihre Windows-Instance die Verwendung von mehreren IP-Adressen zuzulassen, müssen Sie Ihre Instance so konfigurieren, dass anstelle eines DHCP-Servers die statische IP-Adresszuweisung verwendet wird.

> **Important**
>
> Wenn Sie auf Ihrer Instance die statische IP-Adresszuweisung konfigurieren, muss die IP-Adresse mit den Angaben in der Konsole, der CLI oder der API übereinstimmen. Die Instance ist u. U. nicht erreichbar, wenn Sie diese IP-Adressen falsch eingeben.

So konfigurieren Sie die statische IP-Adresszuweisung auf einer Windows-Instance

1. Verbinden Sie sich mit der Instance.
2. Suchen Sie nach der IP-Adresse, der Subnetzmaske und den Standard-Gateway-Adressen für die Instance, indem Sie die folgenden Schritte ausführen:

   - Führen Sie den folgenden Befehl in PowerShell aus:

     ```
     ipconfig /all
     ```

     Überprüfen Sie die Ausgabe und notieren Sie die Werte für IPv4-Adresse, Subnetzmaske, Standard-Gateway und DNS-Server für die Netzwerkschnittstelle. Die Ausgabe sollte wie das folgende Beispiel aussehen:

     ```
     ...

     Ethernet adapter Ethernet 4:

        Connection-specific DNS Suffix  . : us-west-2.compute.internal
        Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
        Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
        IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Lease Obtained. . . . . . . . . . : Monday, April 8, 2024 12:19:29 PM
     ```

```
   Lease Expires . . . . . . . . . . : Monday, April 8, 2024 4:49:30 PM
   Default Gateway . . . . . . . . . : 10.200.0.1
   DHCP Server . . . . . . . . . . . : 10.200.0.1
   DHCPv6 IAID . . . . . . . . . . . : 151166011
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-
E7
   DNS Servers . . . . . . . . . . . : 10.200.0.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

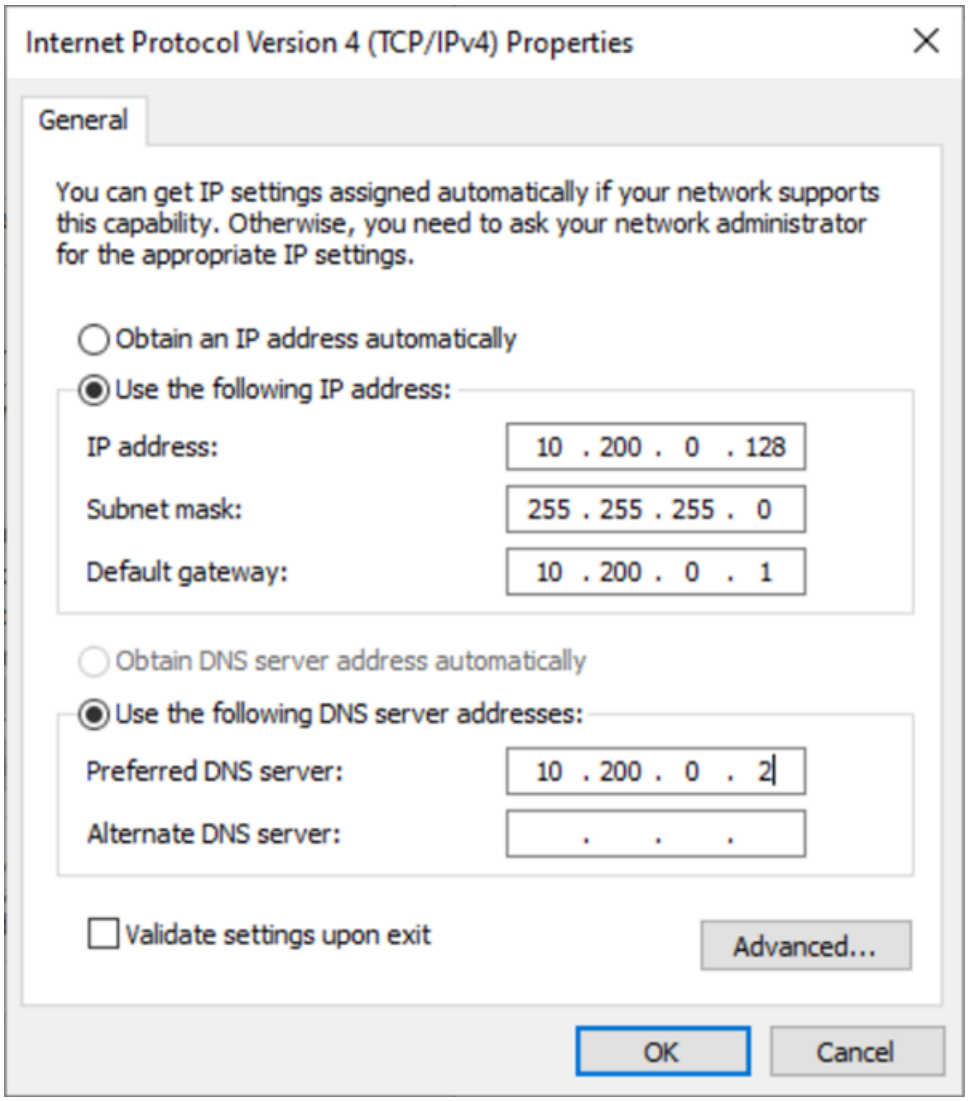
3. Öffnen Sie das Netzwerk- und Freigabecenter, indem Sie den folgenden Befehl in PowerShell ausführen:

```
& $env:SystemRoot\system32\control.exe ncpa.cpl
```

4. Öffnen Sie das Kontextmenü (rechte Maustaste) für die Netzwerkschnittstelle (Local Area Connection oder Ethernet) und wählen Sie Eigenschaften aus.
5. Wählen Sie Internetprotokoll Version 4 (TCP/IPv4) und dann Eigenschaften aus.
6. Wählen Sie im Dialogfeld Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4) die Option Folgende IP-Adresse verwenden: aus, geben Sie folgende Werte ein und wählen Sie anschließend OK.

Feld	Value
IP-Adresse	Die oben in Schritt 2 ermittelte IPv4-Adresse.
Subnetzmaske	Die oben in Schritt 2 ermittelte Subnetzmaske.
Standard-Gateway	Das oben in Schritt 2 ermittelte Standard-Gateway.
Bevorzugter DNS-Server	Der oben in Schritt 2 ermittelte DNS-Server.
Alternativer DNS-Server	Der oben in Schritt 2 ermittelte alternative DNS-Server. Lassen Sie dieses Feld leer, wenn kein alternativer DNS-Server aufgeführt wurde.

> **Important**
>
> Wenn Sie die IP-Adresse auf einen beliebigen anderen Wert als die aktuelle IP-Adresse festlegen, geht die Verbindung zur Instance verloren.



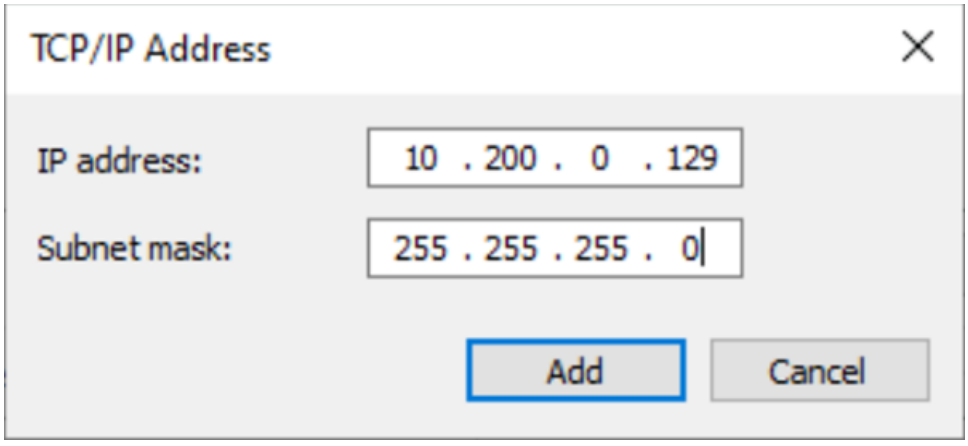
Die RDP-Verbindung zur Windows-Instance geht für einige Sekunden verloren, während die Instance von der DHCP-Adresszuweisung zur statischen Adresszuweisung wechselt. Die Instance behält dieselben IP-Adressinformationen wie zuvor, allerdings sind diese Informationen jetzt statisch und werden nicht vom DHCP-Server verwaltet.

Schritt 2: Konfigurieren einer sekundären privaten IP-Adresse für Ihre Instance

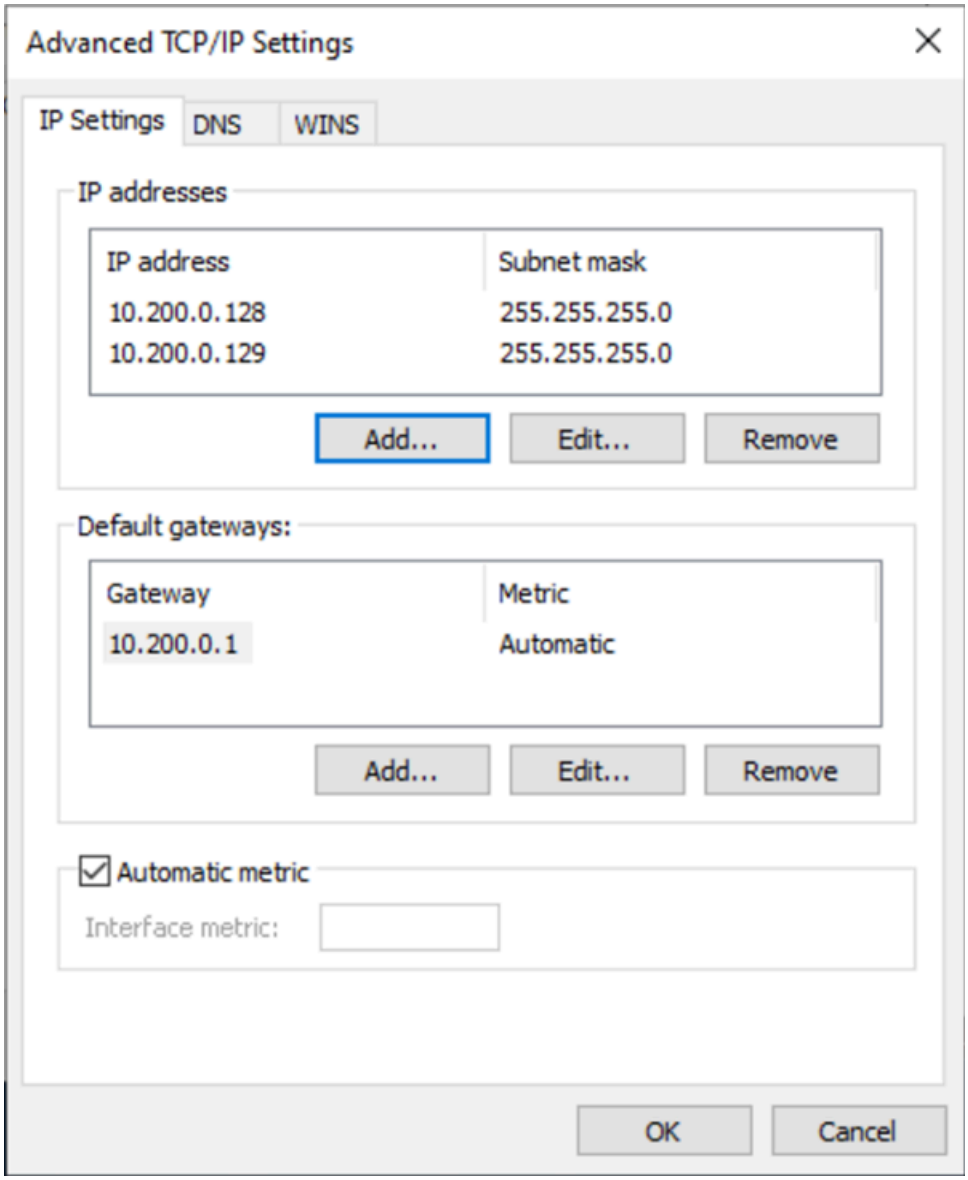
Nachdem Sie die statische IP-Adresszuweisung auf Ihrer Windows-Instance eingerichtet haben, können Sie jetzt eine zweite private IP-Adresse vorbereiten.

So konfigurieren Sie eine sekundäre IP-Adresse

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie anschließend Ihre Instance aus.
3. Notieren Sie sich die auf Networking (Netzwerk) die sekundäre IP-Adresse.
4. Verbinden Sie sich mit der Instance.
5. Wählen Sie auf Ihrer Windows-Instance die Optionen Start und anschließend Systemsteuerung aus.
6. Wählen Sie dann Netzwerk und Internet und anschließend Netzwerk- und Freigabecenter aus.
7. Wählen Sie die Netzwerkschnittstelle (Local Area Connection oder Ethernet) und anschließend die Option Eigenschaften aus.
8. Wählen Sie auf der Seite Eigenschaften von LAN-Verbindung die Option Internetprotokoll Version 4 (TCP/IPv4) und dann Eigenschaften und Erweitert aus.
9. Wählen Sie Add (Hinzufügen) aus.
10. Geben Sie im Dialogfeld TCP/IP-Adresse die sekundäre private IP-Adresse als IP-Adresse ein. Geben Sie unter Subnetzmaske dieselbe Subnetzmaske ein, die Sie für die primäre private IP-Adresse unter Schritt 1: Statische IP-Adresszuweisung auf Ihrer Instance konfigurieren eingegeben haben, und wählen Sie anschließend Hinzufügen aus.



11. Überprüfen Sie die Einstellungen der IP-Adresse und wählen Sie OK.



12. Wählen Sie zuerst OK und dann Schließen aus.
13. Um zu bestätigen, dass die sekundäre IP-Adresse dem Betriebssystem hinzugefügt wurde, führen Sie den Befehl `ipconfig /all` in Powershell aus. Die Ausgabe sollte in etwa wie folgt aussehen:

```
Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
   Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

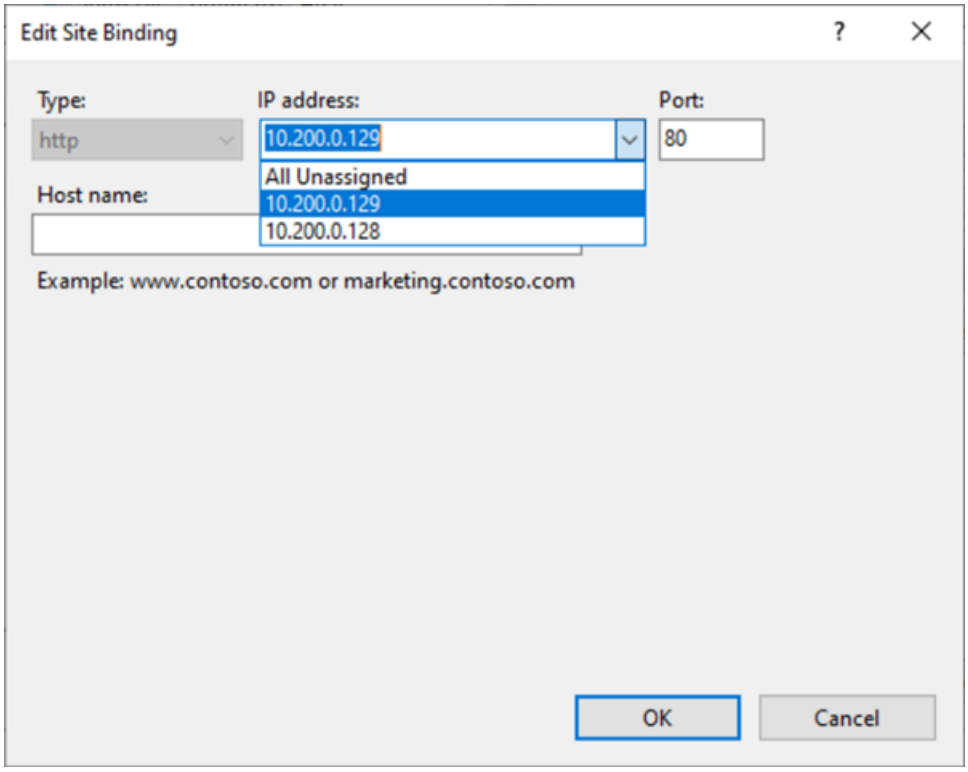
```
Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
IPv4 Address. . . . . . . . . . . : 10.200.0.129(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 10.200.0.1
DHCPv6 IAID . . . . . . . . . . . : 151166011
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-E7
DNS Servers . . . . . . . . . . . : 10.200.0.2
NetBIOS over Tcpip. . . . . . . . : Enabled
```

Schritt 3: Konfigurieren von Anwendungen für die Verwendung der sekundären privaten IP-Adresse

Sie können beliebige Anwendungen für die Verwendung der sekundären privaten IP-Adresse konfigurieren. Beispiel: Wenn Ihre Instance eine Website unter IIS ausführt, können Sie IIS so konfigurieren, dass die sekundäre private IP-Adresse verwendet wird.

So konfigurieren Sie IIS für die Verwendung der sekundären privaten IP-Adresse

1. Verbinden Sie sich mit der Instance.
2. Öffnen Sie den Internetinformationsdienste-Manager (IIS).
3. Erweitern Sie im Bereich Verbindungen die Option Sites.
4. Öffnen Sie das Kontextmenü (rechte Maustaste) für Ihre Website und wählen Sie Bindungen bearbeiten aus.
5. Wählen Sie im Dialogfeld Sitebindungen unter Typ die Option http und anschließend Bearbeiten aus.
6. Wählen Sie im Dialogfeld Sitebindung bearbeiten unter IP-Adresse die sekundäre private IP-Adresse aus. (Standardmäßig akzeptiert jede Website HTTP-Anforderungen von allen IP-Adressen.)



7. Wählen Sie zuerst OK und dann Schließen aus.

Hostnamen und Domains der EC2-Instance

Es ist wichtig, die EC2-Instance-Hostnamen und -Domains zu verstehen, um effektiv Ihre Amazon-EC2-Instances verwalten und darauf zugreifen zu können. Jede EC2-Instance kann verschiedene Arten von Hostnamen haben – private und öffentliche – die unterschiedlichen Zwecken dienen und bestimmten Namenskonventionen folgen.

In diesem Thema werden die Struktur von EC2-Instance-Hostnamen, ihre Konstruktion und die verschiedenen verfügbaren Hostnamentypen erläutert. Sie erfahren, wie Sie Hostnamen-Einstellungen anzeigen und ändern, und lernen, wann Sie die einzelnen Typen verwenden sollten, sowie bewährte Methoden für die Hostnamenverwaltung in Ihrer AWS-Umgebung.

Inhalt

- Hostnamen und Domains der EC2-Instance verstehen
- Hostnamentypen

Hostnamen und Domains der EC2-Instance verstehen

Eine EC2-Instance-Adresse besteht aus verschiedenen Komponenten. Im Folgenden finden Sie ein Beispiel für eine EC2-Instance, die die private IPv4-Adresse der Instance verwendet:

```
   IP address         Domain name
   #--------# #----------------------#
ip-10-24-34-0.us-west-2.compute.internal
#-----------#
  Hostname
#-------------------------------------#
    Fully qualified domain name (FQDN)
```

Wobei Folgendes gilt:

- IP-Adresse: Die primäre IPv4-Adresse der primären Netzwerkschnittstelle, die einer Instance zugeordnet ist.
- Hostname: Der lokale Name einer bestimmten EC2-Instance (wird vom Betriebssystem und zur Identifizierung des lokalen Netzwerks verwendet)
- Domain-Name: Der Teil des FQDN, den AWS bereitstellt
- Vollqualifizierter Domain-Name (FQDN): Die vollständige Adresse, die sowohl den Hostnamen als auch den Domain-Namen enthält. Dies ist die vollständige, weltweit eindeutige Kennung, die verwendet wird, um Ihre Instance netzwerkübergreifend zu erreichen.

Je nachdem, welchen Hostnamentyp Sie für die Instance oder die primäre Netzwerkschnittstelle wählen, die mit der Instance verbunden ist, unterscheiden sich die Formate für Hostnamen und Domain-Namen von dem obigen Beispiel. In diesem Abschnitt werden die Optionen des Hostnamentyps erläutert.

Hostnamentypen

AWS bietet zwei Arten von Hostnamen: private und öffentliche. In der folgenden Tabelle werden die wichtigsten Unterschiede zwischen privaten und öffentlichen Hostnamen verglichen, einschließlich der Art und Weise, wie sie aufgelöst werden, wie sie konfiguriert sind und wann die einzelnen Typen verwendet werden.

	Private Hostnamen	Öffentliche Hostnamen
DNS-Auflösung	Private Hostnamen ermöglichen private FQDNs, die vom öffentlichen Internet aus nicht zugänglich sind. Private Hostnamen erlauben nur die Auflösung von Anfragen an private IPv4- und IPv6-GUA-Adressen innerhalb der VPC.	Öffentliche Hostnamen ermöglich en öffentliche FQDNs, auf die über das öffentliche Internet zugegriffen werden kann. Öffentliche Hostnamen ermöglichen die Auflösung von Anfragen an private IPv4- und IPv6-GUA innerhalb der VPC und an öffentliche IPs aus dem Internet (Split-Horizon-DNS).
Konfiguration	Private Hostnamen werden auf Instance-Ebene konfiguriert.	Öffentliche Hostnamen werden auf der Ebene der Netzwerkschnittstelle konfiguriert.
Wann sollte dies verwendet werden?	• Für Hostnamen, die nur innerhalb Ihrer VPC aufgelöst werden, für interne Kommunikation • Um Ihr internes Benennung sschema geheim zu halten • Um die interne Ressource nverwaltung ohne externe DNS-Überlegungen zu vereinfachen	• Um vom Internet aus über IPv4 und IPv6 auf Instances zuzugreifen • Um eine reibungslose Migration von IPv4 auf IPv6-Umgebungen zu ermöglichen

Inhalt

- Öffentliche Hostnamen
- Private Hostnamen

Öffentliche Hostnamen

Sie können öffentliche Hostnamen für den Zugriff auf EC2-Instances verwenden, wobei Hostnamen verwendet werden, die in die öffentliche IPv4- oder IPv6-Adresse der Instance aufgelöst werden und den Übergang zu IPv6 erleichtern.

Öffentliche Hostnamen ermöglichen Ihnen:

- Über IPv4 und IPv6 auf Ihre EC2-Instances zuzugreifen, was Ihnen mehr Flexibilität bei der Verbindung mit Ihren Ressourcen bietet.
- In Ihrem eigenen Tempo von IPv4 zu IPv6-Umgebungen zu migrieren. Sie können beispielsweise Ihre Datenbank- und Anwendungsmigrationen entkoppeln und so Komplexität und Risiken reduzieren.
- Verwenden Sie mehrere Hostnamenoptionen (nur IPv4, nur IPv6 und Dual-Stack), die automatisch in die entsprechenden IP-Adressen aufgelöst werden.
- Profitieren Sie von verbesserter Sicherheit mit Split-Horizon DNS, das Hostnamen in private IP-Adressen auflöst, wenn sie von Ihrer VPC aus abgefragt werden.

Inhalt

- Typen von öffentlichen Hostnamen und wann sie verwendet werden
- Öffentliche Hostnamen anzeigen
- Ändern Sie die Typen von öffentlichen Hostnamen

Typen von öffentlichen Hostnamen und wann sie verwendet werden

Um öffentliche Hostnamen zu verwenden, müssen Sie eine bestehende Netzwerkschnittstelle ändern. Dieser Abschnitt beschreibt die drei Optionen für öffentliche Hostnamen und hilft Ihnen bei der Entscheidung, welche Sie verwenden möchten:

- Dual-Stack – IP-basierter Name
  - Dies ist die beste Option, wenn Sie von IPv4 auf IPv6 migrieren oder eine Migration planen. Diese Option ermöglicht Konnektivität sowohl über IPv4 als auch über IPv6, was Clients, die möglicherweise eines der beiden Protokolle verwenden, Flexibilität bietet und es den Clients ermöglicht, während der Migration zu IPv6 denselben Hostnamen beizubehalten.
  - Anfragen aus der VPC werden sowohl an die private IPv4-Adresse als auch an die IPv6-Global-Unicast-Adresse (GUA) der Netzwerkschnittstelle aufgelöst. Anfragen aus dem Internet werden sowohl an die öffentliche IPv4- als auch an die IPv6-GUA-Adresse der Netzwerkschnittstelle weitergeleitet.
  - Beispiel
    - Wenn Sie diese Option wählen, wird ein Dual-Stack-FQDN für diese Netzwerkschnittstelle generiert. Dies ist ein Beispiel für den FQDN, der generiert wird:
      - f5lnz-0khrm-nt2u3-gyqqt-nbdl5-q3cdpO.ap-southeast-2.ip.aws

    - Wobei Folgendes gilt:
        - f5lnz-0khrm-nt2u3-gyqqt-nbdl5-q3cdpO ist der Hostname, der eine base36-Darstellung der primären öffentlichen IPv6-Adresse (f5lnz-0khrm-nt2u3-gyqqt-nbdl5) auf der Netzwerkschnittstelle zusammen mit einer base36-Darstellung der primären öffentlichen IPv4-Adresse (q3cdpO) auf der Netzwerkschnittstelle ist.
        - f5lnz-0khrm-nt2u3-gyqqt-nbdl5 wird vom Amazon-DNS-Resolver in die IPv6-GUA-Adresse FFFF:1407:4:f000:81d:2689:1066:4489 aufgelöst. Das ist der erste IPv6-GUA, der der Netzwerkschnittstelle zugewiesen ist.
        - q3cdpO wurde in die IPv4-Adresse 52.54.55.56 aufgelöst. Dies ist die öffentliche IPv4-Adresse, die an die primäre Netzwerkschnittstelle angehängt ist.
        - ap-southeast-2 ist die Region des Subnetzes, in dem sich die Netzwerkschnittstelle befindet.
        - ip.aws ist die Domain, die von AWS bereitgestellt wird.
- IPv6 – IP-basierter Name
    - Dies ist eine gute Option, wenn Sie bereits auf IPv6 migriert sind und Konnektivität nur über IPv6 benötigen.
    - Anfragen aus der VPC oder aus dem Internet werden an die IPv6-GUA der Netzwerkschnittstelle aufgelöst.
    - Beispiel
        - Wenn Sie diese Option wählen, wird ein FQDN für diese Netzwerkschnittstelle generiert. Dies ist ein Beispiel für den FQDN, der generiert wird:
            - f5lnz-0khrm-nt2u3-gyqqt-nbdl5.ap-southeast-2.ip.aws
        - Wobei Folgendes gilt:
            - f5lnz-0khrm-nt2u3-gyqqt-nbdl5 ist ein Hostname, der eine base36-Darstellung der primären öffentlichen IPv6-Adresse auf der Netzwerkschnittstelle ist.
            - f5lnz-0khrm-nt2u3-gyqqt-nbdl5 wird vom Amazon-DNS-Resolver in die IPv6-GUA-Adresse FFFF:1407:4:f000:81d:2689:1066:4489 aufgelöst. Das ist der erste IPv6-GUA, der der Netzwerkschnittstelle zugewiesen ist.
            - ap-southeast-2 ist die Region des Subnetzes, in dem sich die Netzwerkschnittstelle befindet.
            - ip.aws ist die Domain, die von AWS bereitgestellt wird.
- IPv4 – IP-basierter Name
    - Dies ist eine gute Option, wenn die Instance, die diese Netzwerkschnittstelle verwendet, während der Umstellung auf IPv6 den IPv4-Zugriff aufrechterhalten muss oder wenn Anwendungen oder Systeme, die auf der Instance ausgeführt werden, nur IPv4 unterstützen. Dies ist die beste

Option, wenn Sie nur die IPv4-Konnektivität aufrechterhalten müssen und Ihre Workloads keine IPv6-Unterstützung benötigen. Wenn Sie beispielsweise zu IPv6 migrieren, können Sie beschließen, einige Anwendungen auf IPv4 zu belassen, während andere auf IPv6 umsteigen.

- Anfragen aus der VPC werden an die private primäre IPv4-Adresse der Netzwerkschnittstelle aufgelöst. Anfragen aus dem Internet werden an die öffentliche IPv4-Adresse der Netzwerkschnittstelle aufgelöst.
- Beispiel
  - Wenn Sie diese Option wählen, wird ein IPv4-ermöglichter Hostname für diese Netzwerkschnittstelle generiert. Dies ist ein Beispiel für den DNS-Namen, der generiert wird:
    - ec2-52-54-55-66.ap-southeast-2.compute.amazonaws.com
  - Wobei Folgendes gilt:
    - ec2-52-54-55-66 ist ein Hostname, der eine base36-Darstellung der primären öffentlichen IPv4-Adresse einer Netzwerkschnittstelle ist.
    - ec2-52-54-55-66 wird zur IPv4-Adresse 52.54.55.56 aufgelöst. Dies ist die öffentliche IPv4-Adresse, die an die primäre Netzwerkschnittstelle angehängt ist.
    - ap-southeast-2 ist die Region des Subnetzes, in dem sich die Netzwerkschnittstelle befindet.
    - ip.aws ist die Domain, die von AWS bereitgestellt wird.

> **Important**
>
> In den obigen Beispielen können Sie sehen, dass IP-Adressen zur Generierung des Hostnamens verwendet werden. Wenn Sie die primäre private IPv4-Adresse oder die erste IPv6-GUA ändern, die der Netzwerkschnittstelle zugewiesen ist, ändert sich der Teil des Hostnamens, der in die IP-Adresse übersetzt wird, und der zuvor generierte öffentliche Hostname ist nicht mehr gültig. Darüber hinaus erzwingt die Änderung der primären öffentlichen IPv4-Adresse eine nachgelagerte Aktualisierung des Instance Metadata Service (IMDS) im Amazon-EC2-Benutzerhandbuch, sodass die IMDS-Metadaten der EC2-Instance automatisch aktualisiert werden.

Öffentliche Hostnamen anzeigen

Wenn für die VPC, in der sich die Netzwerkschnittstelle befindet, nicht sowohl EnableDnsHostnames als auch EnableDnsSupport aktiviert sind, wird kein Hostnamentyp definiert oder generiert.

Console

Sie können die öffentlichen Hostnamen für eine Instance oder eine primäre Netzwerkschnittstelle anzeigen lassen.

So zeigen Sie den Hostnamentyp und die DNS-Namen einer Instance an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Aktivieren Sie das Kontrollkästchen für die Instance.
4. Suchen Sie auf der Registerkarte Netzwerk unter Hostname und DNS nach folgenden Informationen:
   - Typ des öffentlichen Hostnamens
   - Öffentliches DNS
   - Nur IPv4 – IP-basierter Name
   - Nur IPv6 – IP-basierter Name
   - Dual-Stack – IP-basierter Name

So zeigen Sie den Hostnamentyp und die DNS-Namen einer Netzwerkschnittstelle an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces (Netzwerkschnittstellen) aus.
3. Geben Sie im Suchfeld die ID der Instance ein. Wählen Sie die ID der Netzwerkschnittstelle aus, um die Detailseite zu öffnen.
4. Suchen Sie unter Hostname und DNS nach folgenden Informationen:
   - Typ des öffentlichen Hostnamens
   - Öffentlicher DNS-Name
   - Öffentlicher IPv4-DNS-Name
   - Öffentlicher IPv6-DNS-Name
   - Öffentlicher Dual-Stack-DNS-Name

AWS CLI

So zeigen Sie den Hostnamentyp und die DNS-Namen einer Netzwerkschnittstelle an

Verwenden Sie den Befehl describe-network-interfaces.

```
aws ec2 describe-network-interfaces \
    --network-interface-id eni-1234567890abcdef0 \
    --query NetworkInterfaces[].PublicIpDnsNameOptions
```

Es folgt eine Beispielausgabe. Da der Hostnamentyp `public-dual-stack-dns-name` ist, ist der DNS-Hostname derselbe wie `PublicDualStackDnsName`.

```
[
     {
          "DnsHostnameType": "public-dual-stack-dns-name",
          "PublicIpv4DnsName": "ec2-52-54-55-66.ap-
southeast-2.compute.amazonaws.com",
          "PublicIpv6DnsName": "f5lnz-0khrm-nt2u3-gyqqt-nbdl5.ap-
southeast-2.ip.aws",
          "PublicDualStackDnsName": "f5lnz-0khrm-nt2u3-gyqqt-nbdl5-q3cdp0.ap-
southeast-2.ip.aws"
     }
]
```

PowerShell

So zeigen Sie den Hostnamentyp und die DNS-Namen einer Netzwerkschnittstelle an

Verwenden Sie das cmdlet Get-EC2NetworkInterface.

```
(Get-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0).PublicIpDnsNameOptions
```

Es folgt eine Beispielausgabe. Da der Hostnamentyp `public-dual-stack-dns-name` ist, ist der DNS-Hostname derselbe wie `PublicDualStackDnsName`.

```
DnsHostnameType        : public-dual-stack-dns-name
PublicDualStackDnsName : f5lnz-0khrm-nt2u3-gyqqt-nbdl5-q3cdp0.ap-southeast-2.ip.aws
PublicIpv4DnsName      : ec2-52-54-55-66.ap-southeast-2.compute.amazonaws.com
PublicIpv6DnsName      : f5lnz-0khrm-nt2u3-gyqqt-nbdl5.ap-southeast-2.ip.aws
```

Ändern Sie die Typen von öffentlichen Hostnamen

Die Optionen für öffentliche Hostnamen hängen von den IP-Adressen ab, die der Netzwerkschnittstelle zugeordnet sind:

- Wenn die Netzwerkschnittstelle nur über eine öffentliche IPv4-Adresse verfügt, muss der Hostnamentyp ein IPv4-IP-basierter Name sein.
- Wenn die Netzwerkschnittstelle nur über eine IPv6-Adresse verfügt, muss der Hostnamentyp ein IPv6-IP-basierter Name sein.
- Wenn die Netzwerkschnittstelle sowohl über eine öffentliche IPv4-Adresse als auch über eine IPv6-Adresse verfügt, kann der Hostnamentyp ein Dual-Stack-IP-basierter Name sein.

Voraussetzungen

- Der Netzwerkschnittstelle muss über eine zugeordnete öffentliche IPv4-Adresse oder IPv6-Adresse verfügen.
- Für die VPC, in der sich die Netzwerkschnittstelle befindet, müssen EnableDnsHostnames und EnableDnsSupport aktiviert sein. Weitere Informationen finden Sie unter Anzeigen und Aktualisieren von DNS-Attributen für Ihre VPC im Amazon-VPC-Benutzerhandbuch.

Console

So ändern Sie den öffentlichen Hostnamentyp

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces (Netzwerkschnittstellen) aus.
3. Geben Sie im Suchfeld die ID der Instance ein. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.

   Sie können auch auf der Detailseite der Instance die Registerkarte Netzwerk und dann die ID der Netzwerkschnittstelle für den Geräteindex 0 auswählen.
4. Wählen Sie Aktionen, Typ des öffentlichen Hostnamens ändern.
5. Eine Option auswählen:

   - Dual-Stack – IP-basierter Name: Ein öffentlicher Dual-Stack-Hostname für eine Netzwerkschnittstelle. Anfragen innerhalb der VPC werden sowohl an die private IPv4-Adresse als auch an die globale IPv6-Unicast-Adresse der Netzwerkschnittstelle aufgelöst.

Anfragen aus dem Internet werden sowohl an die öffentliche IPv4- als auch an die IPv6-GUA-Adresse der Netzwerkschnittstelle weitergeleitet.

- IPv4 – IP-basierter Name: Ein IPv4-fähiger öffentlicher Hostname für eine Netzwerkschnittstelle. Anfragen aus der VPC werden an die private primäre IPv4-Adresse der Netzwerkschnittstelle aufgelöst. Anfragen aus dem Internet werden an die öffentliche IPv4-Adresse der Netzwerkschnittstelle aufgelöst.
- IPv6 – IP-basierter Name: Ein IPv6-fähiger öffentlicher Hostname für eine Netzwerkschnittstelle. Anfragen aus der VPC oder aus dem Internet werden an die IPv6-GUA der Netzwerkschnittstelle aufgelöst.

6. Wählen Sie Ändern aus.

AWS CLI

So ändern Sie den öffentlichen Hostnamentyp

Verwenden Sie den Befehl modify-public-ip-dns-name-options.

```
aws ec2 modify-public-ip-dns-name-options \
    --network-interface-id eni-1234567890abcdef0 \
    --hostname-type public-dual-stack-dns-name
```

Es folgt eine Beispielausgabe.

```
{
    "Successful": true
}
```

PowerShell

So ändern Sie den öffentlichen Hostnamentyp

Verwenden Sie das cmdlet Edit-EC2PublicIpDnsNameOption.

```
Edit-EC2PublicIpDnsNameOption `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -HostNameType public-dual-stack-dns-name
```

Private Hostnamen

In diesem Abschnitt werden die privaten Hostnamen der Amazon-EC2-Instance beschrieben, die verfügbar sind, wenn Sie Instances in Ihren VPC-Subnetzen starten.

Der private Hostname unterscheidet die EC2-Instances in Ihrem Netzwerk. Sie können den privaten Hostnamen einer Instance verwenden, wenn Sie beispielsweise Skripte ausführen möchten, um mit einigen oder allen Instances in Ihrem Netzwerk zu kommunizieren.

Inhalt

- Private Hostnamentypen
- Wo die Ressourcennamen und IP-Namen zu finden sind
- Wählen Sie zwischen Ressourcennamen und IP-Namen
- Die ressourcenbasierten Benennungsoptionen für Amazon EC2 ändern

Private Hostnamentypen

Es gibt zwei private Hostnamentypen für den Hostnamen des Gastbetriebssystems, wenn EC2-Instances in einer VPC gestartet werden:

- IP Name (IP-Name): Das Legacy-Namensschema, in dem beim Start einer Instance die Private IPv4-Adresse die Instance im Hostnamen der Instance enthalten ist. Der IP-Adressenname existiert für die Lebensdauer der EC2-Instance. Wenn er als privater DNS-Hostname verwendet wird, wird nur die private IPv4-Adresse (Ein Datensatz) zurückgegeben.
- Resource name (Ressourcenname): Beim Start einer Instance ist die EC2-Instance-ID im Hostnamen der Instance enthalten. Der Ressourcenname existiert für die Lebensdauer der EC2-Instance. Wenn er als privater DNS-Hostname verwendet wird, kann er sowohl die private IPv4-Adresse (A-Datensatz) und/oder die IPv6-Global-Unicast-Adresse (AAAA-Datensatz) zurückgeben.

Der Hostname des EC2-Instance-Gastbetriebssystems hängt von den Subnetzeinstellungen ab:

- Wenn die Instance in ein reines IPv4-Subnetz gestartet wird, können Sie entweder den IP-Namen oder den Ressourcennamen auswählen.
- Wenn die Instance in einem Dual-Stack-Subnetz (IPv4+IPv6) gestartet wird, können Sie entweder den IP-Namen oder den Ressourcennamen auswählen.
- Wenn die Instance in ein reines IPv6-Subnetz gestartet wird, wird automatisch der Ressourcenname verwendet.

Inhalt

- IP-Name
- Ressourcenname
- Der Unterschied zwischen IP-Name und Ressourcenname

IP-Name

Wenn Sie eine EC2-Instance mit dem Hostname-Typ von IP-Name starten, wird der Hostname des Gastbetriebssystems so konfiguriert, dass er die private IPv4-Adresse verwendet.

- Format für eine Instance in us-east-1: *private-ipv4-address*.ec2.internal
- Beispiel: *ip-10-24-34-0*.ec2.internal
- Format für eine Instance in einer anderen AWS-Region: *private-ipv4-address.region*.compute.internal
- Beispiel: *ip-10-24-34-0.us-west-2*.compute.internal

Ressourcenname

Wenn Sie EC2-Instances in reinen IPv6-Subnetzen starten, wird der Hostname type (Hostname-Typ) Resource name (Ressourcenname) standardmäßig ausgewählt. Wenn Sie eine Instance in reinen IPv4-Subnetzen oder Dual-Stack-Subnetzen (IPv4+IPv6) starten, ist der Resource name (Ressourcenname) eine Option, die Sie auswählen können. Nach dem Start einer Instance können Sie die Hostnamenkonfiguration verwalten. Weitere Informationen finden Sie unter Die ressourcenbasierten Benennungsoptionen für Amazon EC2 ändern.

Wenn Sie eine EC2-Instance mit einem Hostname type (Hostname-Typ) Resource name (Ressourcenname) starten, wird der Hostname des Gastbetriebssystems so konfiguriert, dass er die EC2-Instance-ID verwendet.

- Format für eine Instance in us-east-1: *ec2-instance-id*.ec2.internal
- Beispiel: *i-0123456789abcdef*.ec2.internal
- Format für eine Instance in einer anderen AWS-Region: *ec2-instance-id.region*.compute.internal
- Beispiel: *i-0123456789abcdef.us-west-2*.compute.internal

Der Unterschied zwischen IP-Name und Ressourcenname

DNS-Abfragen für IP-Namen und Ressourcennamen existieren nebeneinander, um die Abwärtskompatibilität zu gewährleisten und Ihnen die Migration von der IP-basierten Benennung für Hostnamen zur ressourcenbasierten Benennung zu ermöglichen. Für private DNS-Hostnamen basierend auf IP-Namen können Sie nicht konfigurieren, ob eine DNS-A-Datensatzabfrage für die Instance beantwortet wird oder nicht. DNS-A-Datensatzabfragen werden unabhängig von den Hostnameneinstellungen des Gastbetriebssystems immer beantwortet. Im Gegensatz dazu können Sie für private DNS-Hostnamen basierend auf dem Ressourcennamen konfigurieren, ob DNS-A- und/oder DNS-AAAA-Abfragen für die Instance beantwortet werden oder nicht. Sie konfigurieren das Antwortverhalten, wenn Sie eine Instance starten oder ein Subnetz ändern. Weitere Informationen finden Sie unter Die ressourcenbasierten Benennungsoptionen für Amazon EC2 ändern.

Wo die Ressourcennamen und IP-Namen zu finden sind

Die Host-Namen-Typen, der Ressourcenname und der IP-Name werden in der Amazon-EC2-Konsole angezeigt.

Inhalt

- Beim Erstellen einer EC2-Instance
- Beim Anzeigen der Details einer vorhandenen EC2-Instance

Beim Erstellen einer EC2-Instance

Wenn Sie eine EC2-Instance erstellen, sind je nachdem, welchen Subnetztyp Sie auswählen, Hostname type (Hostname-Typ) und Resource name (Ressourcenname), verfügbar oder er ist möglicherweise ausgewählt und nicht modifizierbar. In diesem Abschnitt wird die Szenarien beschrieben, wo Sie die Hostname-Typen „Ressourcenname“ und „IP-Name“ sehen können.

Szenario 1

Sie erstellen eine EC2-Instance im Assistenten (siehe EC2-Instance mit dem Launch Instance Wizard in der Konsole starten) und wählen bei der Konfiguration der Details ein Subnetz aus, das Sie als nur IPv6 konfiguriert haben.

In diesem Fall wird der Hostname type (Hostname-Typ) Resource name (Ressourcenname) automatisch ausgewählt und kann nicht geändert werden. Die Optionen für den DNS-Hostnamen Enable IP name IPv4 (A record) DNS requests (IP-Namen-IPv4-DNS-Anforderungen (A-Datensatz) aktivieren) und Ressourcenbasierte IP-Namen-IPv4-DNS-Anforderungen (A-Datensatz) aktivieren)

werden automatisch deaktiviert und können nicht geändert werden. Enable resource-based IPv6 (AAAA record) DNS requests (Ressourcenbasierte IPv6-DNS-Anfragen (AAAA-Datensatz) aktibieren) ist standardmäßig ausgewählt, aber modifizierbar. Wenn diese Option aktiviert ist, werden DNS-Anfragen an den Ressourcennamen in die IPv6-Adresse (AAAA-Datensatz) dieser EC2-Instance aufgelöst.

Szenario 2

Sie erstellen eine EC2-Instance im Assistenten (siehe EC2-Instance mit dem Launch Instance Wizard in der Konsole starten) und wählen bei der Konfiguration der Details ein Subnetz aus, das mit einem IPv4-CIDR-Block oder einem IPv4- und IPv6-CIDR-Block („Dual-Stack“) konfiguriert ist.

In diesem Fall ist Enable IP name IPv4 (A record) DNS requests (IP-Namen-IPv4-DNS-Anforderungen (A-Datensatz) aktivieren) automatisch ausgewählt und nicht modifizierbar. Dies bedeutet, dass Anfragen an den IP-Namen an die IPv4-Adresse (A-Datensatz) dieser EC2-Instance aufgelöst werden.

Die Optionen sind standardmäßig auf die Konfigurationen des Subnetzes festgelegt, aber Sie können die Optionen für diese Instance abhängig von den Subnetzeinstellungen ändern:

- Hostname type (Hostnamen-Typ): Bestimmt, ob der Hostname des Gastbetriebssystems der EC2-Instance der Ressourcenname oder der IP-Name sein soll. Der Standardwert ist IP name (IP-Name).
- Enable resource-based IPv4 (A record) DNS requests (Ressourcenbasierte IPv4-DNS-Anforderungen (A-Datensatz) aktivieren): Bestimmt, ob Anforderungen an Ihren Ressourcennamen an die private IPv4-Adresse (A-Datensatz) dieser EC2-Instance aufgelöst werden. Diese Option ist standardmäßig ausgewählt.
- Enable resource-based IPv6 (AAAA record) DNS requests (Ressourcenbasierte IPV6-DNS-Anforderungen (AAAA-Datensatz) aktivieren): Bestimmt, ob Anfragen an Ihren Namen der Ressource an die private IPv6-GUA-Adresse (AAAA-Datensatz) dieser EC2-Instance aufgelöst werden. Diese Option ist standardmäßig nicht ausgewählt.

Beim Anzeigen der Details einer vorhandenen EC2-Instance

Sie können die Hostnamenwerte für eine vorhandene EC2-Instance auf der Registerkarte Details (Details) für die EC2-Instance anzeigen.

- Hostname type (Hostnamen-Typ): Der Hostname im IP-Namen- oder im Ressourcennamenformat.

- Private IP DNS name (IPv4 only) (Privater IP-DNS-Name (nur IPv4)): Der IP-Name, der immer an die private IPv4-Adresse der Instance aufgelöst wird.
- Private resource DNS name (DNS-Name der privaten Ressource): Der Ressourcenname, der zu den für diese Instance ausgewählten DNS-Datensätzen aufgelöst wird.
- Answer private resource DNS name (Mit privatem Ressourcen-DNS-Namen antworten): Der Ressourcenname wird in IPv4 (A)-, IPv6 (AAAA)- oder IPv4- und IPv6-DNS-Datensätze (A und AAAA) aufgelöst.

Wenn Sie sich außerdem direkt über SSH mit Ihrer EC2-Instance verbinden und den `hostname`-Befehl eingeben, wird der Hostname entweder im IP- oder im Ressourcennamenformat angezeigt.

Wählen Sie zwischen Ressourcennamen und IP-Namen

Wenn beim Starten einer EC2-Instance (siehe EC2-Instance mit dem Launch Instance Wizard in der Konsole starten) für den Hostname type (Hostname-Typ) und Resource name (Ressourcenname) entscheiden, wird die EC2-Instance mit einem Hostnamen im Ressourcennamenformat gestartet. In solchen Fällen kann der DNS-Datensatz für diese EC2-Instance auch auf den Ressourcennamen verweisen. Dies gibt Ihnen die Flexibilität zu wählen, ob dieser Hostname in die IPv4-Adresse, die IPv6-Adresse oder sowohl die IPv4- als auch die IPv6-Adresse der Instance aufgelöst wird. Wenn Sie planen, IPv6 in Zukunft zu verwenden oder wenn Sie heute Dual-Stack-Subnetze verwenden, ist es am besten, einen Hostname type (Hostname-Typ) des Resource name (Ressourcennamens) zu verwenden, damit Sie die DNS-Auflösung für die Hostnamen Ihrer Instances ändern können, ohne die DNS-Einträge selbst zu ändern. Der Ressourcenname ermöglicht es Ihnen, IPv4- und IPv6-DNS-Auflösung bei einer EC2-Instance hinzuzufügen und zu entfernen.

Wenn Sie stattdessen einen Hostname type (Hostnamen-Typ) des IP name (IP-Namens) und ihn als DNS-Hostnamen verwenden, kann er nur an die IPv4-Adresse der Instance aufgelöst werden. Er wird nicht an die IPv6-Adresse der Instance aufgelöst, selbst wenn der Instance sowohl eine IPv4-Adresse als auch eine IPv6-Adresse zugeordnet ist.

Die ressourcenbasierten Benennungsoptionen für Amazon EC2 ändern

Sie können den Host-Namen-Typ und die DNS-Host-Namen-Konfigurationen für Subnetze ändern, was sich auf alle nachfolgenden Instance-Starts in diesem Betreff auswirkt, oder Sie können sie für EC2-Instances ändern, nachdem Sie sie gestartet haben.

Ressourcenbasierten Benennungsoptionen

- Hostnamentyp: Legt die Standardeinstellung des Hostnamens des Gastbetriebssystems der im Subnetz gestarteten EC2-Instance fest. Dies ist entweder der Ressourcenname oder der IP-Name.
- DNS-Hostnamen-IPv4-Anforderungen (A-Datensatz) ermöglichen: Bestimmt, ob DNS-Anforderungen/-Abfragen an den Ressourcennamen in die private IPv4-Adresse (A-Datensatz) der EC2-Instance aufgelöst werden.
- DNS-Hostnamen-IPv6-Anforderungen (AAAA-Datensatz) ermöglichen: Bestimmt, ob DNS-Anfragen/-Anforderungen an Ihren Ressourcennamen in die IPv6-Adresse (AAAA-Datensatz) der EC2-Instance aufgelöst werden.

Subnetze

Das Ändern der Subnetzeinstellungen ändert nicht die Konfiguration von EC2-Instances, die bereits im Subnetz gestartet wurden.

Console

So ändern Sie die Optionen für ein Subnetz

Öffnen Sie die Amazon-VPC-Konsole und wählen Sie das Subnetz aus. Wählen Sie Aktionen und VPC-Einstellungen bearbeiten. Ändern Sie nach Bedarf die Einstellungen, und speichern Sie dann Ihre Änderungen.

AWS CLI

So ändern Sie die Optionen für ein Subnetz

Verwenden Sie den Befehl modify-subnet-attribute.

```
aws ec2 modify-subnet-attribute \
    --subnet-id subnet-0abcdef1234567890 \
    --private-dns-hostname-type-on-launch resource-name \
    --enable-resource-name-dns-a-record-on-launch \
    --enable-resource-name-dns-aaaa-record-on-launch
```

PowerShell

So ändern Sie die Optionen für ein Subnetz

Verwenden Sie das cmdlet Edit-EC2SubnetAttribute.

```
Edit-EC2SubnetAttribute `
    -SubnetId subnet-0abcdef1234567890 `
    -PrivateDnsHostnameTypeOnLaunch ResourceName `
    -EnableResourceNameDnsAAAARecordOnLaunch $true `
    -EnableResourceNameDnsARecordOnLaunch $true
```

EC2-Instances

Überlegungen

- Um den Hostnamentyp ändern zu können, müssen Sie zuerst die Instance anhalten. Es ist nicht erforderlich, eine Instance anzuhalten, um die anderen beiden Optionen zu ändern.
- Da Sie eine Instance mit einem Instance-Speicher-Root-Volume nicht anhalten können, können Sie den Hostnamentyp und die DNS-Hostnamen-Optionen nur beim Instance-Start konfigurieren. Nur die folgenden Instance-Typen unterstützen Instance-Speicher-Root-Volumes: C1, C3, D2, I2, M1, M2, M3, R3 und X1.

Console

So ändern Sie die Optionen des Hostnamentyps und des DNS-Hostnamens für eine Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wenn Sie die Einstellung Use resource based naming as guest OS hostname (Ressourcenbasierte Benennungen als Hostnamen des Gastbetriebssystems verwenden) ändern möchten, stoppen Sie zuerst die EC2-Instance. Andernfalls überspringen Sie diesen Schritt.

   Um die Instance zu stoppen, wählen Sie die Instance aus und wählen Sie Instance-Status, Instance stoppen.
3. Wählen Sie die Instance aus und wählen Sie Aktionen, Instance-Einstellungen, Optionen für die ressourcenbasierte Benennung ändern.

   - Use resource based naming as guest OS hostname (Ressourcenbasierte Benennungen als Hostnamen des Gastbetriebssystems verwenden): Bestimmt, ob der Hostname des Gastbetriebssystems der EC2-Instance der Ressourcenname oder der IP-Name sein soll.

- Answer DNS hostname IPv4 (A record) requests (Auf DNS Hostnamen IPv4 (A-Datensatz)-Anforderungen antworten): Bestimmt, ob DNS-Anforderungen/-Abfragen an Ihren Ressourcennamen in die private IPv4-Adresse dieser EC2-Instance aufgelöst werden.
- Auf DNS-Hostnamen-IPv6-Anforderungen (AAAA-Datensatz) antworten: Bestimmt, ob DNS-Anfragen/-Anforderungen an Ihren Ressourcennamen in die IPv6-Adresse (AAAA-Datensatz) dieser EC2-Instance aufgelöst werden.

4. Wählen Sie Speichern.
5. Wenn Sie die Instance gestoppt haben, starten Sie sie erneut.

AWS CLI

So ändern Sie die Optionen des Hostnamentyps und des DNS-Hostnamens für eine Instance

Verwenden Sie den Befehl modify-private-dns-name-options.

```
aws ec2 modify-private-dns-name-options \
    --instance-id i-1234567890abcdef0 \
    --private-dns-hostname-type resource-name \
    --enable-resource-name-dns-a-record \
    --enable-resource-name-dns-aaaa-record
```

PowerShell

So ändern Sie die Optionen des Hostnamentyps und des DNS-Hostnamens für eine Instance

Verwenden Sie das cmdlet Edit-EC2PrivateDNSNameOption.

```
Edit-EC2PrivateDnsNameOption `
    -InstanceId i-1234567890abcdef0 `
    -PrivateDnsHostnameType ResourceName `
    -EnableResourceNameDnsAAAARecord $true`
    -EnableResourceNameDnsARecord $true
```

Bringen Sie Ihre eigenen IP-Adressen (BYOIP) zu Amazon EC2

Sie können einen Teil oder den gesamten öffentlich routbaren Bereich IPv4 oder IPv6 Adressbereich aus Ihrem lokalen Netzwerk in Ihr übertragen. AWS-Konto Sie haben weiterhin die Kontrolle über den

Adressbereich und können den Adressbereich im Internet über bewerben. AWS Nachdem Sie den Adressbereich zu Amazon gebracht haben EC2, wird er in Ihrem AWS-Konto Adresspool angezeigt.

> **Note**
>
> In dieser Dokumentation wird beschrieben, wie Sie Ihren eigenen IP-Adressbereich EC2 nur zur Verwendung in Amazon verwenden können. Informationen zur Verwendung in AWS Global Accelerator Ihrem eigenen IP-Adressbereich finden Sie unter Bring your own IP Addresses (BYOIP) im AWS Global Accelerator Entwicklerhandbuch. Informationen zur Verwendung mit Amazon VPC IP Address Manager Ihrem eigenen IP-Adressbereich finden Sie unter Tutorial: Bringen Sie Ihre IP-Adressen zu IPAM im Amazon VPC IPAM-Benutzerhandbuch.

Wenn Sie einen IP-Adressbereich hinzufügen, wird AWS bestätigt AWS, dass Sie den IP-Adressbereich kontrollieren. Sie können mit zwei Methoden überprüfen, ob Sie den Bereich kontrollieren:

- Wenn Ihr IP-Adressbereich bei einem Internetregister registriert ist, das RDAP unterstützt (wie ARIN, RIPE und APNIC), können Sie ein X.509-Zertifikat verwenden, um die Eigentümerschaft Ihrer Domain zu überprüfen. Das Zertifikat darf nur für die Dauer des Bereitstellungsprozesses gültig sein. Sie können das Zertifikat aus dem Verzeichnis Ihres RIRs entfernen, nachdem die nachfolgende Bereitstellungsphase abgeschlossen ist.
- Unabhängig davon, ob Ihr Internetregister RDAP unterstützt, können Sie ein Amazon VPC IPAM und einen DNS-TXT-Datensatz verwenden, um die Eigentümerschaft Ihrer Domain zu überprüfen. Dieser Vorgang ist unter Tutorial: Bringen Sie Ihre IP-Adressen zu IPAM im Amazon-VPC-IPAM-Benutzerhandbuch dokumentiert.

Weitere Informationen finden Sie im AWS Online-Tech-Talk Deep Dive zum Thema Bring Your Own IP.

Inhalt

- BYOIP-Definitionen
- Voraussetzungen und Kontingente
- Regionale Verfügbarkeit
- Verfügbarkeit der Local Zone

- Voraussetzungen für BYOIP in Amazon EC2
- Integrieren Sie Ihren Adressbereich zur Verwendung in Amazon EC2
- Verwenden Sie Ihren BYOIP-Adressbereich in Amazon EC2

BYOIP-Definitionen

- Selbstsigniertes X.509-Zertifikat – ein Zertifikatsstandard, der am häufigsten zum Verschlüsseln und Authentifizieren von Daten innerhalb eines Netzwerks verwendet wird. Es handelt sich um ein Zertifikat, das verwendet wird AWS , um die Kontrolle über den IP-Bereich anhand eines RDAP-Datensatzes zu validieren. Weitere Informationen zu X.509-Zertifikaten finden Sie unter RFC 3280.
- Autonome Systemnummer (ASN) – Eine weltweit eindeutige Kennung, die eine Gruppe von IP-Präfixen definiert, die von einem oder mehreren Netzwerkbetreibern betrieben werden und eine einzige, klar definierte Routing-Richtlinie einhalten.
- Regional Internet Registry (RIR) — Eine Organisation, die die Zuweisung und Registrierung von IP-Adressen ASNs innerhalb einer Region der Welt verwaltet.
- Registry Data Access Protocol (RDAP) – Ein schreibgeschütztes Protokoll zur Abfrage aktueller Registrierungsdaten innerhalb einer RIR. Einträge in der abgefragten RIR-Datenbank werden als „RDAP-Einträge“ bezeichnet. Bestimmte Datensatztypen müssen von Kunden über einen von RIR bereitgestellten Mechanismus aktualisiert werden. Diese Datensätze werden von abgefragt, AWS um die Kontrolle über einen Adressraum im RIR zu überprüfen.
- Route Origin Authorization (ROA) — Ein Objekt, das von Kunden RIRs zur Authentifizierung von IP-Werbung in bestimmten autonomen Systemen erstellt wurde. Eine Übersicht finden Sie unter Route Origin-Autorisierungen (ROAs) auf der ARIN-Website.
- Local Internet Registry (LIR) – Organisationen wie Internet-Serviceanbieter, die ihren Kunden einen Block von IP-Adressen aus einem RIR zuweisen.

Voraussetzungen und Kontingente

- Der Adressbereich muss bei Ihrem regionalen Internetregister (RIR) registriert sein. Alle Richtlinien in Bezug auf geografische Regionen finden Sie in Ihrem RIR. BYOIP unterstützt derzeit die Registrierung im American Registry for Internet Numbers (ARIN), dem Réseaux IP Européens Network Coordination Centre (RIPE) oder dem Asia-Pacific Network Information Centre (APNIC). Er muss auf ein Unternehmen oder eine juristische Person registriert sein und kann nicht auf eine natürliche Person registriert werden.

- Der spezifischste IPv4 Adressbereich, den Sie angeben können, ist /24.
- Der spezifischste IPv6 Adressbereich, den Sie angeben können, ist /48 für solche CIDRs , die öffentlich beworben werden können, und /60 für solche CIDRs , die nicht öffentlich beworben werden können.
- ROAs sind für CIDR-Bereiche, die nicht öffentlich beworben werden können, nicht erforderlich, aber die RDAP-Einträge müssen trotzdem aktualisiert werden.
- Sie können jeden Adressbereich jeweils einer AWS Region zuordnen.
- Sie können Ihrem Konto insgesamt fünf BYOIP IPv4 - und IPv6 Adressbereiche pro AWS Region hinzufügen AWS . Sie können die Kontingente für BYOIP nicht CIDRs mit der Servicekontingenten-Konsole anpassen, aber Sie können eine Erhöhung des Kontingents beantragen, indem Sie sich an das AWS Support Center wenden, wie unter AWS Service Quotas in der beschrieben. Allgemeine AWS-Referenz
- Sie können Ihren IP-Adressbereich nicht mit anderen Konten teilen, AWS RAM es sei denn, Sie verwenden Amazon VPC IP Address Manager (IPAM) und integrieren IPAM mit Organizations. AWS Weitere Informationen finden Sie unter Integrate IPAM with AWS Organizations im Amazon VPC IPAM-Benutzerhandbuch.
- Die Adressen im IP-Adressbereich müssen über einen sauberen Verlauf verfügen. Wir könnten die Reputation des IP-Adressbereichs untersuchen und uns das Recht vorbehalten, einen IP-Adressbereich abzulehnen, wenn er eine IP-Adresse enthält, die eine schlechte Reputation hat oder mit schädlichem Verhalten in Verbindung gebracht wird.
- Für den Legacy-Adressraum, IPv4 also den Adressraum, der vor der Gründung des Regional Internet Registry (RIR) -Systems vom Zentralregister der Internet Assigned Numbers Authority (IANA) verteilt wurde, ist weiterhin ein entsprechendes ROA-Objekt erforderlich.
- Denn LIRs es ist üblich, dass sie ihre Datensätze manuell aktualisieren. Die Bereitstellung kann je nach LIR mehrere Tage dauern.
- Für einen großen CIDR-Block werden ein einzelnes ROA-Objekt und ein RDAP-Datensatz benötigt. Mithilfe eines einzigen Objekts und Datensatzes können Sie mehrere kleinere CIDR-Blöcke aus diesem Bereich in mehrere AWS Regionen übertragen. AWS
- BYOIP wird für Wellenlängenzonen oder aktiviert nicht unterstützt. AWS Outposts
- Nehmen Sie keine manuellen Änderungen für BYOIP RADb oder andere IRR vor. BYOIP wird automatisch aktualisiert. RADb Alle manuellen Änderungen, welche die BYOIP-ASN beinhalten, führen dazu, dass der BYOIP-Bereitstellungsvorgang fehlschlägt.

- Sobald Sie einen IPv4 Adressbereich eingegeben haben AWS, können Sie alle IP-Adressen in diesem Bereich verwenden, einschließlich der ersten Adresse (der Netzwerkadresse) und der letzten Adresse (der Broadcast-Adresse).

Regionale Verfügbarkeit

Das BYOIP-Feature ist derzeit in allen kommerziellen AWS -Regionen mit Ausnahme der Regionen China verfügbar.

Verfügbarkeit der Local Zone

Eine lokale Zone ist eine Erweiterung einer AWS Region in geografischer Nähe zu Ihren Benutzern. Local Zones werden in „Netzwerkgrenzgruppen“ gruppiert. In AWS ist eine Netzwerkgrenzgruppe eine Sammlung von Availability Zones (AZs), Local Zones oder Wavelength Zones, von denen aus eine AWS öffentliche IP-Adresse beworben wird. Local Zones können andere Netzwerkgrenzgruppen als die innerhalb AZs einer AWS Region haben, um eine minimale Latenz oder physische Entfernung zwischen dem AWS Netzwerk und den Kunden sicherzustellen, die auf die Ressourcen in diesen Zonen zugreifen.

Mit dieser `--network-border-group` Option können Sie BYOIPv4 Adressbereiche für die folgenden Netzwerkgrenzgruppen der lokalen Zone bereitstellen und für sie werben:

- af-south-1-los-1
- ap-northeast-1-tpe-1
- ap-south-1-ccu-1
- ap-south-1-del-1
- ap-southeast-1-bkk-1
- ap-southeast-1-mnl-1
- ap-southeast-2-akl-1
- ap-southeast-2-per-1
- eu-central-1-ham-1
- eu-central-1-waw-1
- eu-north-1-cph-1
- eu-north-1-hel-1
- me-south-1-mct-1

- us-east-1-atl-2
- us-east-1-bos-1
- us-east-1-bue-1
- us-east-1-chi-2
- us-east-1-dfw-2
- us-east-1-iah-2
- us-east-1-lim-1
- us-east-1-mci-1
- us-east-1-mia-2
- us-east-1-msp-1
- us-east-1-nyc-1
- us-east-1-nyc-2
- us-east-1-phl-1
- us-east-1-qro-1
- us-east-1-scl-1
- us-west-2-den-1
- us-west-2-hnl-1
- us-west-2-las-1
- us-west-2-lax-1
- us-west-2-pdx-1
- us-west-2-phx-2
- us-west-2-sea-1

Wenn Sie Local Zones aktiviert haben (siehe Aktivieren einer lokalen Zone), können Sie bei der Bereitstellung und Ankündigung eines BYOIPv4 CIDR eine Netzwerkgrenzgruppe für Local Zones auswählen. Wählen Sie die Netzwerkgrenzgruppe sorgfältig aus, da sich die EIP und die AWS Ressource, der sie zugeordnet ist, in derselben Netzwerkgrenzgruppe befinden müssen.

> **Note**
>
> Sie können derzeit keine BYOIPv6 Adressbereiche in Local Zones bereitstellen oder bewerben.

Voraussetzungen für BYOIP in Amazon EC2

Der Onboarding-Prozess für BYOIP hat zwei Phasen, für die Sie drei Schritte ausführen müssen. Diese Schritte werden im folgenden Diagramm dargestellt. Wir schließen manuelle Schritte in diese Dokumentation ein, aber Ihr RIR bietet möglicherweise verwaltete Services an, um Sie bei diesen Schritten zu unterstützen.

> **Tip**
>
> Die Aufgaben in diesem Abschnitt erfordern ein Linux-Terminal und können mit Linux AWS CloudShell, dem oder dem Windows-Subsystem für Linux ausgeführt werden.

Inhalt

- Übersicht
- Einen privaten Schlüssel erstellen und ein X.509-Zertifikat generieren
- Das X.509-Zertifikat in den RDAP-Eintrag in Ihrem RIR hochladen
- Erstellen eines ROA-Objekts in Ihrem RIR

Übersicht

Vorbereitungsphase

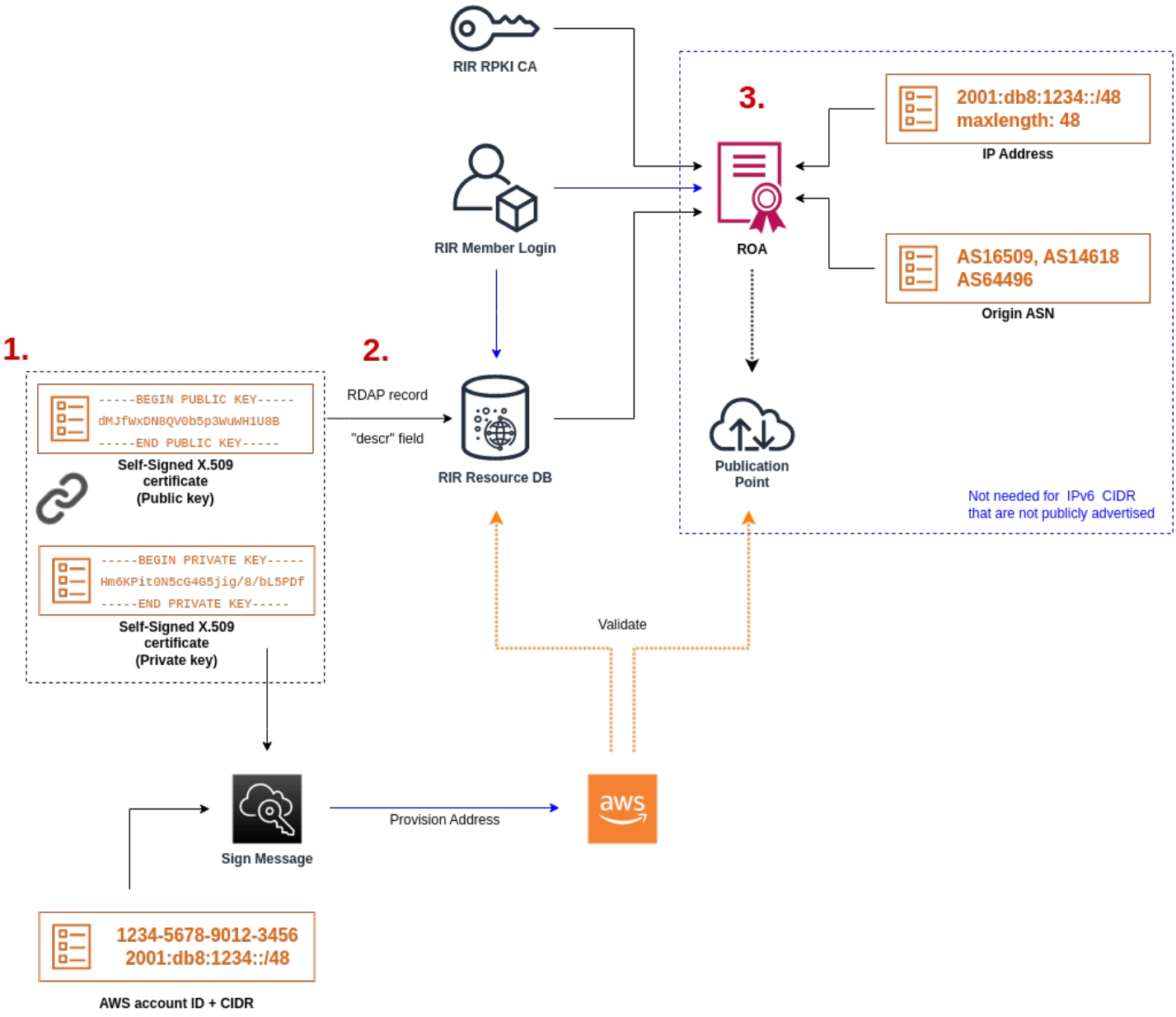
[1] Erstellen Sie einen privaten Schlüssel und verwenden Sie ihn zum Generieren eines selbstsignierten X.509-Zertifikats. Dieses Zertifikat wird nur während der Bereitstellungsphase verwendet. Sie können das Zertifikat aus dem Verzeichnis Ihres RIRs entfernen, wenn die nachfolgende Bereitstellungsphase abgeschlossen ist

RIR-Konfigurationsphase

[2] Laden Sie das selbstsignierte Zertifikat in Ihre Kommentare zum RDAP-Datensatz hoch.

3] Erstellen Sie ein ROA-Objekt in Ihrem RIR. Der ROA definiert den gewünschten Adressbereich, die Autonomous System Numbers (ASNs), die für den Adressbereich werben dürfen, und ein Ablaufdatum für die Registrierung bei der Resource Public Key Infrastructure (RPKI) Ihres RIR.

> **Note**
>
> Für Adressräume, die nicht öffentlich beworben werden können, ist kein ROA erforderlich. IPv6



Um mehrere nicht zusammenhängende Adressbereiche einzubeziehen, müssen Sie diesen Vorgang mit jedem Adressbereich wiederholen. Die Schritte zur Vorbereitung und RIR-Konfiguration müssen jedoch nicht wiederholt werden, wenn ein zusammenhängender Block auf mehrere verschiedene Regionen aufgeteilt wird. AWS

Das Aktivieren eines Adressbereichs hat keine Auswirkungen auf Adressbereiche, die Sie zuvor aktiviert haben.

Einen privaten Schlüssel erstellen und ein X.509-Zertifikat generieren

Gehen Sie zum Erstellen eines selbsignierten X.509-Zertifikats folgendermaßen vor und fügen Sie es dann zum RDAP-Datensatz für Ihr RIR hinzu. Dieses Schlüsselpaar dient zur Authentifizierung des Adressbereichs im RIR. Für die openssl-Befehle ist OpenSSL Version 1.0.2 oder höher erforderlich.

Kopieren Sie die folgenden Befehle und ersetzen Sie nur die Platzhalterwerte (in farbigem kursivem Text).

Dieses Verfahren folgt der bewährten Methode, Ihren privaten RSA-Schlüssel zu verschlüsseln und zum Zugriff darauf eine Passphrase zu erfordern.

1. Generieren Sie einen privaten RSA-Schlüssel mit 2 048 Bit, wie im Folgenden gezeigt.

   ```
   $ openssl genpkey -aes256 -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out
    private-key.pem
   ```

   Der Parameter `-aes256` gibt den Algorithmus an, der zum Verschlüsseln des privaten Schlüssels verwendet wird. Der Befehl gibt die folgende Ausgabe zurück, einschließlich Aufforderungen zum Festlegen einer Passphrase:

   ```
   ......+++
   .+++
   Enter PEM pass phrase: xxxxxxx
   Verifying - Enter PEM pass phrase: xxxxxxx
   ```

   Sie können den Schlüssel mit dem folgenden Befehl prüfen:

   ```
   $ openssl pkey -in private-key.pem -text
   ```

   Dadurch wird eine Eingabeaufforderung für die Passphrase und der Inhalt des Schlüssels zurückgegeben, der etwa wie folgt aussehen sollte:

   ```
   Enter pass phrase for private-key.pem: xxxxxxx
   -----BEGIN PRIVATE KEY-----
   MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDFBXHRI4HVKAhh
   3seiciooizCRTbJe1+YsxNTja4XyKypVGIFWDGhZs44FCHlPOOSVJ+NqP74w96oM
   ```

```
7DPS3xo9kaQyZBFn2YEp2EBq5vf307KHNRmZZUmkn0zHOSEpNmY2fMxISBxewlxR
FAniwmSd/8TDvHJMY9FvAIvWuTsv5l0tJKk+a91K4+tO3UdDR7Sno5WXExfsBrW3
g1ydo3TBsx8i5/YiVOcNApy7ge2/FiwY3aCXJB6r6nuF6H8mRgI4r4vkMRsOlAhJ
DnZPNeweboo+K3Q3lwbgbmOKD/z9svk8N/+hUTBtIX0fRtbG+PLIw3xWRHGrMSn2
BzsPVuDLAgMBAAECggEACiJUj2hfJkKv47Dc3es3Zex67A5uDVjXmxfox2Xhdupn
fAcNqAptV6fXt0SPUNbhUxbBKNbshoJGufFwXPli1SXnpzvkdU4Hyco4zgbhXFsE
RNYjYfOGzTPwdBLpNMB6k3Tp4RHse6dNrlH0jDhpioL8cQEBdBJyVF5X0wymEbmV
mC0jgH/MxsBAPWW6ZKicg9ULMlWiAZ3MRAZPjHHgpYkAAsUWKAbCBwVQcVjGO59W
jfZjzTX5pQtVVH68ruciH88DTZCwjCkjBhxg+OIkJBLE5wkh82jIHSivZ63flwLw
z+E0+HhELSZJrn2MY6Jxmik3qNNUOF/Z+3msdj2luQKBgQDjwlC/3jxp8zJy6P8o
JQKv7TdvMwUj4VSWOHZBHLv4evJaaia0uQjIo1UDa8AYitqhX1NmCCehGH8yuXj/
v6V3CzMKDkmRr1NrONnSz5QsndQ04Z6ihAQlPmJ96g4wKtgoC7AYpyP0g1a+4/sj
b1+o3YQI4pD/F71c+qaztH7PRwKBgQDdc23yNmT3+Jyptf0fKjEvONK+xwUKzi9c
L/OzBq5yOIC1Pz2T85gOe1i8kwZws+xlpG6uBT6lmIJELd0k59FyupNu4dPvX5SD
6GGqdx4jk9KvI74usGeOBohmF0phTHkrWKBxXiyT0oS8zjnJlEn8ysIpGgO28jjr
LpaHNZ/MXQKBgQDfLNcnS0LzpsS2aK0tzyZU8SMyqVHOGMxj7quhneBq2T6FbiLD
T9TVlYaGNZ0j71vQaLI19qOubWymbautH0Op5KV8owdf4+bf1/NJaPIOzhDUSIjD
Qo01WW31Z9XDSRhKFTnWzmCjBdeIcajyzf10YKsycaAW9lItu8aBrMndnQKBgQDb
nNp/JyRwqjOrNljk7DHEs+SD39kHQzzCfqd+dnTPv2sc06+cpym3yulQcbokULpy
fmRo3bin/pvJQ3aZX/Bdh9woTXqhXDdrrSwWInVYMQPyPk8f/D9mIOJp5FUWMwHD
U+whIZSxsEeE+jtixlWtheKRYkQmzQZXbWdIhYyI3QKBgD+F/6wcZ85QW8nAUykA
3WrSIx/3cwDGdm4NRGct8ZOZjTHjiy9ojMOD1L7iMhRQ/3k3hUsin5LDMp/ryWGG
x4uIaLat40kiC7T4I66DM7P59euqdz3w0PD+VU+h7GSivvsFDdySUt7bNK0AUVLh
dMJfWxDN8QV0b5p3WuWH1U8B
-----END PRIVATE KEY-----
Private-Key: (2048 bit)
modulus:
    00:c5:05:71:d1:23:81:d5:28:08:61:de:c7:a2:72:
    2a:28:8b:30:91:4d:b2:5e:d7:e6:2c:c4:d4:e3:6b:
    85:f2:2b:2a:55:18:81:56:0c:68:59:b3:8e:05:08:
    79:4f:38:e4:95:27:e3:6a:3f:be:30:f7:aa:0c:ec:
    33:d2:df:1a:3d:91:a4:32:64:11:67:d9:81:29:d8:
    40:6a:e6:f7:f7:d3:b2:87:35:19:99:65:49:a4:9f:
    4c:c7:39:21:29:36:66:36:7c:cc:48:48:1c:5e:c2:
    5c:51:14:09:e2:c2:64:9d:ff:c4:c3:bc:72:4c:63:
    d1:6f:00:8b:d6:b9:3b:2f:e6:5d:2d:24:a9:3e:6b:
    dd:4a:e3:eb:4e:dd:47:43:47:b4:a7:a3:95:97:13:
    17:ec:06:b5:b7:83:5c:9d:a3:74:c1:b3:1f:22:e7:
    f6:22:54:e7:0d:02:9c:bb:81:ed:bf:16:2c:18:dd:
    a0:97:24:1e:ab:ea:7b:85:e8:7f:26:46:02:38:af:
    8b:e4:31:1b:0e:94:08:49:0e:76:4f:35:ec:1e:6e:
    8a:3e:2b:74:37:97:06:e0:6e:63:8a:0f:fc:fd:b2:
    f9:3c:37:ff:a1:51:30:6d:21:7d:1f:46:d6:c6:f8:
    f2:c8:c3:7c:56:44:71:ab:31:29:f6:07:3b:0f:56:
```

```
    e0:cb
publicExponent: 65537 (0x10001)
privateExponent:
    0a:22:54:8f:68:5f:26:42:af:e3:b0:dc:dd:eb:37:
    65:ec:7a:ec:0e:6e:0d:58:d7:9b:17:e8:c7:65:e1:
    76:ea:67:7c:07:0d:a8:0a:6d:57:a7:d7:b7:44:8f:
    50:d6:e1:53:16:c1:28:d6:ec:86:82:46:b9:f1:70:
    5c:f9:62:d5:25:e7:a7:3b:e4:75:4e:07:c9:ca:38:
    ce:06:e1:5c:5b:04:44:d6:23:61:f3:86:cd:33:f0:
    74:12:e9:34:c0:7a:93:74:e9:e1:11:ec:7b:a7:4d:
    ae:51:f4:8c:38:69:8a:82:fc:71:01:01:74:12:72:
    54:5e:57:d3:0c:a6:11:b9:95:98:2d:23:80:7f:cc:
    c6:c0:40:3d:65:ba:64:a8:9c:83:d5:0b:32:55:a2:
    01:9d:cc:44:06:4f:8c:71:e0:a5:89:00:02:c5:16:
    28:06:c2:07:05:50:71:58:c6:3b:9f:56:8d:f6:63:
    cd:35:f9:a5:0b:55:54:7e:bc:ae:e7:22:1f:cf:03:
    4d:90:b0:8c:29:23:06:1c:60:f8:e2:24:24:12:c4:
    e7:09:21:f3:68:c8:1d:28:af:67:ad:df:97:02:f0:
    cf:e1:34:f8:78:44:2d:26:49:ae:7d:8c:63:a2:71:
    9a:29:37:a8:d3:54:38:5f:d9:fb:79:ac:76:3d:a5:
    b9
prime1:
    00:e3:c2:50:bf:de:3c:69:f3:32:72:e8:ff:28:25:
    02:af:ed:37:6f:33:05:23:e1:54:96:38:76:41:1c:
    bb:f8:7a:f2:5a:6a:26:b4:b9:08:c8:a3:55:03:6b:
    c0:18:8a:da:a1:5f:53:66:08:27:a1:18:7f:32:b9:
    78:ff:bf:a5:77:0b:33:0a:0e:49:91:af:53:6b:38:
    d9:d2:cf:94:2c:9d:d4:34:e1:9e:a2:84:04:25:3e:
    62:7d:ea:0e:30:2a:d8:28:0b:b0:18:a7:23:f4:83:
    56:be:e3:fb:23:6f:5f:a8:dd:84:08:e2:90:ff:17:
    bd:5c:fa:a6:b3:b4:7e:cf:47
prime2:
    00:dd:73:6d:f2:36:64:f7:f8:9c:a9:b5:fd:1f:2a:
    31:2f:38:d2:be:c7:05:0a:ce:2f:5c:2f:f3:b3:06:
    ae:72:38:80:b5:3f:3d:93:f3:98:0e:7b:58:bc:93:
    06:70:b3:ec:65:a4:6e:ae:05:3e:a5:98:82:44:2d:
    dd:24:e7:d1:72:ba:93:6e:e1:d3:ef:5f:94:83:e8:
    61:aa:77:1e:23:93:d2:af:23:be:2e:b0:67:8e:06:
    88:66:17:4a:61:4c:79:2b:58:a0:71:5e:2c:93:d2:
    84:bc:ce:39:c9:94:49:fc:ca:c2:29:1a:03:b6:f2:
    38:eb:2e:96:87:35:9f:cc:5d
exponent1:
    00:df:2c:d7:27:4b:42:f3:a6:c4:b6:68:ad:2d:cf:
    26:54:f1:23:32:a9:51:ce:18:cc:63:ee:ab:a1:9d:
```

```
    e0:6a:d9:3e:85:6e:22:c3:4f:d4:d5:95:86:86:35:
    9d:23:ef:5b:d0:68:b2:35:f6:a3:ae:6d:6c:a6:6d:
    ab:ad:1f:43:a9:e4:a5:7c:a3:07:5f:e3:e6:df:d7:
    f3:49:68:f2:0e:ce:10:d4:48:88:c3:42:8d:35:59:
    6d:f5:67:d5:c3:49:18:4a:15:39:d6:ce:60:a3:05:
    d7:88:71:a8:f2:cd:fd:74:60:ab:32:71:a0:16:f6:
    52:2d:bb:c6:81:ac:c9:dd:9d
exponent2:
    00:db:9c:da:7f:27:24:70:aa:33:ab:36:58:e4:ec:
    31:c4:b3:e4:83:df:d9:07:43:3c:c2:7e:a7:7e:76:
    74:cf:bf:6b:1c:d3:af:9c:a7:29:b7:ca:e9:50:71:
    ba:24:50:ba:72:7e:64:68:dd:b8:a7:fe:9b:c9:43:
    76:99:5f:f0:5d:87:dc:28:4d:7a:a1:5c:37:6b:ad:
    2c:16:22:75:58:31:03:f2:3e:4f:1f:fc:3f:66:20:
    e2:69:e4:55:16:33:01:c3:53:ec:21:21:94:b1:b0:
    47:84:fa:3b:62:c6:55:ad:85:e2:91:62:44:26:cd:
    06:57:6d:67:48:85:8c:88:dd
coefficient:
    3f:85:ff:ac:1c:67:ce:50:5b:c9:c0:53:29:00:dd:
    6a:d2:23:1f:f7:73:00:c6:76:6e:0d:44:67:2d:f1:
    93:99:8d:31:e3:8b:2f:68:8c:c3:83:d4:be:e2:32:
    14:50:ff:79:37:85:4b:22:9f:92:c3:32:9f:eb:c9:
    61:86:c7:8b:88:68:b6:ad:e3:49:22:0b:b4:f8:23:
    ae:83:33:b3:f9:f5:eb:aa:77:3d:f0:d0:f0:fe:55:
    4f:a1:ec:64:a2:be:fb:05:0d:dc:92:52:de:db:34:
    ad:00:51:52:e1:74:c2:5f:5b:10:cd:f1:05:74:6f:
    9a:77:5a:e5:87:d5:4f:01
```

Bewahren Sie Ihren privaten Schlüssel an einem sicheren Ort auf, wenn er nicht verwendet wird.

2. Generieren Sie ein X.509-Zertifikat unter Verwendung des im vorherigen Schritt erstellten privaten Schlüssels. In diesem Beispiel läuft das Zertifikat nach 365 Tagen ab und ist dann nicht mehr vertrauenswürdig. Stellen Sie sicher, das Sie das Ablaufdatum korrekt festlegen. Das Zertifikat darf nur für die Dauer des Bereitstellungsprozesses gültig sein. Sie können das Zertifikat aus dem Verzeichnis Ihres RIRs entfernen, nachdem die nachfolgende Bereitstellungsphase abgeschlossen ist. Der `tr -d "\n"`-Befehl entfernt Zeilenvorschubzeichen (Zeilenumbrüche) aus der Ausgabe. Sie müssen einen Common Name angeben, wenn Sie dazu aufgefordert werden, aber die übrigen Felder können leer gelassen werden.

```
$ openssl req -new -x509 -key private-key.pem -days 365 | tr -d "\n" >
 certificate.pem
```

Daraus resultiert eine Ausgabe ähnlich der folgenden:

```
Enter pass phrase for private-key.pem: xxxxxxx
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, fully qualified host name) []:example.com
Email Address []:
```

> **Note**
>
> Der Common Name wird für die Bereitstellung nicht benötigt. AWS Der Domain-Name kann intern oder öffentlich sein.

Sie können das Zertifikat mit dem folgenden Befehl prüfen:

```
$ cat certificate.pem
```

Die Ausgabe sollte eine lange, PEM-codierte Zeichenfolge ohne Zeilenumbrüche sein, eingeleitet durch `-----BEGIN CERTIFICATE-----` und gefolgt von `-----END CERTIFICATE-----`.

Das X.509-Zertifikat in den RDAP-Eintrag in Ihrem RIR hochladen

Fügen Sie das zuvor erstellte Zertifikat zum RDAP-Datensatz für Ihr RIR hinzu. Achten Sie darauf, dass die `-----BEGIN CERTIFICATE-----` und `-----END CERTIFICATE-----`-Zeichenfolgen

vor und nach dem kodierten Teil enthalten sind. Der gesamte Inhalt muss sich in einer einzigen, langen Zeile befinden. Das Verfahren zum Aktualisieren des RDAP hängt von Ihrem RIR ab:

- Verwenden Sie für ARIN das Accountmanager-Portal, um das Zertifikat im Abschnitt „Öffentliche Kommentare“ für das Objekt „Netzwerkinformationen“ hinzuzufügen, das Ihren Adressbereich darstellt. Fügen Sie es nicht dem Kommentarbereich Ihrer Organisation hinzu.
- Für RIPE fügen Sie das Zertifikat als neues „descr“-Feld zum Objekt „inetnum“ oder „inet6num“ hinzu, das Ihren Adressbereich darstellt. Diese finden Sie normalerweise im Bereich „Meine Ressourcen“ des RIPE-Datenbankportals. Fügen Sie es nicht dem Kommentarbereich für Ihre Organisation oder dem Feld „Anmerkungen“ der oben genannten Objekte hinzu.
- Fügen Sie für APNIC das Zertifikat hinzu, indem Sie die Anmerkungen zum Datensatz „inetnum“ oder „inet6num“ bearbeiten.

Sie können das Zertifikat aus dem Verzeichnis Ihres RIRs entfernen, nachdem die nachfolgende Bereitstellungsphase abgeschlossen ist.

Erstellen eines ROA-Objekts in Ihrem RIR

Erstellen Sie ein ROA-Objekt, um Amazon ASNs 16509 und 14618 zu autorisieren, Ihren Adressbereich zu bewerben, sowie diejenigen, die derzeit autorisiert sind ASNs , für diesen Adressbereich zu werben. Autorisieren Sie für den AWS GovCloud (US) Regions ASN 8987 anstelle von 16509 und 14618. Sie müssen die maximale Länge auf die Größe des CIDR festlegen, das Sie einbinden möchten. Das IPv4 spezifischste Präfix, das Sie verwenden können, ist /24. Der spezifischste IPv6 Adressbereich, den Sie angeben können, ist /48 für solche CIDRs , die öffentlich beworben werden können, und /60 für solche CIDRs , die nicht öffentlich beworben werden können.

> **Important**
>
> Wenn Sie ein ROA-Objekt für Amazon VPC IP Address Manager (IPAM) erstellen, müssen IPv4 CIDRs Sie bei der Erstellung des ROAs, für die maximale Länge eines IP-Adresspräfixes auf festlegen. `/24` Denn IPv6 CIDRs wenn Sie sie zu einem Pool mit Werbung hinzufügen, muss die maximale Länge eines IP-Adresspräfixes sein. `/48` Dies stellt sicher, dass Sie bei der Aufteilung Ihrer öffentlichen IP-Adresse auf verschiedene AWS Regionen die volle Flexibilität haben. IPAM erzwingt die von Ihnen festgelegte maximale Länge. Weitere Informationen zu BYOIP-Adressen für IPAM finden Sie unter Tutorial: BYOIP-Adresse CIDRs zu IPAM im Amazon VPC IPAM-Benutzerhandbuch.

Es kann bis zu 24 Stunden dauern, bis das ROA für Amazon verfügbar ist. Weitere Informationen erhalten Sie von Ihrem RIR:

- ARIN: — ROA-Anforderungen
- RIPE — Verwaltung ROAs
- APNIC — Routenmanagement

Wenn Sie Werbung von einem lokalen Workload auf einen Workload migrieren AWS, müssen Sie zunächst einen ROA für Ihre bestehende ASN erstellen, bevor Sie den ROAs für Amazon erstellen. ASNs Andernfalls könnte der Vorgang Auswirkungen auf Ihr vorhandenes Routing und Ihre Anzeigen haben.

Important

Damit Amazon Ihren IP-Adressbereich bewerben und weiterhin bewerben kann, ASNs müssen Sie ROAs bei Amazon die oben genannten Richtlinien einhalten. Wenn Sie ungültig ROAs sind oder die oben genannten Richtlinien nicht einhalten, behält sich Amazon das Recht vor, die Werbung für Ihren IP-Adressbereich einzustellen.

Note

Dieser Schritt ist für Adressräume, die nicht öffentlich beworben werden können IPv6 , nicht erforderlich.

Integrieren Sie Ihren Adressbereich zur Verwendung in Amazon EC2

Der Integrationsprozess für BYOIP umfasst, abhängig von Ihren Anforderungen, die folgenden Aufgaben.

Aufgaben

- Stellen Sie einen öffentlich beworbenen Adressbereich bereit in AWS
- Stellen Sie einen IPv6 Adressbereich bereit, der nicht öffentlich beworben werden kann
- Kündigen Sie den Adressbereich über AWS
- Aufheben der Bereitstellung des Adressbereichs

- Validieren Ihres BYOIP

Stellen Sie einen öffentlich beworbenen Adressbereich bereit in AWS

Wenn Sie einen Adressbereich zur Verwendung mit angeben, bestätigen Sie AWS, dass Sie die Kontrolle über den Adressbereich haben, und autorisieren Amazon, für ihn zu werben. Wir bestätigen ebenso mit einer signierten Autorisierungsnachricht, dass Sie den Adressbereich kontrollieren. Diese Nachricht ist mit dem selbstsignierten X.509-Schlüsselpaar signiert, das Sie bei der Aktualisierung des RDAP-Eintrags mit dem X.509-Zertifikat verwendet haben. AWS erfordert eine kryptografisch signierte Autorisierungsnachricht, die dem RIR vorgelegt wird. Das RIR authentifiziert die Signatur mit dem Zertifikat, das Sie zum RDAP hinzugefügt haben, und vergleicht die Autorisierungsdetails mit dem ROA.

Aufheben der Bereitstellung des Adressbereichs

1. Verfassen einer Nachricht

   Verfassen Sie die Nur-Text-Autorisierungsnachricht. Das Format der Nachricht ist wie folgt, wobei das Datum das Ablaufdatum der Nachricht ist:

   ```
   1|aws|account|cidr|YYYYMMDD|SHA256|RSAPSS
   ```

   Ersetzen Sie die Kontonummer, den Adressbereich und das Ablaufdatum mit Ihren eigenen Werten, um eine Nachricht zu erstellen, die der folgenden ähnelt:

   ```
   text_message="1|aws|0123456789AB|198.51.100.0/24|20211231|SHA256|RSAPSS"
   ```

   Dies ist nicht mit einer ROA-Nachricht zu verwechseln, die ähnlich aussieht.

2. Nachrichten signieren

   Signieren Sie die Nur-Text-Nachricht mit dem privaten Schlüssel, den Sie zuvor erstellt haben. Die vom Befehl zurückgegebene Signatur ist eine lange Zeichenfolge, die Sie für den nächsten Schritt nutzen müssen.

> **Important**
>
> Es wird empfohlen, diesen Befehl zu kopieren und einzufügen. Ändern oder ersetzen Sie mit Ausnahme des Nachrichteninhalts keine Werte.

```
signed_message=$( echo -n $text_message | openssl dgst -sha256 -sigopt
 rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private-key.pem -keyform PEM
 | openssl base64 | tr -- '+=/' '-_~' | tr -d "\n")
```

3. Adresse zur Verfügung stellen

   Verwenden Sie den AWS CLI provision-byoip-cidrBefehl, um den Adressbereich bereitzustellen. Die Option `--cidr-authorization-context` verwendet die Nachrichten- und Signaturzeichenfolgen, die Sie zuvor erstellt haben.

   > **Important**
   >
   > Sie müssen die AWS Region angeben, in der der BYOIP-Bereich bereitgestellt werden soll, falls er sich von Ihrem Configure the unterscheidet. AWS CLI `Default region name`

   ```
   aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
    Message="$text_message",Signature="$signed_message" --region us-east-1
   ```

   Die Bereitstellung eines Adressbereichs ist eine asynchrone Operation. Daher gibt der Aufruf sofort Daten zurück, der Adressbereich ist jedoch erst zur Verwendung bereit, wenn der Status von `pending-provision` zu `provisioned` wechselt.

4. Überwachen des Fortschritts

   Während die Bereitstellung in den meisten Fällen innerhalb von zwei Stunden abgeschlossen sein wird, kann es bis zu einer Woche dauern, bis der Bereitstellungsprozess für öffentlich beworbene Bereiche abgeschlossen ist. Verwenden Sie den describe-byoip-cidrsBefehl, um den Fortschritt zu überwachen, wie in diesem Beispiel:

```
aws ec2 describe-byoip-cidrs --max-results 5 --region us-east-1
```

Wenn während der Bereitstellung Probleme auftreten und der Status in `failed-provision` wechselt, müssen Sie den `provision-byoip-cidr`-Befehl erneut ausführen, nachdem die Probleme behoben wurden.

Stellen Sie einen IPv6 Adressbereich bereit, der nicht öffentlich beworben werden kann

Standardmäßig wird ein Adressbereich bereitgestellt, der öffentlich im Internet beworben wird. Sie können einen IPv6 Adressbereich bereitstellen, der nicht öffentlich beworben werden kann. Bei Routen ohne öffentliches Advertising ist der Bereitstellungsprozess in der Regel innerhalb von Minuten abgeschlossen. Wenn Sie einer VPC einen IPv6 CIDR-Block aus einem nicht öffentlichen Adressbereich zuordnen, kann auf den IPv6 CIDR nur über hybride Konnektivitätsoptionen zugegriffen werden IPv6, die AWS Site-to-Site VPN oder Amazon VPC Direct ConnectTransit Gateways unterstützen.

Eine ROA ist nicht erforderlich, um einen nicht-öffentlichen Adressbereich bereitzustellen.

> **Important**
>
> - Sie können nur während der Bereitstellung angeben, ob ein Adressbereich öffentlich beworben werden kann. Sie können den Anzeigenstatus nachträglich nicht mehr ändern.
> - Amazon VPC unterstützt keine eindeutige lokale Adresse (ULA) CIDRs. Alle VPCs müssen einzigartig IPv6 CIDRs sein. Zwei VPCs können nicht den gleichen IPv6 CIDR-Bereich haben.

Verwenden Sie den folgenden Befehl, um einen IPv6 Adressbereich bereitzustellen, der nicht öffentlich beworben werden kann. provision-byoip-cidr

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
 Message="$text_message",Signature="$signed_message" --no-publicly-advertisable --
region us-east-1
```

Kündigen Sie den Adressbereich über AWS

Nachdem der Adressbereich bereitgestellt wurde, kann er veröffentlicht werden. Sie müssen den genauen Adressbereich ankündigen, den Sie bereitgestellt haben. Sie können nur einen Teil des bereitgestellten Adressbereichs ankündigen.

Wenn Sie einen IPv6 Adressbereich bereitgestellt haben, der nicht öffentlich bekannt gegeben wird, müssen Sie diesen Schritt nicht abschließen.

Wir empfehlen, dass Sie den Adressbereich oder einen Teil des Adressbereichs nicht mehr an anderen Standorten bewerben, bevor Sie ihn über diese Website bewerben. AWS Wenn Sie den IP-Adressbereich weiterhin von anderen Orten aus bewerben, können wir ihn nicht zuverlässig unterstützen oder Probleme beheben. Insbesondere können wir nicht garantieren, dass der Datenverkehr für den Adressbereich oder einen Teil des Bereichs in unser Netz gelangt.

Um Ausfallzeiten zu minimieren, können Sie Ihre AWS Ressourcen so konfigurieren, dass sie eine Adresse aus Ihrem Adresspool verwenden, bevor sie veröffentlicht wird, und dann gleichzeitig die Werbung für die Adresse vom aktuellen Standort aus beenden und mit der Werbung beginnen. AWS Weitere Informationen zur Zuweisung einer Elastic IP-Adresse aus Ihrem Adresspool finden Sie unter Zuweisen einer Elastic-IP-Adresse.

Einschränkungen

- Sie können den Befehl advertise-byoip-cidr höchstens alle 10 Sekunden ausführen, auch wenn Sie jedes Mal einen anderen Adressbereich angeben.
- Sie können den Befehl withdraw-byoip-cidr höchstens alle 10 Sekunden ausführen, auch wenn Sie jedes Mal einen anderen Adressbereich angeben.

Verwenden Sie den folgenden advertise-byoip-cidrBefehl, um den Adressbereich bekannt zu geben.

```
aws ec2 advertise-byoip-cidr --cidr address-range --region us-east-1
```

Verwenden Sie den folgenden withdraw-byoip-cidrBefehl, um die Werbung für den Adressbereich zu beenden.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Aufheben der Bereitstellung des Adressbereichs

Um die Verwendung Ihres Adressbereichs mit zu beenden AWS, geben Sie zunächst alle Elastic IP-Adressen frei und trennen Sie die Zuordnung aller IPv6 CIDR-Blöcke, die noch dem Adresspool zugewiesen sind. Beenden Sie dann die Veröffentlichung des Adressbereichs und heben Sie schließlich die Bereitstellung des Adressbereichs auf.

Sie können die Bereitstellung eines Teils des Adressbereichs nicht aufheben. Wenn Sie einen spezifischeren Adressbereich mit verwenden möchten AWS, heben Sie die Bereitstellung des gesamten Adressbereichs auf und stellen Sie einen spezifischeren Adressbereich bereit.

(IPv4) Verwenden Sie den folgenden Befehl release-address, um jede Elastic IP-Adresse freizugeben.

```
aws ec2 release-address --allocation-id eipalloc-12345678abcabcabc --region us-east-1
```

(IPv6) Verwenden Sie den folgenden Befehl, um die Zuordnung eines IPv6 CIDR-Blocks aufzuheben. disassociate-vpc-cidr-block

```
aws ec2 disassociate-vpc-cidr-block --association-id vpc-cidr-assoc-12345abcd1234abc1
 --region us-east-1
```

Verwenden Sie den folgenden withdraw-byoip-cidrBefehl, um die Werbung für den Adressbereich zu beenden.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Verwenden Sie den folgenden deprovision-byoip-cidrBefehl, um die Bereitstellung des Adressbereichs aufzuheben.

```
aws ec2 deprovision-byoip-cidr --cidr address-range --region us-east-1
```

Es kann bis zu einem Tag dauern, bis die Bereitstellung eines Adressbereichs aufgehoben wird.

Validieren Ihres BYOIP

1. Validieren des selbstsignierten x.509-Schlüsselpaars

   Validieren Sie, ob das Zertifikat hochgeladen wurde, und seine Gültigkeit mit dem Befehl whois.

Verwenden Sie für ARIN `whois -h whois.arin.net r + 2001:0DB8:6172::/48`, um den RDAP-Datensatz für Ihren Adressbereich nachzuschlagen. Überprüfen Sie den `Public Comments`-Abschnitt für `NetRange` (Netzwerkbereich) in der Befehlsausgabe. Das Zertifikat sollte im `Public Comments`-Abschnitt für den Adressbereich hinzugefügt werden.

Sie können `Public Comments` mit dem Zertifikat als Inhalt mit dem folgenden Befehl prüfen:

```
whois -h whois.arin.net r + 2001:0DB8:6172::/48 | grep Comments | grep BEGIN
```

Dadurch wird eine Ausgabe mit dem Inhalt des Schlüssels zurückgegeben, der etwa wie folgt aussehen sollte:

```
Public Comments:
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

Verwenden Sie für RIPE `whois -r -h whois.ripe.net 2001:0DB8:7269::/48`, um den RDAP-Datensatz für Ihren Adressbereich nachzuschlagen. Überprüfen Sie den `descr`-Abschnitt

für das `inetnum`-Objekt (Netzwerkbereich) in der Befehlsausgabe. Das Zertifikat sollte als neues `descr`-Feld für den Adressbereich hinzugefügt werden.

Sie können `descr` mit dem Zertifikat als Inhalt mit dem folgenden Befehl prüfen:

```
whois -r -h whois.ripe.net 2001:0DB8:7269::/48 | grep descr | grep BEGIN
```

Dadurch wird eine Ausgabe mit dem Inhalt des Schlüssels zurückgegeben, der etwa wie folgt aussehen sollte:

```
descr:
-----BEGIN CERTIFICATE-----MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8
RDAHSP+I1TowDQYJKoZIhvcNAQELBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAg
MCEF1Y2tsYW5kMREwDwYDVQQHDAhBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIF
dlYiBTZXJ2aWNlczETMBEGA1UECwwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPS
VAgRGVtbzAeFw0yMTEyMDcyMDI0NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNV
BAYTAk5aMREwDwYDVQQIDAhBdWNrbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDA
aBgNVBAoME0FtYXpvbiBXZWIgU2VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW
8xEzARBgNVBAMMCkJZT0lQIERlbW8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwg
gEKAoIBAQCfmacvDp0wZ0ceiXXcR/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanA
EskgAseyFypwEEQr4CJijI/5hp9prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3
stsI5QesHVRwOaXUdprAnndaTugmDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq
35wU/x+wXlAqBXg4MZK2KoUu27kYt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp
1ZnVIc7NqnhdeIW48QaYjhMlUEfxdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2r
GlHWkJsbhr0VEUyAGu1bwkgcdww3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBS
tFyujN6SYBr2glHpGt0XGF7GbGTAfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0
XGF7GbGTAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6Y
Lhz521lfyVfxY0t6o3410bQAeAF08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyL
xngwMYN0XY5tVhDQqk4/gmDNEKSZy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9
wySL507XQz76Uk5cFypBOzbnk35UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8
mBGqVpPpey+dXpzzzv1iBKN/VY4ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGC
vRDl/qdO/GIDJi77dmZWkh/ic90MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoN
PyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

Verwenden Sie für APNIC `whois -h whois.apnic.net 2001:0DB8:6170::/48`, um den RDAP-Datensatz für Ihren BYOIP-Adressbereich nachzuschlagen. Überprüfen Sie den `remarks`-Abschnitt für das `inetnum`-Objekt (Netzwerkbereich) in der Befehlsausgabe. Das Zertifikat sollte als neues `remarks`-Feld für den Adressbereich hinzugefügt werden.

Sie können `remarks` mit dem Zertifikat als Inhalt mit dem folgenden Befehl prüfen:

```
whois -h whois.apnic.net 2001:0DB8:6170::/48 | grep remarks | grep BEGIN
```

Dadurch wird eine Ausgabe mit dem Inhalt des Schlüssels zurückgegeben, der etwa wie folgt aussehen sollte:

```
remarks:
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

2. Überprüfung der Erstellung eines ROA-Objekts

   Überprüfen Sie die erfolgreiche Erstellung der ROA-Objekte mithilfe der RIPEstat Daten-API. Stellen Sie sicher, dass Sie Ihren Adressbereich mit den Werten ASNs 16509 und 14618 von Amazon sowie mit denen vergleichen, ASNs die derzeit autorisiert sind, für diesen Adressbereich zu werben.

   Sie können die ROA-Objekte von verschiedenen Amazon ASNs mit Ihrem Adressbereich überprüfen, indem Sie den folgenden Befehl verwenden:

```
curl --location --request GET "https://stat.ripe.net/data/rpki-validation/data.json?
resource=ASN&prefix=CIDR
```

In dieser Beispielausgabe hat die Antwort ein Ergebnis von `"status": "valid"` für die Amazon ASN 16509. Dies gibt an, dass das ROA-Objekt für den Adressbereich erfolgreich erstellt wurde:


```
{
    "messages": [],
    "see_also": [],
    "version": "0.3",
    "data_call_name": "rpki-validation",
    "data_call_status": "supported",
    "cached": false,
    "data": {
        "validating_roas": [
            {
                "origin": "16509",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "valid"
            },
            {
                "origin": "14618",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "invalid_asn"
            },
            {
                "origin": "64496",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "invalid_asn"
            }
        ],
        "status": "valid",
        "validator": "routinator",
        "resource": "16509",
        "prefix": "2001:0DB8::/32"
    },
    "query_id": "20230224152430-81e6384e-21ba-4a86-852a-31850787105f",
    "process_time": 58,
    "server_id": "app116",
```

```
    "build_version": "live.2023.2.1.142",
    "status": "ok",
    "status_code": 200,
    "time": "2023-02-24T15:24:30.773654"
}
```

Der Status “unknown” gibt an, dass das ROA-Objekt für den Adressbereich nicht erstellt wurde. Der Status “invalid_asn” gibt an, dass das ROA-Objekt für den Adressbereich nicht erfolgreich erstellt wurde.

Verwenden Sie Ihren BYOIP-Adressbereich in Amazon EC2

Sie können die IPv6 Adressbereiche, die Sie in Ihrem Konto bereitgestellt haben, einsehen IPv4 und verwenden. Weitere Informationen finden Sie unter the section called “Integrieren Ihres Adressbereichs”.

IPv4 Adressbereiche

Sie können eine Elastic IP-Adresse aus Ihrem IPv4 Adresspool erstellen und sie mit Ihren AWS Ressourcen wie EC2 Instances, NAT-Gateways und Network Load Balancers verwenden.

Verwenden Sie den folgenden describe-public-ipv 4-pools-Befehl, um Informationen zu den IPv4 Adresspools anzuzeigen, die Sie in Ihrem Konto bereitgestellt haben.

```
aws ec2 describe-public-ipv4-pools --region us-east-1
```

Verwenden Sie den Befehl allocate-address, um eine Elastic IP-Adresse aus Ihrem IPv4 Adresspool zu erstellen. Mit der Option `--public-ipv4-pool` können Sie die ID des von `describe-byoip-cidrs` zurückgegebenen Adressbereichs angeben. Oder Sie können die Option `--address` verwenden, um eine Adresse aus dem von Ihnen bereitgestellten Adressbereich anzugeben.

IPv6 Adressbereiche

Verwenden Sie den folgenden Befehl IPv6 describe-ipv6-pools, um Informationen zu den Adresspools anzuzeigen, die Sie in Ihrem Konto bereitgestellt haben.

```
aws ec2 describe-ipv6-pools --region us-east-1
```

Verwenden Sie den folgenden Befehl create-vpc, um eine VPC zu erstellen und eine IPv6 CIDR aus Ihrem IPv6 Adresspool anzugeben. Lassen Sie die Option weg, damit Amazon den IPv6 CIDR aus Ihrem IPv6 Adresspool auswählen kann. `--ipv6-cidr-block`

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --ipv6-cidr-block ipv6-cidr --ipv6-
pool pool-id --region us-east-1
```

Verwenden Sie den folgenden associate-vpc-cidr-blockBefehl, um einen IPv6 CIDR-Block aus Ihrem IPv6 Adresspool einer VPC zuzuordnen. Lassen Sie die Option weg, damit Amazon den IPv6 CIDR aus Ihrem IPv6 Adresspool auswählen kann. `--ipv6-cidr-block`

```
aws ec2 associate-vpc-cidr-block --vpc-id vpc-123456789abc123ab --ipv6-cidr-block ipv6-
cidr --ipv6-pool pool-id --region us-east-1
```

Verwenden Sie den Befehl describe-vpcs, um Ihre VPCs und die zugehörigen IPv6 Adresspool-Informationen anzuzeigen. Verwenden Sie den folgenden Befehl IPv6 6-pool-cidrs, um Informationen zu zugehörigen CIDR-Blöcken aus einem bestimmten IPv6 Adresspool anzuzeigen. get-associated-ipv

```
aws ec2 get-associated-ipv6-pool-cidrs --pool-id pool-id --region us-east-1
```

Wenn Sie den IPv6 CIDR-Block von Ihrer VPC trennen, wird er wieder in Ihren IPv6 Adresspool freigegeben.

Elastic-IP-Adressen

Eine Elastic IP-Adresse ist eine statische IPv4 Adresse, die für dynamisches Cloud Computing konzipiert wurde. Ihrem AWS Konto wird eine Elastic IP-Adresse zugewiesen und gehört Ihnen, bis Sie sie freigeben. Durch Verwenden einer Elastic IP-Adresse können Sie Ausfälle bei Instances oder Software maskieren. Weisen Sie dazu die Adresse einer anderen Instance in Ihrem Konto neu zu. Alternativ können Sie die Elastic IP-Adresse in einem DNS-Eintrag für Ihre Domain angeben, damit Ihre Domain auf Ihre Instance verweist. Weitere Informationen finden Sie in der Dokumentation zu Ihrem Domain-Registrar.

Eine Elastic IP-Adresse ist eine öffentliche IPv4 Adresse, die über das Internet erreichbar ist. Wenn Sie eine Verbindung zu einer Instance herstellen müssen, die keine öffentliche IPv4 Adresse hat, können Sie Ihrer Instance eine Elastic IP-Adresse zuordnen, um die Kommunikation mit dem Internet zu ermöglichen.

Inhalt

- Grundlagen zu Elastic IP-Preisen
- Grundlagen zu Elastic IP-Adressen
- Kontingent für Elastic-IP-Adressen
- Zuordnen einer Elastic-IP-Adresse zu einer Instance
- Übertragen Sie eine Elastic IP-Adresse zwischen AWS-Konten
- Freigeben einer Elastic-IP-Adresse
- Erstellen Sie einen Reverse-DNS-Eintrag für E-Mails bei Amazon EC2

Grundlagen zu Elastic IP-Preisen

Für alle Elastic IP-Adressen fallen Gebühren an, unabhängig davon, ob sie verwendet (einer Ressource wie einer EC2 Instance zugewiesen) oder inaktiv sind (in Ihrem Konto erstellt, aber nicht zugewiesen).

AWS Gebühren für alle öffentlichen IPv4 Adressen, einschließlich öffentlicher IPv4 Adressen, die mit laufenden Instances verknüpft sind, und Elastic IP-Adressen. Weitere Informationen finden Sie auf der Amazon VPC-Preisseite auf der Registerkarte Öffentliche IPv4 Adresse.

Grundlagen zu Elastic IP-Adressen

Im Folgenden finden Sie eine Auflistung der grundlegenden Merkmale einer Elastic IP-Adresse:

- Eine Elastic IP-Adresse ist statisch; sie ändert sich im Laufe der Zeit nicht.
- Eine Elastic IP-Adresse ist nur für die Verwendung in einer bestimmten Region bestimmt und kann nicht in eine andere Region verschoben werden.
- Eine Elastic IP-Adresse stammt aus dem Adresspool von IPv4 Amazon oder aus einem benutzerdefinierten IPv4 Adresspool, den Sie in Ihren AWS-Konto eigenen Adresspool aufgenommen haben. Wir unterstützen keine Elastic IP-Adressen für IPv6.
- Um eine Elastic IP-Adresse zu verwenden, verknüpfen Sie sie zuerst mit Ihrem Konto und anschließend mit Ihrer Instance oder Netzwerkschnittstelle.
- Wenn Sie einer Instance eine Elastic IP-Adresse zuordnen, wird sie auch der primären Netzwerkschnittstelle der Instance zugeordnet. Wenn Sie eine Elastic IP-Adresse einer Netzwerkschnittstelle zuordnen, die einer Instance zugewiesen ist, wird sie auch der Instance zugeordnet.

- Wenn Sie einer Instance oder ihrer primären Netzwerkschnittstelle eine Elastic IP-Adresse zuordnen und der Instance bereits eine öffentliche IPv4 Adresse zugeordnet ist, wird diese öffentliche IPv4 Adresse wieder in den Pool der öffentlichen IPv4 Adressen von Amazon freigegeben und die Elastic IP-Adresse wird stattdessen der Instance zugeordnet. Sie können die öffentliche IPv4 Adresse, die zuvor mit der Instance verknüpft war, nicht wiederverwenden und Sie können diese öffentliche IPv4 Adresse nicht in eine Elastic IP-Adresse konvertieren. Weitere Informationen finden Sie unter Öffentliche IPv4-Adressen.
- Sie können die Zuordnung einer Elastic IP-Adresse zu einer Ressource aufheben und die Adresse einer anderen Ressource erneut zuordnen. Um unerwartetes Verhalten zu vermeiden, stellen Sie sicher, dass alle aktiven Verbindungen zu der in der vorhandenen Zuordnung genannten Ressource geschlossen werden, bevor Sie die Änderung vornehmen. Nachdem Sie Ihre Elastic IP-Adresse einer anderen Ressource zugeordnet haben, können Sie Ihre Verbindungen mit der neu verknüpften Ressource erneut öffnen.
- Eine getrennte Elastic IP-Adresse bleibt mit Ihrem Konto verknüpft, bis Sie sie explizit freigeben. Ihnen werden alle Elastic IP-Adressen in Ihrem Konto in Rechnung gestellt, unabhängig davon, ob sie mit einer Instance verknüpft oder getrennt sind. Weitere Informationen finden Sie auf der Amazon VPC-Preisseite auf der Registerkarte Öffentliche IPv4 Adresse.
- Wenn Sie einer Instance, die zuvor eine öffentliche IPv4 Adresse hatte, eine Elastic IP-Adresse zuordnen, ändert sich der öffentliche DNS-Hostname der Instance entsprechend der Elastic IP-Adresse.
- Wir lösen einen öffentlichen DNS-Hostnamen in die öffentliche IPv4 Adresse oder die Elastic IP-Adresse der Instance außerhalb des Netzwerks der Instance und innerhalb des Netzwerks der Instance in die private IPv4 Adresse der Instance auf.
- Wenn Sie eine Elastic IP-Adresse aus einem IP-Adresspool zuweisen, den Sie Ihrem AWS Konto hinzugefügt haben, wird sie nicht auf Ihre Elastic IP-Adresslimits angerechnet. Weitere Informationen finden Sie unter Kontingent für Elastic-IP-Adressen.
- Wenn Sie die Elastic IP-Adressen zuweisen, können Sie die Elastic IP-Adressen einer Netzwerkgrenzgruppe zuordnen. Dies ist der Ort, von dem aus wir den CIDR-Block bewerben. Durch Festlegen der Netzwerkgrenzgruppe wird der CIDR-Block auf dieser Gruppe beschränkt. Wenn Sie die Netzwerkgrenzgruppe nicht angeben, legen wir die Grenzgruppe fest, die alle Availability Zones in der Region enthält (z. B. `us-west-2`).
- Eine elastische IP-Adresse ist nur zur Verwendung in einer spezifischen Netzwerkgrenzgruppe bestimmt.

Kontingent für Elastic-IP-Adressen

Standardmäßig AWS-Konten haben alle ein Kontingent von fünf (5) Elastic IP-Adressen pro Region, da öffentliche (IPv4) Internetadressen eine knappe öffentliche Ressource sind. Wir empfehlen Ihnen dringend, eine Elastic-IP-Adresse in erster Linie wegen der Möglichkeit zu verwenden, die Adresse im Fall eines Instance-Ausfalls einer anderen Instance zuzuweisen und für alle anderen Kommunikationen zwischen Knoten DNS-Hostnamen zu verwenden.

Wenn Ihre Architektur zusätzliche Elastic IP-Adressen erfordert, können Sie direkt in der Service-Quotas-Konsole eine Erhöhung des Kontingents anfordern. Zum Anfordern einer Erhöhung für ein Kontingent wählen Sie Erhöhung auf Kontoebene beantragen. Weitere Informationen finden Sie unter EC2 Amazon-Servicekontingente.

Zuordnen einer Elastic-IP-Adresse zu einer Instance

Nachdem Sie eine Elastic IP-Adresse zugewiesen haben, können Sie sie einer AWS Ressource zuordnen, z. B. einer EC2 Instance, einem NAT-Gateway oder einem Network Load Balancer. Um eine Elastic IP-Adresse später einer anderen AWS Ressource zuzuordnen, können Sie sie von ihrer aktuellen Ressource trennen und sie dann der neuen Ressource zuordnen.

Aufgaben

- Zuweisen einer Elastic-IP-Adresse
- So ordnen Sie eine Elastic-IP-Adresse zu
- Aufheben der Zuordnung einer Elastic IP-Adresse

Zuweisen einer Elastic-IP-Adresse

Sie weisen eine Elastic IP-Adresse zur Verwendung in einer Region zu. Für alle Elastic IP-Adressen fallen Gebühren an, unabhängig davon, ob sie verwendet werden (mit einer Ressource verknüpft, EC2 z. B. einer Instanz) oder inaktiv sind (in Ihrem Konto erstellt, aber nicht verknüpft).

Console

So weisen Sie eine Elastic IP-Adresse zu

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network & Security, Elastic aus IPs.
3. Wählen Sie Elastic-IP-Adresse zuweisen aus.

4. (Optional) Wenn Sie eine Elastic IP-Adresse (EIP) zuweisen, wählen Sie die Netzwerkgrenzgruppe aus, der die EIP zugewiesen werden soll. Eine Netzwerkgrenzgruppe ist eine Sammlung von Availability Zones (AZs), Local Zones oder Wavelength Zones, von denen aus AWS eine öffentliche IP-Adresse beworben wird. Local Zones und Wellenlängenzonen können andere Netzwerkgrenzgruppen als die AZs in einer Region haben, um eine minimale Latenz oder physische Entfernung zwischen dem AWS Netzwerk und den Kunden sicherzustellen, die auf die Ressourcen in diesen Zonen zugreifen.

   > **Important**
   >
   > Sie müssen eine EIP derselben Netzwerkgrenzgruppe zuordnen wie die AWS Ressource, die der EIP zugeordnet wird. Eine EIP in einer Netzwerkgrenzgruppe kann nur in Zonen dieser Netzwerkgrenzgruppe angekündigt werden und nicht in anderen Zonen, die durch andere Netzwerkgrenzgruppen repräsentiert werden.

   Wenn Sie Local Zones oder Wellenlängenzonen aktiviert haben (weitere Informationen finden Sie unter Aktivieren einer lokalen Zone oder Aktivieren von Wellenlängenzonen), können Sie eine Netzwerkgrenzgruppe für AZs, Local Zones oder Wellenlängenzonen auswählen. Wählen Sie die Netzwerkgrenzgruppe sorgfältig aus, da sich die EIP und die AWS Ressource, der sie zugeordnet ist, in derselben Netzwerkgrenzgruppe befinden müssen. Sie können die EC2 Konsole verwenden, um die Netzwerkgrenzgruppe anzuzeigen, in der sich Ihre Availability Zones, Local Zones oder Wavelength Zones befinden. In der Regel gehören alle Availability Zones in einer Region derselben Netzwerkgrenzgruppe an, wohingegen Local Zones oder Wavelength Zones zu ihren eigenen separaten Netzwerkgrenzgruppen gehören.

   Wenn Sie Local Zones oder Wavelength Zones nicht aktiviert haben, ist bei der Zuweisung einer EIP die Netzwerkgrenzgruppe, die alle AZs für die Region darstellt (z. B. `us-west-2`), für Sie vordefiniert und Sie können sie nicht ändern. Das bedeutet, dass die EIP, die Sie dieser Netzwerkgrenzgruppe zuweisen, in der gesamten Region, AZs in der Sie sich befinden, beworben wird.

5. Wählen Sie für den öffentlichen IPv4 Adresspool eine der folgenden Optionen aus:

   - IPv4 Adresspool von Amazon — Wenn Sie möchten, dass eine IPv4 Adresse aus dem IPv4 Adresspool von Amazon zugewiesen wird.
   - Öffentliche IPv4 Adresse, die Sie Ihrem AWS Konto hinzufügen — Wenn Sie eine nicht zusammenhängende (nicht sequentielle) öffentliche IPv4 Adresse aus einem IP-Adresspool

zuweisen möchten, den Sie Ihrem Konto hinzugefügt haben. AWS Diese Option ist deaktiviert, wenn Sie keine IP-Adresspools haben. Weitere Informationen darüber, wie Sie Ihrem Konto Ihren eigenen IP-Adressbereich hinzufügen können, finden Sie unter. AWS Bringen Sie Ihre eigenen IP-Adressen (BYOIP) zu Amazon EC2

- Kundeneigener IPv4 Adresspool — Wenn Sie eine IPv4 Adresse aus einem Pool, der in Ihrem lokalen Netzwerk erstellt wurde, für die Verwendung mit einem Outpost zuweisen möchten. AWS Diese Option ist deaktiviert, wenn Sie keinen AWS -Außenposten haben.
- Zuweisung mithilfe eines IPv4 IPAM-Pool: Wenn Sie sequentielle Elastic IP-Adressen aus einem zusammenhängenden öffentlichen Block in einem IPAM-Pool zuweisen möchten. IPv4 Durch die Zuweisung sequenzieller Elastic-IP-Adressen kann der Verwaltungsaufwand für Sicherheitszugriffskontrolllisten erheblich reduziert und die Zuweisung und Nachverfolgung von IP-Adressen für Unternehmen mit einer Skalierung von AWS vereinfacht werden. Weitere Informationen finden Sie unter Zuweisen sequenzieller Elastic IP-Adressen aus einem IPAM-Pool im Amazon VPC IPAM-Benutzerhandbuch.

6. (Optional) Um einen Tag hinzuzufügen, wählen Sie Neuen Tag hinzufügen und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.

AWS CLI

So weisen Sie eine Elastic IP-Adresse zu

Verwenden Sie den AWS CLI -Befehl allocate-address .

Im folgenden Beispiel EC2 wählt Amazon eine Adresse aus dem Adresspool von Amazon aus.

```
aws ec2 allocate-address
```

Im folgenden Beispiel EC2 wählt Amazon eine Adresse aus dem angegebenen Pool aus, zu der Sie AWS mithilfe von BYOIP weitergeleitet haben.

```
aws ec2 allocate-address \
    --public-ipv4-pool ipv4pool-ec2-012345abcdef67890
```

Im folgenden Beispiel wird eine Adresse aus dem angegebenen IPv4 IPAM-Pool angegeben.

```
aws ec2 allocate-address \
    --ipam-pool-id ipam-pool-1234567890abcdef0 \
    --address 192.0.2.0
```

PowerShell

So weisen Sie eine Elastic IP-Adresse zu

Verwenden Sie das cmdlet New-EC2Address.

Im folgenden Beispiel EC2 wählt Amazon eine Adresse aus dem Adresspool von Amazon aus.

```
New-EC2Address
```

Im folgenden Beispiel EC2 wählt Amazon eine Adresse aus dem angegebenen Pool aus, zu der Sie AWS mithilfe von BYOIP weitergeleitet haben.

```
New-EC2Address \
    --PublicIpv4Pool ipv4pool-ec2-012345abcdef67890
```

Im folgenden Beispiel wird eine Adresse aus dem angegebenen IPv4 IPAM-Pool angegeben.

```
New-EC2Address \
    --IpamPoolId ipam-pool-1234567890abcdef0 \
    --Address 192.0.2.0
```

So ordnen Sie eine Elastic-IP-Adresse zu

Wenn Sie Ihrer Instance eine Elastic IP-Adresse zuordnen, um die Kommunikation mit dem Internet zu ermöglichen, müssen Sie sicherstellen, dass sich Ihre Instance in einem öffentlichen Subnetz befindet. Weitere Informationen finden Sie unter Internetzugriff über ein Internet-Gateway aktivieren im Amazon-VPC-Benutzerhandbuch.

Console

Zuordnen einer Elastic IP-Adresse zu einer Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic aus IPs.
3. Wählen Sie die zu verknüpfende Elastic IP-Adresse aus, und wählen Sie Actions (Aktionen), Associate Elastic IP address (Elastic IP-Adresse zuordnen).
4. Wählen Sie für Resource type (Ressourcentyp) die Option Instance aus.

5. Wählen Sie die Instance aus, der die Elastic IP-Adresse zugeordnet werden soll. Sie können auch Text eingeben, um nach einer bestimmten Instance zu suchen.
6. (Optional) Geben Sie für Private IP address (Private IP-Adresse) eine private IP-Adresse an, mit der die Elastic IP-Adresse verknüpft werden soll.
7. Wählen Sie Associate aus.

So ordnen Sie einer Elastic IP-Adresse eine Netzwerkschnittstelle zu:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic aus IPs.
3. Wählen Sie die zu verknüpfende Elastic IP-Adresse aus, und wählen Sie Actions (Aktionen), Associate Elastic IP address (Elastic IP-Adresse zuordnen).
4. Wählen Sie für Resource type (Ressourcentyp) Network interface (Netzwerkschnittstelle) aus.
5. Wählen Sie für Network interface (Netzwerkschnittstelle) die Netzwerkschnittstelle aus, der die Elastic IP-Adresse zugeordnet werden soll. Sie können auch Text eingeben, um nach einer bestimmten Netzwerkschnittstelle zu suchen.
6. (Optional) Geben Sie für Private IP address (Private IP-Adresse) eine private IP-Adresse an, mit der die Elastic IP-Adresse verknüpft werden soll.
7. Wählen Sie Associate aus.

AWS CLI

So ordnen Sie eine Elastic IP-Adresse zu:

Verwenden Sie den Befehl associate-address AWS CLI .

```
aws ec2 associate-address \
    --instance-id i-0b263919b6498b123 \
    --allocation-id eipalloc-64d5890a
```

PowerShell

So ordnen Sie eine Elastic IP-Adresse zu:

Verwenden Sie das cmdlet Register-EC2Address.

```
Register-EC2Address `
    -InstanceId i-0b263919b6498b123 `
```

```
    -AllocationId eipalloc-64d5890a
```

Aufheben der Zuordnung einer Elastic IP-Adresse

Sie können die Zuordnung einer Elastic IP-Adresse jederzeit von einer Instance oder einer Netzwerkschnittstelle trennen. Nachdem Sie die Elastic-IP-Adresse getrennt haben, können Sie sie einer anderen Ressource zuordnen.

Console

So heben Sie die Zuordnung einer Elastic IP-Adresse auf und ordnen sie wieder zu:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic aus IPs.
3. Wählen Sie die Elastic IP-Adresse, deren Zuordnung Sie aufheben möchten, und wählen Sie Actions (Aktionen), Disassociate Elastic IP address (Elastic IP-Adresse trennen).
4. Wählen Sie Disassociate (Zuordnung aufheben) aus.

AWS CLI

So heben Sie die Zuordnung einer Elastic-IP-Adresse auf

Verwenden Sie den Befehl disassociate-address AWS CLI .

```
aws ec2 disassociate-address --association-id eipassoc-12345678
```

PowerShell

So heben Sie die Zuordnung einer Elastic-IP-Adresse auf

Verwenden Sie das cmdlet Unregister-EC2Address.

```
Unregister-EC2Address -AssociationId eipassoc-12345678
```

Übertragen Sie eine Elastic IP-Adresse zwischen AWS-Konten

Sie können eine Elastic IP-Adresse von einer AWS-Konto zur anderen übertragen. Dies kann in folgenden Situationen hilfreich sein:

- Notfallwiederherstellung – Schnelle Neuzuordnung der IP-Adressen für öffentlich zugängliche Internet-Workloads bei Notfällen.
- Organisatorische Umstrukturierung — Verschieben Sie einen Workload schnell von einem Workload AWS-Konto auf einen anderen. Bei einer Adressübertragung müssen Sie nicht warten, bis neue Elastic IP-Adressen von Ihren Sicherheitsgruppen und Ihrem Netzwerk zugelassen werden ACLs.
- Zentralisierte Sicherheitsadministration — Verwenden Sie ein zentrales AWS Sicherheitskonto, um Elastic IP-Adressen zu verfolgen und zu übertragen, die auf Einhaltung der Sicherheitsbestimmungen überprüft wurden.

Preisgestaltung

Für die Übertragung von Elastic-IP-Adressen fallen keine Gebühren an.

Aufgaben

- Übertragung für Elastic-IP-Adressen aktivieren
- Akzeptieren einer übertragenen Elastic-IP-Adresse
- Deaktivieren der Übertragung von Elastic-IP-Adressen

Übertragung für Elastic-IP-Adressen aktivieren

In diesem Abschnitt wird beschrieben, wie Sie eine übertragene Elastic-IP-Adresse akzeptieren. Beachten Sie die folgenden Einschränkungen in Bezug auf die Aktivierung von Elastic-IP-Adressen für die Übertragung:

- Sie können Elastic IP-Adressen von einem beliebigen AWS-Konto (Quellkonto) auf ein beliebiges anderes Konto AWS-Konto im selben Konto AWS-Region (Übertragungskonto) übertragen. Sie können keine Elastic-IP-Adressen in eine andere Region übertragen.
- Wenn Sie eine Elastic-IP-Adresse übertragen, findet ein zweistufiger Handshake zwischen den AWS-Konten statt. Wenn das Quellkonto die Übertragung startet, haben die Übertragungskonten sieben Tage Zeit, die Übertragung der Elastic-IP-Adresse zu akzeptieren. Während dieser sieben Tage kann das Quellkonto die ausstehende Übertragung einsehen (z. B. in der AWS Konsole oder mithilfe des describe-address-transfersBefehls). Nach sieben Tagen läuft die Übertragung ab und das Eigentum an der Elastic-IP-Adresse geht zurück an das Quellkonto.

- Akzeptierte Übertragungen sind für das Quellkonto (z. B. in der AWS Konsole oder mithilfe des describe-address-transfersBefehls) 14 Tage lang sichtbar, nachdem die Übertragungen akzeptiert wurden.
- AWS benachrichtigt Übertragungskonten nicht über ausstehende Elastic IP-Adressübertragungsanfragen. Der Besitzer des Quellkontos muss den Besitzer des Übertragungskontos darüber informieren, dass eine Elastic-IP-Adressübertragungsanforderung vorliegt, die er akzeptieren muss.
- Alle Tags, die einer übertragenen Elastic-IP-Adresse zugeordnet sind, werden zurückgesetzt, wenn die Übertragung abgeschlossen ist.
- Sie können Elastic IP-Adressen, die Ihnen aus öffentlichen IPv4 Adresspools zugewiesen wurden, nicht in Ihre eigenen AWS-Konto — allgemein als Bring Your Own IP (BYOIP) -Adresspools (Bring Your Own IP) bezeichnet — übertragen.
- Sie können keine Elastic IP-Adressen übertragen, die aus einem von Amazon bereitgestellten zusammenhängenden öffentlichen IPv4 Amazon VPC IP Address Manager (IPAM) -Pool zugewiesen wurden. Stattdessen können Sie mit IPAM IPAM-Pools für mehrere AWS Konten gemeinsam nutzen, indem Sie IPAM in AWS Organizations integrieren und verwenden. AWS RAM Weitere Informationen finden Sie unter Zuweisen sequenzieller Elastic IP-Adressen aus einem IPAM-Pool im Amazon VPC IPAM-Benutzerhandbuch.
- Wenn Sie versuchen, eine Elastic-IP-Adresse zu übertragen, der ein umgekehrter DNS-Eintrag zugeordnet ist, können Sie zwar mit der Übertragung beginnen, aber das Übertragungskonto kann die Übertragung erst dann akzeptieren, wenn der zugeordnete DNS-Eintrag entfernt wurde.
- Wenn Sie die Option aktiviert und konfiguriert haben AWS Outposts, haben Sie Elastic IP-Adressen möglicherweise aus einem kundeneigenen IP-Adresspool (CoIP) zugewiesen. Sie können keine Elastic-IP-Adressen übertragen, die von einem CoIP zugewiesen wurden. Sie können es jedoch verwenden, AWS RAM um eine CoIP mit einem anderen Konto zu teilen. Weitere Informationen finden Sie unter Kundeneigene IP-Adressen im AWS Outposts -Benutzerhandbuch.
- Sie können Amazon VPC IPAM verwenden, um die Übertragung von Elastic-IP-Adressen an Konten in einer Organisation von AWS Organizations zu verfolgen. Weitere Informationen finden Sie unter Anzeigen des IP-Adressverlaufs. Wenn eine Elastic IP-Adresse an ein Unternehmen AWS-Konto außerhalb der Organisation übertragen wird, geht der IPAM-Auditverlauf der Elastic IP-Adresse verloren.

Diese Schritte müssen vom Quellkonto ausgeführt werden.

Console

So aktivieren Sie die Übertragung von Elastic-IP-Adressen

1. Stellen Sie sicher, dass Sie das AWS Quellkonto verwenden.
2. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
3. Wählen Sie im Navigationsbereich Elastic aus IPs.
4. Wählen Sie eine oder mehrere Elastic-IP-Adressen aus, die für die Übertragung aktiviert werden sollen, und wählen Sie Actions (Aktionen), Enable transfer (Übertragung aktivieren).
5. Wenn Sie mehrere Elastic-IP-Adressen übertragen, wird Ihnen die Option Transfer type (Übertragungstyp) angezeigt. Wählen Sie eine der folgenden Optionen:
   - Wählen Sie Einzelkonto, wenn Sie die Elastic-IP-Adressen auf ein einzelnes AWS Konto übertragen möchten.
   - Wählen Sie Mehrere Konten, wenn Sie die Elastic IP-Adressen auf mehrere AWS Konten übertragen möchten.
6. Geben Sie unter Konto-ID übertragen IDs die AWS Konten ein, auf die Sie die Elastic IP-Adressen übertragen möchten.
7. Bestätigen Sie die Übertragung, indem Sie **`enable`** in das Textfeld eingeben.
8. Wählen Sie Absenden aus.
9. Informationen zum Akzeptieren der Übertragung finden Sie unter Akzeptieren einer übertragenen Elastic-IP-Adresse. Informationen zum Deaktivieren der Übertragung finden Sie unter Deaktivieren der Übertragung von Elastic-IP-Adressen.

AWS CLI

So aktivieren Sie die Übertragung von Elastic-IP-Adressen

Verwenden Sie den Befehl enable-address-transfer.

```
aws ec2 enable-address-transfer \
    --allocation-id eipalloc-09ad461b0d03f6aaf \
    --transfer-account-id 123456789012
```

PowerShell

So aktivieren Sie die Übertragung von Elastic-IP-Adressen

Verwenden Sie das cmdlet Enable-EC2AddressTransfer.

```
Enable-EC2AddressTransfer `
    -AllocationId eipalloc-09ad461b0d03f6aaf `
    -TransferAccountId 123456789012
```

Akzeptieren einer übertragenen Elastic-IP-Adresse

In diesem Abschnitt wird beschrieben, wie Sie eine übertragene Elastic-IP-Adresse akzeptieren.

Wenn Sie eine Elastic-IP-Adresse übertragen, findet ein zweistufiger Handshake zwischen den AWS-Konten statt. Wenn das Quellkonto die Übertragung startet, haben die Übertragungskonten sieben Tage Zeit, die Übertragung der Elastic-IP-Adresse zu akzeptieren. Während dieser sieben Tage kann das Quellkonto die ausstehende Übertragung einsehen (z. B. in der AWS Konsole oder mithilfe des describe-address-transfersBefehls). Nach sieben Tagen läuft die Übertragung ab und das Eigentum an der Elastic-IP-Adresse geht zurück an das Quellkonto.

Beachten Sie bei dem Akzeptieren von Übertragungen die folgenden Ausnahmen, die auftreten können, und wie Sie sie beheben können:

- AddressLimitExceeded: Wenn Ihr Übertragungskonto das Elastic IP-Adresskontingent überschritten hat, kann das Quellkonto die Elastic IP-Adressübertragung aktivieren. Diese Ausnahme tritt jedoch auf, wenn das Übertragungskonto versucht, die Übertragung zu akzeptieren. Standardmäßig sind alle AWS Konten auf 5 Elastic IP-Adressen pro Region beschränkt. Anweisungen zur Erhöhung des Limits finden Sie unter Kontingent für Elastic-IP-Adressen.
- InvalidTransfer. AddressCustomPtrSet: Wenn Sie oder jemand in Ihrer Organisation die Elastic IP-Adresse, die Sie übertragen möchten, für die umgekehrte DNS-Suche konfiguriert haben, kann das Quellkonto die Übertragung für die Elastic IP-Adresse ermöglichen. Diese Ausnahme tritt jedoch auf, wenn das Übertragungskonto versucht, die Übertragung zu akzeptieren. Um dieses Problem zu beheben, muss das Quellkonto den DNS-Datensatz für die Elastic-IP-Adresse entfernen. Weitere Informationen finden Sie unter Erstellen Sie einen Reverse-DNS-Eintrag für E-Mails bei Amazon EC2.
- InvalidTransfer. AddressAssociated: Wenn eine Elastic IP-Adresse mit einer ENI oder EC2 Instance verknüpft ist, kann das Quellkonto die Übertragung für die Elastic IP-Adresse ermöglichen. Diese Ausnahme tritt jedoch auf, wenn das Übertragungskonto versucht, die Übertragung zu akzeptieren. Um dieses Problem zu beheben, muss die Zuordnung für das

Quellkonto der Elastic-IP-Adresse aufgehoben worden. Weitere Informationen finden Sie unter Aufheben der Zuordnung einer Elastic IP-Adresse.

Für alle anderen Ausnahmen wenden Sie sich an Support.

Diese Schritte müssen von dem Übertragungskonto ausgeführt werden.

Console

So akzeptieren Sie die Übertragung einer Elastic-IP-Adresse

1. Stellen Sie sicher, dass Sie das Übertragungskonto verwenden.
2. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
3. Wählen Sie im Navigationsbereich Elastic aus IPs.
4. Wählen Sie Actions (Aktionen), Accept transfer (Übertragung akzeptieren).
5. Wenn Sie die Übertragung akzeptieren, werden keine Tags, die der übertragenen Elastic-IP-Adresse zugeordnet sind, mit der Elastic-IP-Adresse übertragen. Wenn Sie ein Tag Name für die von Ihnen akzeptierte Elastic-IP-Adresse definieren möchten, wählen Sie Create a tag with a key of 'Name' and a value that you specify (Erstellen eines Tags mit dem Schlüssel „Name“ und einem von Ihnen angegebenen Wert) aus.
6. Geben Sie die Elastic-IP-Adresse ein, die Sie übertragen möchten.
7. Wenn Sie mehrere übertragene Elastic-IP-Adressen akzeptieren, wählen Sie Add address (Adresse hinzufügen), um eine zusätzliche Elastic-IP-Adresse einzugeben.
8. Wählen Sie Absenden aus.

AWS CLI

So akzeptieren Sie die Übertragung einer Elastic-IP-Adresse

Verwenden Sie den Befehl accept-address-transfer.

```
aws ec2 accept-address-transfer --address 100.21.184.216
```

PowerShell

So akzeptieren Sie die Übertragung einer Elastic-IP-Adresse

Verwenden Sie das cmdlet Approve-EC2AddressTransfer.

```
Approve-EC2AddressTransfer -Address 100.21.184.216
```

Deaktivieren der Übertragung von Elastic-IP-Adressen

In diesem Abschnitt wird beschrieben, wie Sie eine Elastic-IP-Übertragung deaktivieren, nachdem die Übertragung aktiviert wurde.

Diese Schritte müssen von dem Quellkonto ausgeführt werden, das die Übertragung aktiviert hat.

Console

So deaktivieren Sie die Übertragung einer Elastic-IP-Adresse

1. Stellen Sie sicher, dass Sie das Quell- AWS-Konto verwenden.
2. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
3. Wählen Sie im Navigationsbereich Elastic aus IPs.
4. Vergewissern Sie sich IPs, dass Sie in der Ressourcenliste von Elastic die Eigenschaft aktiviert haben, die die Spalte Übertragungsstatus anzeigt.
5. Wählen Sie eine oder mehrere Elastic-IP-Adressen aus, die den Transfer status (Übertragungsstatus) Pending (Ausstehend) haben, und wählen Sie Actions (Aktionen), Disable transfer (Übertragung deaktivieren) aus.
6. Bestätigen Sie durch Eingabe von **`disable`** in das Textfeld.
7. Wählen Sie Absenden aus.

AWS CLI

So deaktivieren Sie die Übertragung von Elastic-IP-Adressen

Verwenden Sie den Befehl disable-address-transfer.

```
aws ec2 disable-address-transfer --allocation-id eipalloc-09ad461b0d03f6aaf
```

PowerShell

So deaktivieren Sie die Übertragung von Elastic-IP-Adressen

Verwenden Sie das cmdlet Disable-EC2AddressTransfer.

```
Disable-EC2AddressTransfer -AllocationId eipalloc-09ad461b0d03f6aaf
```

Freigeben einer Elastic-IP-Adresse

Wenn Sie eine Elastic-IP-Adresse nicht mehr benötigen, empfehlen wir, diese freizugeben. Die Elastic IP-Adresse, die veröffentlicht werden soll, darf derzeit keiner AWS Ressource zugeordnet sein.

Console

So geben Sie eine Elastic-IP-Adresse frei

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic aus IPs.
3. Wählen Sie die Elastic IP-Adresse, die freigegeben werden soll, und wählen Sie Actions (Aktionen), Release Elastic IP addresses (Elastic IP-Adressen freigeben).
4. Wählen Sie Release (Freigeben).

AWS CLI

So geben Sie eine Elastic-IP-Adresse frei

Verwenden Sie den Befehl release-address AWS CLI .

```
aws ec2 release-address --allocation-id eipalloc-64d5890a
```

PowerShell

So geben Sie eine Elastic-IP-Adresse frei

Verwenden Sie das cmdlet Remove-EC2Address.

```
Remove-EC2Address -AllocationId eipalloc-64d5890a
```

Nachdem Sie Ihre Elastic-IP-Adresse freigeben, können Sie sie möglicherweise wiederherstellen. Die folgenden Regeln gelten:

- Sie können eine Elastic-IP-Adresse nicht wiederherstellen, wenn sie einem anderen AWS -Konto zugeordnet wurde oder wenn dies dazu führen würde, dass Sie Ihren Elastic-IP-Adressen-Grenzwert überschreiten.
- Sie können keine Tags wiederherstellen, die einer Elastic-IP-Adresse zugeordnet sind.

AWS CLI

So stellen Sie eine Elastic IP-Adresse wieder her:

Verwenden Sie den -Befehl allocate-address.

```
aws ec2 allocate-address \
    --domain vpc \
    --address 203.0.113.3
```

PowerShell

So stellen Sie eine Elastic IP-Adresse wieder her:

Verwenden Sie das cmdlet New-EC2Address.

```
New-EC2Address `
    -Address 203.0.113.3 `
    -Domain vpc `
    -Region us-east-1
```

Erstellen Sie einen Reverse-DNS-Eintrag für E-Mails bei Amazon EC2

Wenn Sie beabsichtigen, E-Mails von einer EC2 Instance aus an Dritte zu senden, empfehlen wir Ihnen, eine oder mehrere Elastic IP-Adressen bereitzustellen und den Elastic IP-Adressen, die Sie zum Senden von E-Mails verwenden, statische Reverse-DNS-Einträge zuzuweisen. Auf diese Weise können Sie verhindern, dass Ihre E-Mail von einigen Anti-Spam-Organisationen als Spam gekennzeichnet wird. AWS arbeitet mit ISPs Anti-Spam-Organisationen im Internet zusammen, um die Wahrscheinlichkeit zu verringern, dass Ihre von diesen Adressen gesendeten E-Mails als Spam gekennzeichnet werden.

Überlegungen

- Bevor Sie einen Reverse-DNS-Datensatz erstellen, müssen Sie einen entsprechenden Forward-DNS-Datensatz (Record-Typ A) einrichten, der auf Ihre Elastic IP-Adresse verweist.
- Wenn einer Elastic IP-Adresse ein Reverse-DNS-Datensatz zugewiesen ist, wird die Elastic IP-Adresse fest mit Ihrem Konto verknüpft und kann von dem Konto nur freigegeben werden, wenn der Datensatz entfernt wird.
- Wenn Sie Kontakt aufgenommen haben Support , um Reverse-DNS für eine Elastic IP-Adresse einzurichten, können Sie das Reverse-DNS entfernen, aber Sie können die Elastic IP-Adresse nicht freigeben, da sie gesperrt ist von. Support Wenden Sie sich an den AWS -Support, um die elastische IP-Adresse zu entsperren. Nachdem die Elastic-IP-Adresse entsperrt wurde, können Sie sie freigeben.
- [AWS GovCloud (US) Region] Sie können keinen umgekehrten DNS-Datensatz erstellen. AWS muss die statischen Reverse-DNS-Datensätze für Sie zuweisen. Eröffnen Sie einen Support-Fall, um Einschränkungen beim Reverse-DNS und beim Senden von E-Mails aufzuheben. Sie müssen Ihre Elastic-IP-Adressen und Reverse-DNS-Datensätze angeben.

Erstellen eines Reverse-DNS-Datensatzes

Sie können einen Reverse-DNS-Eintrag für Ihre Elastic IP-Adresse wie folgt erstellen.

Console

So erstellen Sie einen Reverse-DNS-Datensatz

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic aus IPs.
3. Wählen Sie die Elastic IP-Adresse aus und wählen Sie Actions (Aktionen), Reverse-DNS aktualisieren.
4. Geben Sie für Reverse DNS domain name (Reverse-DNS-Domain-Name) den Domain-Namen ein.
5. Geben Sie **`update`** zur Bestätigung ein.
6. Wählen Sie Update (Aktualisieren) aus.

AWS CLI

So erstellen Sie einen Reverse-DNS-Datensatz

Verwenden Sie den Befehl modify-address-attribute.

```
aws ec2 modify-address-attribute \
    --allocation-id eipalloc-abcdef01234567890 \
    --domain-name example.com
```

Es folgt eine Beispielausgabe.

```
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.net.",
            "PtrRecordUpdate": {
                "Value": "example.com.",
                "Status": "PENDING"
            }
        }
    ]
}
```

PowerShell

So erstellen Sie einen Reverse-DNS-Datensatz

Verwenden Sie das cmdlet Edit-EC2AddressAttribute.

```
Edit-EC2AddressAttribute `
    -AllocationId 'eipalloc-abcdef01234567890' `
    -DomainName 'example.com' |
Format-List `
    AllocationId, PtrRecord, PublicIp,
    @{Name='PtrRecordUpdate';Expression={$_.PtrRecordUpdate | Format-List | Out-
String}}
```

Es folgt eine Beispielausgabe.

```
AllocationId    : eipalloc-abcdef01234567890
PtrRecord       : example.net.
PublicIp        : 192.0.2.0
PtrRecordUpdate :
                  Reason :
                  Status : PENDING
                  Value  : example.com.
```

Entfernen eines Reverse-DNS-Datensatzes

Sie können einen Reverse-DNS-Eintrag wie folgt aus Ihrer Elastic IP-Adresse entfernen.

Wenn Sie die folgende Fehlermeldung erhalten, können Sie eine Anfrage zur Aufhebung der Einschränkungen beim Senden von E-Mails an uns senden, um Support Unterstützung zu erhalten.

```
The address cannot be released because it is locked to your account.
```

Console

So entfernen Sie einen Reverse-DNS-Datensatz

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic aus IPs.
3. Wählen Sie die Elastic IP-Adresse aus und wählen Sie Actions (Aktionen), Reverse-DNS aktualisieren.
4. Löschen Sie für Reverse DNS domain name (Reverse-DNS-Domain-Name) den Domain-Namen.
5. Geben Sie **`update`** zur Bestätigung ein.
6. Wählen Sie Update (Aktualisieren) aus.

AWS CLI

So entfernen Sie einen Reverse-DNS-Datensatz

Verwenden Sie den Befehl reset-address-attribute.

```
aws ec2 reset-address-attribute \
```

```
    --allocation-id eipalloc-abcdef01234567890 \
    --attribute domain-name
```

Es folgt eine Beispielausgabe.

```
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.com.",
            "PtrRecordUpdate": {
                "Value": "example.net.",
                "Status": "PENDING"
            }
        }
    ]
}
```

PowerShell

So entfernen Sie einen Reverse-DNS-Datensatz

Verwenden Sie das cmdlet Reset-EC2AddressAttribute.

```
Reset-EC2AddressAttribute `
    -AllocationId 'eipalloc-abcdef01234567890' `
    -Attribute domain-name |
Format-List `
    AllocationId, PtrRecord, PublicIp,
    @{Name='PtrRecordUpdate';Expression={$_.PtrRecordUpdate | Format-List | Out-
String}}
```

Es folgt eine Beispielausgabe.

```
AllocationId    : eipalloc-abcdef01234567890
PtrRecord       : example.com.
PublicIp        : 192.0.2.0
PtrRecordUpdate :
                  Reason :
                  Status : PENDING
                  Value  : example.net.
```

Elastic-Network-Schnittstelle

Eine Elastic-Network-Schnittstelle ist eine logische Netzwerkkomponente in einer VPC, die eine virtuelle Netzwerkkarte darstellt. Sie können Netzwerkschnittstellen erstellen und konfigurieren und sie an Instances anfügen, die Sie in derselben Availability Zone starten. Die Attribute einer Netzwerkschnittstelle folgen der Netzwerkschnittstelle, wenn diese an eine Instance angefügt oder von dieser getrennt und erneut an eine andere Instance angefügt wird. Wenn Sie eine Netzwerkschnittstelle von einer Instance zu einer anderen verschieben, wird der Netzwerkdatenverkehr von der originalen Instance zur neuen Instance umgeleitet.

Beachten Sie, dass diese AWS Ressource in der AWS-Managementkonsole und der EC2 Amazon-API als Netzwerkschnittstelle bezeichnet wird. Daher verwenden wir „Netzwerkschnittstelle“ in dieser Dokumentation anstelle von „Elastic-Network-Schnittstelle“. Der Begriff „Netzwerkschnittstelle“ in dieser Dokumentation bedeutet immer „Elastic-Network-Schnittstelle“.

Netzwerkschnittstellen-Attribute

Eine Netzwerkschnittstelle kann folgende Attribute enthalten:

- Eine primäre private IPv4 Adresse aus dem IPv4 Adressbereich Ihres Subnetzes
- Eine primäre IPv6 Adresse aus dem IPv6 Adressbereich Ihres Subnetzes
- Sekundäre private IPv4 Adressen aus dem IPv4 Adressbereich Ihres Subnetzes
- Eine Elastic IP-Adresse (IPv4) für jede private IPv4 Adresse
- Eine öffentliche IPv4 Adresse
- Sekundäre IPv6 Adressen
- Sicherheitsgruppen
- Eine MAC-Adresse
- Ein source/destination Scheckkennzeichen
- Eine Beschreibung

Überwachen von Datenverkehr

Sie können ein VPC-Flow-Protokoll auf Ihrer Netzwerkschnittstelle aktivieren, um Informationen über den Datenverkehr zu und von einer Netzwerkschnittstelle zu erfassen. Nachdem Sie ein Flow-Protokoll erstellt haben, können Sie dessen Daten in Amazon CloudWatch Logs anzeigen und

abrufen. Weitere Informationen finden Sie unter VPC-Flow-Protokolle im Benutzerhandbuch für Amazon VPC.

Inhalt

- Netzwerkschnittstellen-Konzepte
- Netzwerkkarten
- Maximale IP-Adressen pro Netzwerkschnittstelle
- Erstellen Sie eine Netzwerkschnittstelle für Ihre EC2 Instance
- Netzwerkschnittstellen-Anhänge für Ihre EC2 Instance
- Die IP-Adressen für Ihre Netzwerkschnittstellen verwalten
- Ändern der Netzwerkschnittstellen-Attribute
- Mehrere Netzwerkschnittstellen für Ihre EC2 Amazon-Instances
- Vom Anforderer verwaltete Netzwerkschnittstellen
- Präfix-Delegierung von Amazon-EC2-Netzwerkschnittstellen
- Löschen einer Netzwerkschnittstelle

Netzwerkschnittstellen-Konzepte

Die folgenden wichtigen Konzepte sollten Sie verstehen, wenn Sie mit der Verwendung von Netzwerkschnittstellen beginnen.

Primäre Netzwerkschnittstelle

Jede Instance verfügt über eine Standard-Netzwerkschnittstelle, die als primäre Netzwerkschnittstelle bezeichnet wird. Sie können eine primäre Netzwerkschnittstelle nicht von einer Instance trennen.

Sekundäre Netzwerkschnittstellen

Sie können sekundäre Netzwerkschnittstellen erstellen und an Ihre Instance anfügen. Die maximale Anzahl von Netzwerkschnittstellen, die Sie verwenden können, variiert nach Instance-Typ. Weitere Informationen finden Sie unter Maximale IP-Adressen pro Netzwerkschnittstelle.

IPv4 Adressen für Netzwerkschnittstellen

Wenn Sie eine EC2 Instance in einem IPv4 Nur-Only- oder Dual-Stack-Subnetz starten, erhält die Instance eine primäre private IP-Adresse aus dem IPv4 Adressbereich des Subnetzes. Sie können auch zusätzliche private IPv4 Adressen angeben, die als sekundäre private Adressen

bezeichnet werden. IPv4 Im Gegensatz zu privaten IP-Adressen können sekundäre private IP-Adressen von einer Instance zur anderen erneut zugewiesen werden.

Öffentliche IPv4 Adressen für Netzwerkschnittstellen

Alle Subnetze verfügen über ein veränderbares Attribut, das bestimmt, ob Netzwerkschnittstellen, die in diesem Subnetz erstellt wurden (und damit Instances, die in diesem Subnetz gestartet wurden), eine öffentliche Adresse zugewiesen wird. IPv4 Weitere Informationen finden Sie unter Subnetz-Einstellungen im Amazon-VPC-Benutzerhandbuch. Wenn Sie eine Instance starten, wird die IP-Adresse der primären Netzwerkschnittstelle zugewiesen. Wenn Sie beim Starten einer Instance eine vorhandene Netzwerkschnittstelle als primäre Netzwerkschnittstelle angeben, wird die öffentliche IPv4 Adresse durch diese Netzwerkschnittstelle bestimmt.

Wenn Sie eine Netzwerkschnittstelle erstellen, erbt sie das Attribut für die öffentliche IPv4 Adressierung aus dem Subnetz. Wenn Sie später das Attribut für die öffentliche IPv4 Adressierung des Subnetzes ändern, behält die Netzwerkschnittstelle die Einstellung bei, die bei der Erstellung gültig war.

Wir geben die öffentliche IP-Adresse für frei, wenn die Instance angehalten ist, in den Ruhezustand versetzt wurde oder beendet wird. Wir weisen eine neue öffentliche IP-Adresse zu, wenn Sie Ihre gestoppte oder in den Ruhezustand versetzte Instance starten, es sei denn, sie hat eine sekundäre Netzwerkschnittstelle oder eine sekundäre private IPv4 Adresse, die mit einer Elastic IP-Adresse verknüpft ist.

IPv6 Adressen für Netzwerkschnittstellen

Wenn Sie Ihrer VPC und Ihrem Subnetz IPv6 CIDR-Blöcke zuordnen, können Sie einer Netzwerkschnittstelle IPv6 Adressen aus dem Subnetzbereich zuweisen. Jede IPv6 Adresse kann einer Netzwerkschnittstelle zugewiesen werden.

Alle Subnetze verfügen über ein modifizierbares Attribut, das bestimmt, ob Netzwerkschnittstellen, die in diesem Subnetz erstellt wurden (und damit Instances, die in diesem Subnetz gestartet wurden), automatisch eine IPv6 Adresse aus dem Bereich des Subnetzes zugewiesen wird. Wenn Sie eine Instance starten, wird die IPv6 Adresse der primären Netzwerkschnittstelle zugewiesen.

Elastic-IP-Adressen für Netzwerkschnittstelle

Sie können eine Elastic IP-Adresse mit einer der privaten IPv4 Adressen für die Netzwerkschnittstelle verknüpfen. Sie können jeder privaten IPv4 Adresse eine Elastic IP-Adresse zuordnen. Wenn Sie eine Elastic-IP-Adresse von einer Netzwerkschnittstelle trennen, können Sie sie freigeben oder einer anderen Instance zuordnen.

Beendigungsverhalten

Sie können das Beendigungsverhalten für eine Netzwerkschnittstelle ändern, die mit einer Instance verbunden ist. Sie können angeben, ob die Netzwerkschnittstelle automatisch gelöscht werden soll, wenn Sie die Instance beenden, mit der sie verbunden ist.

Quell-/Zielprüfung

Sie können source/destination Prüfungen aktivieren oder deaktivieren, die sicherstellen, dass die Instance entweder die Quelle oder das Ziel des empfangenen Traffics ist. Source/destination checks are enabled by default. You must disable source/destinationprüft, ob auf der Instance Dienste wie Netzwerkadressübersetzung, Routing oder Firewalls ausgeführt werden.

Vom Anforderer verwaltete Netzwerkschnittstellen

Diese Netzwerkschnittstellen werden von erstellt und verwaltet AWS-Services , damit Sie einige Ressourcen und Dienste nutzen können. Sie können diese Netzwerkschnittstellen nicht selbst verwalten. Weitere Informationen finden Sie unter Vom Anforderer verwaltete Netzwerkschnittstellen.

Präfixdelegierung

Ein Präfix ist ein reservierter privater Bereich IPv4 oder IPv6 CIDR-Bereich, den Sie Netzwerkschnittstellen, die einer Instanz zugeordnet sind, für die automatische oder manuelle Zuweisung zuweisen. Mithilfe von delegierten Präfixen können Sie Dienste schneller starten, indem Sie einen Bereich von IP-Adressen als einzelnes Präfix zuweisen.

Verwaltete Netzwerkschnittstellen

Eine verwaltete Netzwerkschnittstelle wird von einem Service-Anbieter wie Amazon EKS Auto Mode verwaltet. Sie können die Einstellungen einer verwalteten Netzwerkschnittstelle nicht direkt ändern. Verwaltete Netzwerkschnittstellen werden durch einen Wahr-Wert im Feld Verwaltet identifiziert. Weitere Informationen finden Sie unter Verwaltete Amazon-EC2-Instances.

Netzwerkkarten

Die meisten Instance-Typen unterstützen eine Netzwerkkarte. Instance-Typen, die mehrere Netzwerkkarten unterstützen, bieten eine höhere Netzwerkleistung, einschließlich Bandbreiten von über 100 Gbit/s und verbesserter Paketratenleistung. Wenn Sie eine Netzwerkschnittstelle an eine Instance anhängen, die mehrere Netzwerkkarten unterstützt, können Sie die Netzwerkkarte für die Netzwerkschnittstelle auswählen. Die primäre Netzwerkschnittstelle muss dem Netzwerkkartenindex 0 zugewiesen sein.

EFA- und Nur-EFA-Netzwerkschnittstellen zählen als Netzwerkschnittstelle. Sie können pro Netzwerkkarte nur eine EFA- oder Nur-EFA-Netzwerkschnittstelle zuweisen. Die primäre Netzwerkschnittstelle kann keine Nur-EFA-Netzwerkschnittstelle sein.

Die folgenden Instance-Typen unterstützen mehrere Netzwerkkarten. Mehr Informationen zur Anzahl der Netzwerkschnittstellen, die ein Instance-Typ unterstützt, finden Sie unter Maximale IP-Adressen pro Netzwerkschnittstelle.

Instance-Typ	Anzahl der Netzwerkkarten
c6in.32xlarge	2
c6in.metal	2
c8gn.48xlarge	2
c8gn.metal-48xl	2
dl1.24xlarge	4
g6e.24xlarge	2
g6e.48xlarge	4
hpc6id.32xlarge	2
hpc7a.12xlarge	2
hpc7a.24xlarge	2
hpc7a.48xlarge	2
hpc7a.96xlarge	2
m6idn.32xlarge	2
m6idn.metal	2
m6in.32xlarge	2
m6in.metal	2

Instance-Typ	Anzahl der Netzwerkkarten
p4d.24xlarge	4
p4de.24xlarge	4
p5.48xlarge	32
p5e.48xlarge	32
p5en.48xlarge	16
p6-b200.48xlarge	8
p6-b300.48xlarge	17
p6e-gb200.36xlarge	17
r8gn.48xlarge	2
r8gn.metal-48xl	2
r6idn.32xlarge	2
r6idn.metal	2
r6in.32xlarge	2
r6in.metal	2
trn1.32xlarge	8
trn1n.32xlarge	16
trn2.48xlarge	16
trn2u.48xlarge	16
u7in-16tb.224xlarge	2
u7in-24tb.224xlarge	2

Instance-Typ	Anzahl der Netzwerkkarten
u7in-32tb.224xlarge	2
u7inh-32tb.480xlarge	2

Maximale IP-Adressen pro Netzwerkschnittstelle

Jeder Instance-Typ unterstützt eine maximale Anzahl von Netzwerkschnittstellen, eine maximale Anzahl von privaten IPv4 Adressen pro Netzwerkschnittstelle und eine maximale Anzahl von IPv6 Adressen pro Netzwerkschnittstelle. Das Limit für IPv6 Adressen ist unabhängig von dem Limit für private IPv4 Adressen pro Netzwerkschnittstelle. Beachten Sie, dass alle Instance-Typen die IPv6 Adressierung unterstützen, mit Ausnahme der folgenden: C1, M1, M2, M3 und T1.

Verfügbare Netzwerkschnittstellen

Der Amazon EC2 Instance Types Guide enthält Informationen zu den Netzwerkschnittstellen, die für jeden Instance-Typ verfügbar sind. Weitere Informationen finden Sie hier:

- Netzwerkspezifikationen – Allgemeiner Zweck
- Netzwerkspezifikationen – Für Datenverarbeitungsleistung optimiert
- Netzwerkspezifikationen – Arbeitsspeicheroptimiert
- Netzwerkspezifikationen – Speicheroptimiert
- Netzwerkspezifikationen – Beschleunigte Datenverarbeitung
- Netzwerkspezifikationen – Hochleistungs-Datenverarbeitung
- Netzwerkspezifikationen – Vorgängergeneration

Console

So rufen Sie die maximale Anzahl an Netzwerkschnittstellen ab

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instance Types (Instance-Typen) aus.
3. Fügen Sie einen Filter hinzu, um den Instance-Typ (Instance-Typ=c5.12xlarge) oder die Instance-Familie (Instance-Familie=c5) anzugeben.

4. (Optional) Wählen Sie das Symbol Einstellungen und aktivieren Sie dann Maximale Anzahl an Netzwerkschnittstellen. Diese Spalte gibt die maximale Anzahl von Netzwerkschnittstellen für jeden Instance-Typ an.
5. (Optional) Wählen Sie den Instance-Typ aus. Suchen Sie auf der Registerkarte Netzwerk nach Maximale Anzahl von Netzwerkschnittstellen.

AWS CLI

So rufen Sie die maximale Anzahl an Netzwerkschnittstellen ab

Sie können den describe-instance-typesBefehl verwenden, um Informationen über einen Instance-Typ anzuzeigen, z. B. die unterstützten Netzwerkschnittstellen und IP-Adressen pro Schnittstelle. Im folgenden Beispiel werden diese Informationen für alle C5-Instances angezeigt.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=c5.*" \
    --query "InstanceTypes[].{ \
        Type: InstanceType, \
        MaxENI: NetworkInfo.MaximumNetworkInterfaces, \
        IPv4addr: NetworkInfo.Ipv4AddressesPerInterface}" \
    --output table
```

Es folgt eine Beispielausgabe.

```
-----------------------------------------
|        DescribeInstanceTypes        |
+----------+----------+---------------+
| IPv4addr | MaxENI   |     Type      |
+----------+----------+---------------+
|  30      |  8       |  c5.4xlarge   |
|  50      |  15      |  c5.24xlarge  |
|  15      |  4       |  c5.xlarge    |
|  30      |  8       |  c5.12xlarge  |
|  10      |  3       |  c5.large     |
|  15      |  4       |  c5.2xlarge   |
|  50      |  15      |  c5.metal     |
|  30      |  8       |  c5.9xlarge   |
|  50      |  15      |  c5.18xlarge  |
+----------+----------+---------------+
```

PowerShell

So rufen Sie die maximale Anzahl an Netzwerkschnittstellen ab

Sie können den Get-EC2InstanceType PowerShell Befehl verwenden, um Informationen über einen Instance-Typ anzuzeigen, z. B. die unterstützten Netzwerkschnittstellen und IP-Adressen pro Schnittstelle. Im folgenden Beispiel werden diese Informationen für alle C5-Instances angezeigt.

```
Get-EC2InstanceType -Filter @{Name="instance-type"; Values="c5.*"} | `
Select-Object `
    @{Name='Ipv4AddressesPerInterface';
 Expression={($_.Networkinfo.Ipv4AddressesPerInterface)}},
    @{Name='MaximumNetworkInterfaces';
 Expression={($_.Networkinfo.MaximumNetworkInterfaces)}},
    InstanceType | `
Format-Table -AutoSize
```

Es folgt eine Beispielausgabe.

```
Ipv4AddressesPerInterface MaximumNetworkInterfaces InstanceType
------------------------- ------------------------ ------------
                       30                        8 c5.4xlarge
                       15                        4 c5.xlarge
                       30                        8 c5.12xlarge
                       50                       15 c5.24xlarge
                       30                        8 c5.9xlarge
                       50                       15 c5.metal
                       15                        4 c5.2xlarge
                       10                        3 c5.large
                       50                       15 c5.18xlarge
```

Erstellen Sie eine Netzwerkschnittstelle für Ihre EC2 Instance

Sie können eine Netzwerkschnittstelle für Ihre EC2 Instances erstellen. Wenn Sie eine Netzwerkschnittstelle erstellen, geben Sie das Subnetz an, für das sie erstellt wurde. Sie können die Netzwerkschnittstelle nach der Erstellung nicht zu einem anderen Subnetz verschieben. Sie müssen eine Netzwerkschnittstelle an eine Instance in derselben Availability Zone anfügen. Sie können eine sekundäre Netzwerkschnittstelle von einer Instance abtrennen und sie dann an eine andere Instance in derselben Availability Zone anhängen. Sie können eine primäre Netzwerkschnittstelle

nicht von einer Instance trennen. Weitere Informationen finden Sie unter the section called “Netzwerkschnittstellen-Anhänge”.

Console

So erstellen Sie eine Netzwerkschnittstelle

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Klicken Sie auf Create network interface (Netzwerkschnittstellen erstellen).
4. (Optional) Geben Sie unter Description (Beschreibung) einen aussagekräftigen Namen ein.
5. Wählen Sie für Subnet (Subnetz) ein Subnetz aus. Die in den nachfolgenden Schritten verfügbaren Optionen ändern sich je nach Art des ausgewählten Subnetzes (IPv4-only, IPv6 - only oder Dual-Stack (IPv4 und)). IPv6
6. Wählen Sie für Schnittstellentyp eine der folgenden Optionen:
   - ENA: Eine leistungsstarke Netzwerkschnittstelle, die entwickelt wurde, um hohen Durchsatz und hohe packet-per-second TCP/IP Protokollraten zu bewältigen und gleichzeitig die CPU-Auslastung zu minimieren. Dies ist der Standardwert. Weitere Informationen über ENA finden Sie unter Elastic Network Adapter.
   - EFA mit ENA: Eine Netzwerkschnittstelle, die sowohl ENA- als auch EFA-Geräte für den herkömmlichen Transport sowie für den TCP/IP SRD-basierten Transport unterstützt. Wenn Sie EFA mit ENA wählen, muss die Instance, an die Sie es anhängen, EFA unterstützen. Weitere Informationen zu EFA finden Sie unter Elastic Fabric Adapter.
   - Nur EFA: Eine leistungsstarke Netzwerkschnittstelle, die für die Kommunikation zwischen Knoten mit hohem Durchsatz und geringer Latenz für SRD-basierten Transport konzipiert ist und gleichzeitig den Betriebssystemstapel umgeht. Wenn Sie diese Option wählen, muss die Instance, an die Sie es anhängen, EFA unterstützen. Nur-EFA-Netzwerkschnittstellen unterstützen keine IP-Adressen. Weitere Informationen zu EFA finden Sie unter Elastic Fabric Adapter.
7. Führen Sie für Private IPv4 Adresse einen der folgenden Schritte aus:
   - Wählen Sie Automatisch zuweisen, EC2 damit Amazon eine IPv4 Adresse aus dem Subnetz auswählen kann.
   - Wählen Sie Benutzerdefiniert und geben Sie eine IPv4 Adresse ein, die Sie aus dem Subnetz auswählen.

8. (Nur Subnetze mit IPv6 Adressen) Führen Sie für die IPv6 Adresse einen der folgenden Schritte aus:
   - Wählen Sie Keine, wenn Sie der Netzwerkschnittstelle keine IPv6 Adresse zuweisen möchten.
   - Wählen Sie Automatisch zuweisen, EC2 damit Amazon eine IPv6 Adresse aus dem Subnetz auswählen kann.
   - Wählen Sie Benutzerdefiniert und geben Sie eine IPv6 Adresse ein, die Sie aus dem Subnetz auswählen.
9. (Optional) Wenn Sie eine Netzwerkschnittstelle in einem Dual-Stack- oder IPv6 Nur-Subnetz erstellen, haben Sie die Möglichkeit, primäre IP zuzuweisen. IPv6 Dadurch wird der Netzwerkschnittstelle eine primäre IPv6 globale Unicast-Adresse (GUA) zugewiesen. Durch die Zuweisung einer primären IPv6 Adresse können Sie verhindern, dass der Datenverkehr zu den Instances oder unterbrochen wird. ENIs Wählen Sie „Aktivieren“, wenn die Instance, an die diese ENI angehängt wird, darauf angewiesen ist, dass sich ihre IPv6 Adresse nicht ändert. AWS weist automatisch eine IPv6 Adresse, die der an Ihre Instance angehängten ENI zugeordnet ist, als primäre IPv6 Adresse zu. Sobald Sie eine IPv6 GUA-Adresse als primäre Adresse aktiviert haben IPv6, können Sie sie nicht mehr deaktivieren. Wenn Sie eine IPv6 GUA-Adresse als primäre Adresse aktivieren IPv6, wird die erste IPv6 GUA zur primären IPv6 Adresse gemacht, bis die Instance beendet oder die Netzwerkschnittstelle getrennt wird. Wenn Sie mehrere IPv6 Adressen mit einer ENI verknüpft haben, die an Ihre Instance angehängt ist, und Sie eine primäre IPv6 Adresse aktivieren, wird die erste mit der ENI verknüpfte IPv6 GUA-Adresse zur primären IPv6 Adresse.
10. (Optional) So erstellen Sie ein Elastic Fabric Adapter, wählen Sie Elastic Fabric Adapter, Aktivieren.
11. (Optional) Unter Erweiterte Einstellungen können Sie optional die IP-Präfix-Delegierung festlegen. Weitere Informationen finden Sie unter Präfixdelegierung.
    - Automatische Zuweisung — AWS wählt das Präfix aus den IPv4 oder IPv6 CIDR-Blöcken für das Subnetz aus und weist es der Netzwerkschnittstelle zu.
    - Benutzerdefiniert — Sie geben das Präfix aus den IPv4 oder IPv6 CIDR-Blöcken für das Subnetz an und AWS überprüfen, ob das Präfix nicht bereits anderen Ressourcen zugewiesen ist, bevor Sie es der Netzwerkschnittstelle zuweisen.
12. (Optional) Ändern Sie unter Erweiterte Einstellungen für Timeout für Nachverfolgung von Leerlaufverbindungen die standardmäßigen Timeouts für Leerlaufverbindungen. Weitere Informationen finden Sie unter Timeout für die Nachverfolgung von Leerlaufverbindungen.

- Timeout für bestehende TCP-Verbindungen: Timeout (in Sekunden) für bestehende TCP-Verbindungen im Leerlauf.
  - Min: `60` Sekunden
  - Max: `432000` Sekunden
  - Standard: `350` Sekunden für Nitrov6-Instance-Typen, ausgenommen P6e- 00. GB2 Und `432000` Sekunden für andere Instance-Typen, einschließlich P6e-00. GB2
  - Empfohlen: Weniger als `432000` Sekunden.
- UDP-Timeout: Timeout (in Sekunden) für UDP-Datenflüsse im Leerlauf, bei denen Datenverkehr nur in eine Richtung oder nur in einer einzelnen Anforderung-Antwort-Transaktion übermittelt wurde.
  - Min: `30` Sekunden
  - Max: `60` Sekunden
  - Standardwert: `30` Sekunden
- UDP-Stream-Timeout: Timeout (in Sekunden) für UDP-Datenflüsse im Leerlauf, die als Streams klassifiziert sind, bei denen mehr als eine Anforderung-Antwort-Transaktion stattgefunden hat.
  - Min: `60` Sekunden
  - Max: `180` Sekunden
  - Standardwert: `180` Sekunden

13. Wählen Sie unter Security groups (Sicherheitsgruppen) eine oder mehrere Sicherheitsgruppen aus.
14. (Optional) Wählen Sie für jeden Tag (Markierung) Neuen Tag (Markierung) hinzufügen und geben Sie einen Tag (Markierung)-Schlüssel und einen optionalen Tag (Markierung)-Wert ein.
15. Klicken Sie auf Create network interface (Netzwerkschnittstellen erstellen).

AWS CLI

Beispiel 1: Um eine Netzwerkschnittstelle mit von Amazon ausgewählten IP-Adressen zu erstellen EC2

Verwenden Sie den folgenden create-network-interface-Befehl. In diesem Beispiel wird eine Netzwerkschnittstelle mit einer öffentlichen IPv4 Adresse und einer von Amazon ausgewählten IPv6 Adresse erstellt EC2.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --description "my dual-stack network interface" \
    --ipv6-address-count 1 \
    --groups sg-1234567890abcdef0
```

Beispiel 2: So erstellen Sie eine Netzwerkschnittstelle mit spezifischen IP-Adressen

Verwenden Sie den folgenden create-network-interface-Befehl.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --description "my dual-stack network interface" \
    --private-ip-address 10.251.50.12 \
    --ipv6-addresses 2001:db8::1234:5678:1.2.3.4 \
    --groups sg-1234567890abcdef0
```

Beispiel 3: So erstellen Sie eine Netzwerkschnittstelle mit einer Anzahl von sekundären IP-Adressen

Verwenden Sie den folgenden create-network-interface-Befehl. In diesem Beispiel EC2 wählt Amazon sowohl die primäre IP-Adresse als auch die sekundären IP-Adressen.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --description "my network interface" \
    --secondary-private-ip-address-count 2 \
    --groups sg-1234567890abcdef0
```

Beispiel 4: So erstellen Sie eine Netzwerkschnittstelle mit einer spezifischen sekundären IP-Adresse

Verwenden Sie den folgenden create-network-interface-Befehl. In diesem Beispiel werden eine primäre IP-Adresse und eine sekundäre IP-Adresse angegeben.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
```

```
    --description "my network interface" \
    --private-ip-addresses PrivateIpAddress=10.0.1.30,Primary=true \
                           PrivateIpAddress=10.0.1.31,Primary=false
    --groups sg-1234567890abcdef0
```

PowerShell

Beispiel 1: Um eine Netzwerkschnittstelle mit von Amazon ausgewählten IP-Adressen zu erstellen EC2

Verwenden Sie das cmdlet New-EC2NetworkInterface. In diesem Beispiel wird eine Netzwerkschnittstelle mit einer öffentlichen IPv4 Adresse und einer von Amazon ausgewählten IPv6 Adresse erstellt EC2.

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -Description "my dual-stack network interface" `
    -Ipv6AddresCount 1 `
    -Group sg-1234567890abcdef0
```

Beispiel 2: So erstellen Sie eine Netzwerkschnittstelle mit spezifischen IP-Adressen

Verwenden Sie das cmdlet New-EC2NetworkInterface.

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -Description "my dual-stack network interface" `
    -PrivateIpAddress 10.251.50.12 `
    -Ipv6Address $ipv6addr `
    -Group sg-1234567890abcdef0
```

Definieren Sie die IPv6 Adressen wie folgt.

```
$ipv6addr = New-Object Amazon.EC2.Model.InstanceIpv6Address
$ipv6addr1.Ipv6Address = "2001:db8::1234:5678:1.2.3.4"
```

Beispiel 3: So erstellen Sie eine Netzwerkschnittstelle mit einer Anzahl von sekundären IP-Adressen

Verwenden Sie das cmdlet New-EC2NetworkInterface. In diesem Beispiel EC2 wählt Amazon sowohl die primäre IP-Adresse als auch die sekundären IP-Adressen.

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -Description "my network interface" `
    -SecondaryPrivateIpAddressCount 2 `
    -Group sg-1234567890abcdef0
```

Beispiel 4: So erstellen Sie eine Netzwerkschnittstelle mit einer spezifischen sekundären IP-Adresse

Verwenden Sie das cmdlet New-EC2NetworkInterface. In diesem Beispiel werden eine primäre IP-Adresse und eine sekundäre IP-Adresse angegeben.

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -Description "my network interface" `
    -PrivateIpAddresses @($primary, $secondary) `
    -Group sg-1234567890abcdef0
```

Definieren Sie die sekundären Adressen wie folgt.

```
$primary = New-Object Amazon.EC2.Model.PrivateIpAddressSpecification
$primary.PrivateIpAddress = "10.0.1.30"
$primary.Primary = $true
$secondary = New-Object Amazon.EC2.Model.PrivateIpAddressSpecification
$secondary.PrivateIpAddress = "10.0.1.31"
$secondary.Primary = $false
```

Netzwerkschnittstellen-Anhänge für Ihre EC2 Instance

Sie können Netzwerkschnittstellen erstellen, die von Ihren EC2 Instances als primäre oder sekundäre Netzwerkschnittstellen verwendet werden. Sie müssen einer EC2 Instance eine Netzwerkschnittstelle hinzufügen, wenn sie sich in derselben Availability Zone wie die Netzwerkschnittstelle befindet. Der Instance-Typ einer Instance bestimmt, wie viele Netzwerkschnittstellen Sie an die Instance anhängen können. Weitere Informationen finden Sie unter the section called “IP-Adressen pro Netzwerkschnittstelle”.

Überlegungen

- Sie können eine Netzwerkschnittstelle an eine Instance anfügen, während diese ausgeführt wird („Hot Attach“), wenn sie angehalten ist („Warm Attach“) oder wenn die Instance gestartet wird („Cold Attach“).
- Sie können sekundäre Netzwerkschnittstellen sowohl von ausgeführten als auch von angehaltenen Instances trennen. Die primäre Netzwerkschnittstelle können Sie jedoch nicht trennen.
- Sie können eine sekundäre Netzwerkschnittstelle von einer Instance trennen und einer anderen Instance zuordnen.
- Beim Starten einer Instance mithilfe der CLI, API oder eines SDK können Sie die primäre Netzwerkschnittstelle sowie zusätzliche Netzwerkschnittstellen angeben. Beachten Sie, dass Sie die automatische Zuweisung von öffentlichen IPv4 Adressen nicht aktivieren können, wenn Sie beim Start eine sekundäre Netzwerkschnittstelle hinzufügen.
- Beim Starten einer Amazon Linux- oder Windows Server-Instance mit mehreren Netzwerkschnittstellen werden automatisch Schnittstellen, private IPv4 Adressen und Routing-Tabellen auf dem Betriebssystem der Instance konfiguriert.
- Bei einem Warm- oder Hot-Attach einer zusätzlichen Netzwerkschnittstelle müssen Sie möglicherweise die zweite Schnittstelle manuell aufrufen, die private IPv4 Adresse konfigurieren und die Routing-Tabelle entsprechend ändern. Instances, auf denen Amazon Linux oder Windows Server ausgeführt wird, erkennen den „Warm Attach“ oder „Hot Attach“ automatisch und konfigurieren sich selbst.
- Sie können keine weitere Netzwerkschnittstelle an eine Instance anschließen (z. B. eine NIC-Teaming-Konfiguration), um die Netzwerkbandbreite zur oder von der Dual-Homed-Instance zu erhöhen oder zu verdoppeln.
- Wenn Sie eine oder mehrere Netzwerkschnittstellen aus demselben Subnetz an eine Instance anfügen, kann es zu Netzwerkproblemen wie asymmetrischem Routing kommen. Wenn möglich, fügen Sie stattdessen eine sekundäre private IPv4 Adresse auf der primären Netzwerkschnittstelle hinzu.
- Wenn Sie bei EC2 Instances IPv6 in einem Subnetz nur eine sekundäre Netzwerkschnittstelle anhängen, wird der private DNS-Hostname der sekundären Netzwerkschnittstelle in die primäre IPv6 Adresse der primären Netzwerkschnittstelle aufgelöst.
- [Windows-Instances] – Wenn Sie einer Instance mehrere Netzwerkschnittstellen hinzufügen, müssen Sie die Netzwerkschnittstellen so konfigurieren, dass sie statisches Routing verwenden.

Netzwerkschnittstelle anhängen

Sie können jeder Instance in derselben Availability Zone wie die Netzwerkschnittstelle eine Netzwerkschnittstelle zuordnen, indem Sie entweder die Seite Instances oder Network Interfaces der EC2 Amazon-Konsole verwenden. Alternativ können Sie beim Starten einer Instance eine vorhandene Netzwerkschnittstelle anhängen.

Wenn die öffentliche IPv4 Adresse auf Ihrer Instance veröffentlicht wird, erhält sie keine neue, wenn mehr als eine Netzwerkschnittstelle an die Instance angeschlossen ist. Weitere Informationen zum Verhalten von öffentlichen IPv4 Adressen finden Sie unterÖffentliche IPv4-Adressen.

Console

So können Sie über die Instances-Seite eine Netzwerkschnittstelle anhängen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Aktivieren Sie das Kontrollkästchen für die Instance.
4. Wählen Sie Aktionen, Netzwerk, Netzwerkschnittstelle, anhängen.
5. Wählen Sie eine VPC aus. Die Netzwerkschnittstelle kann sich in derselben VPC wie Ihre Instance oder in einer anderen VPC befinden, die Sie besitzen, sofern sich die Netzwerkschnittstelle in derselben Availability Zone wie die Instance befindet. Auf diese Weise können Sie mehrfach vernetzte Instances VPCs mit unterschiedlichen Netzwerk- und Sicherheitskonfigurationen erstellen.
6. Wählen Sie eine Netzwerkschnittstelle aus. Wenn die Instance mehrere Netzwerkkarten unterstützt, können Sie eine Netzwerkkarte wählen.
7. Wählen Sie Attach (Anfügen) aus.

So können Sie über die Netzwerkschnittstellen-Seite eine Netzwerkschnittstelle anhängen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.
4. Wählen Sie Actions (Aktionen) und Attach (Anfügen).
5. Wählen einer Instance Wenn die Instance mehrere Netzwerkkarten unterstützt, können Sie eine Netzwerkkarte wählen.

6. Wählen Sie Attach (Anfügen) aus.

AWS CLI

So hängen Sie eine Netzwerkschnittstelle an

Verwenden Sie den folgenden attach-network-interface-Befehl.

```
aws ec2 attach-network-interface \
    --network-interface-id eni-1234567890abcdef0 \
    --instance-id i-1234567890abcdef0 \
    --device-index 1
```

PowerShell

So hängen Sie eine Netzwerkschnittstelle an

Verwenden Sie das cmdlet Add-EC2NetworkInterface.

```
Add-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -InstanceId i-1234567890abcdef0 `
    -DeviceIndex 1
```

Netzwerkschnittstelle abhängen

Sie können eine sekundäre Netzwerkschnittstelle, die mit einer EC2 Instance verbunden ist, jederzeit trennen, indem Sie entweder die Seite Instances oder Network Interfaces der EC2 Amazon-Konsole verwenden.

Wenn Sie versuchen, eine Netzwerkschnittstelle, die mit einer Ressource verbunden ist, von einem anderen Dienst zu trennen, z. B. einem ELB-Load Balancer, einer Lambda-Funktion WorkSpace, einem oder einem NAT-Gateway, wird die Fehlermeldung angezeigt, dass Sie nicht berechtigt sind, auf die Ressource zuzugreifen. Um herauszufinden, welcher Service die mit einer Netzwerkschnittstelle verbundene Ressource erstellt hat, überprüfen Sie die Beschreibung der Netzwerkschnittstelle. Wenn Sie die Ressource löschen, wird ihre Netzwerkschnittstelle gelöscht.

Console

So trennen Sie über die Instances-Seite eine Netzwerkschnittstelle

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Aktivieren Sie das Kontrollkästchen für die Instance. Überprüfen Sie den Abschnitt Netzwerk interfaces (Netzwerkschnittstellen) des Reiters Networking (Netzwerk), um zu überprüfen, ob die Netzwerkschnittstelle als sekundäre Netzwerkschnittstelle mit einer Instance verbunden ist.
4. Wählen Sie Aktionen, Netzwerk, Netzwerkschnittstelle trennen.
5. Wählen Sie die Netzwerkschnittstelle aus und klicken Sie auf Detach.

So trennen Sie über die Netzwerkschnittstellen-Seite eine Netzwerkschnittstelle

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle. Überprüfen Sie den Abschnitt Instance details (Instance-Details) des Reiters Einzelheiten, um zu überprüfen, ob die Netzwerkschnittstelle als sekundäre Netzwerkschnittstelle mit einer Instance verbunden ist.
4. Wählen Sie Actions (Aktionen), Loslösen (Detach).
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Trennen.
6. Wenn die Netzwerkschnittstelle nicht von der Instance getrennt wird, können Sie die Option Force detachment (Trennung erzwingen), Aktivieren (Enable) auswählen und den Vorgang erneut ausführen. Wir empfehlen, die Loslösung nur als letzten Ausweg zu erzwingen. Das Erzwingen einer Trennung kann verhindern, dass Sie demselben Index eine andere Netzwerkschnittstelle anfügen, bis Sie die Instance neu starten. Es kann auch verhindern, dass die Instance-Metadaten das Trennen der Netzwerkschnittstelle widerspiegeln, bis Sie die Instance neu starten.

AWS CLI

So trennen Sie eine Netzwerkschnittstelle

Verwenden Sie den folgenden detach-network-interface-Befehl.

```
aws ec2 detach-network-interface --attachment-id eni-attach-016c93267131892c9
```

PowerShell

So trennen Sie eine Netzwerkschnittstelle

Verwenden Sie das cmdlet Dismount-EC2NetworkInterface.

```
Dismount-EC2NetworkInterface -AttachmentId eni-attach-016c93267131892c9
```

Die IP-Adressen für Ihre Netzwerkschnittstellen verwalten

Sie können die folgenden IP-Adressen für Ihre Netzwerkschnittstellen verwalten:

- Elastische IP-Adressen (eine pro IPv4 Privatadresse)
- IPv4 Adressen
- IPv6 Adressen

Console

So verwalten Sie die IP-Adressen einer Netzwerkschnittstelle

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.
4. Gehen Sie wie folgt vor, um die IPv6 Adressen IPv4 und zu verwalten:
   a. Wählen Sie Actions, Manage IP addresses (IP-Adressen verwalten) aus.
   b. Erweitern Sie die Netzwerkschnittstelle.
   c. Bearbeiten Sie für IPv4 Adressen die IP-Adressen nach Bedarf. Um eine zusätzliche IPv4 Adresse zuzuweisen, wählen Sie Neue IP-Adresse zuweisen und geben Sie dann eine IPv4 Adresse aus dem Subnetzbereich an oder lassen Sie sich eine Adresse AWS auswählen.
   d. (Dual-Stack oder IPv6 nur) Bearbeiten Sie für IPv6 Adressen die IP-Adressen nach Bedarf. Um eine zusätzliche IPv6 Adresse zuzuweisen, wählen Sie Neue IP-Adresse

zuweisen und geben Sie dann eine IPv6 Adresse aus dem Subnetzbereich an oder lassen Sie sich eine Adresse AWS auswählen.

e. Um einer Netzwerkschnittstelle eine öffentliche IPv4 Adresse zuzuweisen oder deren Zuweisung aufzuheben, wählen Sie Öffentliche IP automatisch zuweisen. Sie können dies für jede Netzwerkschnittstelle aktivieren oder deaktivieren, es wirkt sich jedoch nur auf die primäre Netzwerkschnittstelle aus.

f. (Dual Stack oder IPv6 nur) Wählen Sie IPv6unter Primäre IP zuweisen die Option Aktivieren aus, um eine primäre Adresse zuzuweisen. IPv6 Die erste GUA, die der Netzwerkschnittstelle zugeordnet ist, wird als primäre IPv6 Adresse ausgewählt. Nachdem Sie eine primäre IPv6 Adresse zugewiesen haben, können Sie sie nicht mehr ändern. Diese Adresse ist die primäre IPv6 Adresse, bis die Instance beendet oder die Netzwerkschnittstelle getrennt wird.

g. Wählen Sie Speichern.

5. Um eine Elastic IP-Adresse zuzuordnen, gehen Sie wie folgt vor:

   a. Wählen Sie Aktionen, Adresse zuweisen aus.

   b. Wählen Sie unter Elastic IP-Adresse die Elastic IP-Adresse aus.

   c. Wählen Sie unter Private IPv4 Adresse die private IPv4 Adresse aus, die der Elastic IP-Adresse zugeordnet werden soll.

   d. (Optional) Wählen Sie Zulassen einer erneuten Verknüpfung der Elastic IP-Adresse, wenn die Netzwerkschnittstelle derzeit mit einer anderen Instance oder Netzwerkschnittstelle verknüpft ist.

   e. Wählen Sie Associate aus.

6. Um die Zuordnung einer Elastic IP-Adresse aufzuheben, gehen Sie folgendermaßen vor:

   a. Wählen Sie Actions, Disassociate address aus.

   b. Wählen Sie unter Öffentliche IP-Adresse die Elastic IP-Adresse aus.

   c. Wählen Sie Disassociate (Zuordnung aufheben) aus.

AWS CLI

Um die IPv4 Adressen zu verwalten

Verwenden Sie den folgenden assign-private-ip-addressesBefehl, um eine IPv4 Adresse zuzuweisen.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --private-ip-addresses 10.0.0.82
```

Verwenden Sie den folgenden unassign-private-ip-addressesBefehl, um die Zuweisung einer IPv4 Adresse aufzuheben.

```
aws ec2 unassign-private-ip-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --private-ip-addresses 10.0.0.82
```

Um die Adressen zu verwalten IPv6

Verwenden Sie den folgenden Befehl assign-ipv6-addresses, um eine Adresse zuzuweisen. IPv6

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-addresses 2001:db8:1234:1a00:9691:9503:25ad:1761
```

Verwenden Sie den folgenden Befehl unassign-ipv6-addresses, um die Zuweisung einer Adresse aufzuheben. IPv6

```
aws ec2 unassign-ipv6-addresses \
    --network-interface-id eni-1234567890abcdef0 \
    --ipv6-addresses 2001:db8:1234:1a00:9691:9503:25ad:1761
```

Um die Elastic IP-Adresse für die primäre private Adresse zu verwalten IPv4

Verwenden Sie den folgenden Befehl associate-address, um der primären privaten IPv4 Adresse eine Elastic IP-Adresse zuzuordnen.

```
aws ec2 associate-address \
    --allocation-id eipalloc-0b263919b6EXAMPLE \
    --network-interface-id eni-1234567890abcdef0
```

Verwenden Sie den folgenden Befehl disassociate-address, um eine Elastic IP-Adresse von der primären privaten Adresse zu trennen. IPv4

```
aws ec2 disassociate-address --association-id eipassoc-2bebb745a1EXAMPLE
```

PowerShell

Um die Adressen zu verwalten IPv4

Verwenden Sie das Register-EC2PrivateIpAddressCmdlet, um eine IPv4 Adresse zuzuweisen.

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -PrivateIpAddress 10.0.0.82
```

Verwenden Sie das Unregister-EC2PrivateIpAddressCmdlet, um die Zuweisung einer Adresse aufzuheben. IPv4

```
Unregister-EC2PrivateIpAddress `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -PrivateIpAddress 10.0.0.82
```

Um die Adressen zu verwalten IPv6

Verwenden Sie das AddressList Cmdlet Register-EC2Ipv6, um eine IPv6 Adresse zuzuweisen.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6Address 2001:db8:1234:1a00:9691:9503:25ad:1761
```

Verwenden Sie das AddressList Cmdlet Unregister-EC2Ipv6, um die Zuweisung einer Adresse aufzuheben. IPv6

```
Unregister-EC2Ipv6AddressList `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Ipv6Address 2001:db8:1234:1a00:9691:9503:25ad:1761
```

Um die Elastic IP-Adresse für die primäre private Adresse zu verwalten IPv4

Verwenden Sie das Register-EC2AddressCmdlet, um der primären privaten IPv4 Adresse eine Elastic IP-Adresse zuzuordnen.

```
Register-EC2Address `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -AllocationId eipalloc-0b263919b6EXAMPLE
```

Verwenden Sie das Unregister-EC2AddressCmdlet, um eine Elastic IP-Adresse von der primären privaten Adresse zu trennen. IPv4

```
Unregister-EC2Address -AssociationId eipassoc-2bebb745a1EXAMPLE
```

Ändern der Netzwerkschnittstellen-Attribute

Sie können die folgenden Netzwerkschnittstellenattribute ändern:

- Beschreibung
- Sicherheitsgruppen
- Beim Beenden löschen
- Quell-/Zielprüfung
- Timeout für die Nachverfolgung von Leerlaufverbindungen

Überlegungen

Sie können die Attribute einer vom Anforderer verwalteten Netzwerkschnittstelle nicht ändern.

Console

So ändern Sie die Netzwerkschnittstellen-Attribute

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.
4. Um die Beschreibung zu ändern, gehen Sie wie folgt vor.
   a. Wählen Sie Actions (Aktionen), Change description (Beschreibung ändern).
   b. Geben Sie im Feld Description (Beschreibung) eine Beschreibung ein.
   c. Wählen Sie Speichern.
5. Um die Sicherheitsgruppen zu ändern, gehen Sie wie folgt vor:
   a. Wählen Sie Actions (Aktionen), Change security groups (Ändern von Sicherheitsgruppen).

b. Fügen Sie unter Zugeordnete Sicherheitsgruppen nach Bedarf Sicherheitsgruppen hinzu oder entfernen Sie sie. Die Sicherheitsgruppe und die Netzwerkschnittstelle müssen für dieselbe VPC erstellt werden.

c. Wählen Sie Speichern.

6. Um das Beendigungsverhalten zu ändern, gehen Sie wie folgt vor:

a. Wählen Sie Aktionen, Beendigungsverhalten ändern .

b. Wählen oder deaktivieren Sie die Option Bei Beendigung löschen, Aktivieren.

c. Wählen Sie Speichern.

7. Gehen Sie wie folgt vor, um die source/destination Überprüfung zu ändern:

a. Wählen Sie Actions (Aktionen), Change source/dest check (Ändern Quell-/Zielprüfung).

b. Aktivieren oder deaktivieren Sie die Quell-/Zielüberprüfung, Aktivieren.

c. Wählen Sie Speichern.

8. Um die Timeouts für die Nachverfolgung von Verbindungen im Leerlauf zu ändern, gehen Sie wie folgt vor:

a. Wählen Sie Aktionen, Timeout für die Nachverfolgung von Verbindungen im Leerlauf ändern.

b. Ändern Sie die Timeout-Werte nach Bedarf. Weitere Informationen finden Sie unter Timeout für die Nachverfolgung von Leerlaufverbindungen.

- Timeout für bestehende TCP-Verbindungen: Timeout (in Sekunden) für bestehende TCP-Verbindungen im Leerlauf.
  - Min: `60` Sekunden
  - Max: `432000` Sekunden
  - Standard: `350` Sekunden für Nitrov6-Instance-Typen, ausgenommen P6e- 00. GB2 Und `432000` Sekunden für andere Instance-Typen, einschließlich P6e-00. GB2
  - Empfohlen: Weniger als `432000` Sekunden.
- UDP-Timeout: Timeout (in Sekunden) für UDP-Datenflüsse im Leerlauf, bei denen Datenverkehr nur in eine Richtung oder nur in einer einzelnen Anforderung-Antwort-Transaktion übermittelt wurde.
  - Min: `30` Sekunden
  - Max: `60` Sekunden

- Standardwert: 30 Sekunden
- UDP-Stream-Timeout: Timeout (in Sekunden) für UDP-Datenflüsse im Leerlauf, die als Streams klassifiziert sind, bei denen mehr als eine Anforderung-Antwort-Transaktion stattgefunden hat.
  - Min: 60 Sekunden
  - Max: 180 Sekunden
  - Standardwert: 180 Sekunden

c. Wählen Sie Speichern.

AWS CLI

Example Beispiel: So ändern Sie die Beschreibung

Verwenden Sie den folgenden modify-network-interface-attribute-Befehl.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --description "my updated description"
```

Example Beispiel: So ändern Sie die Sicherheitsgruppen

Verwenden Sie den folgenden modify-network-interface-attribute-Befehl.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --groups sg-1234567890abcdef0
```

Example Beispiel: So ändern Sie das Beendigungsverhalten

Verwenden Sie den folgenden modify-network-interface-attribute-Befehl.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --attachment AttachmentId=eni-attach-43348162abEXAMPLE,DeleteOnTermination=false
```

Example Beispiel: Um die Überprüfung zu aktivieren source/destination

Verwenden Sie den folgenden modify-network-interface-attribute-Befehl.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --source-dest-check
```

Example Beispiel: So ändern Sie das Timout für die Nachverfolgung von Verbindungen im Leerlauf

Verwenden Sie den folgenden modify-network-interface-attribute-Befehl. Weitere Informationen finden Sie unter Timeout für die Nachverfolgung von Leerlaufverbindungen.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --connection-tracking-specification
 TcpEstablishedTimeout=172800,UdpStreamTimeout=90,UdpTimeout=60
```

PowerShell

Example Beispiel: So ändern Sie die Beschreibung

Verwenden Sie das cmdlet Edit-EC2NetworkInterfaceAttribute.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Description "my updated description"
```

Example Beispiel: So ändern Sie die Sicherheitsgruppen

Verwenden Sie das cmdlet Edit-EC2NetworkInterfaceAttribute.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -Group sg-1234567890abcdef0
```

Example Beispiel: So ändern Sie das Beendigungsverhalten

Verwenden Sie das cmdlet Edit-EC2NetworkInterfaceAttribute.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
```

```
    -Attachment_AttachmentId eni-attach-43348162abEXAMPLE `
    -Attachment_DeleteOnTermination $false
```

Example Beispiel: Um die source/destination Überprüfung zu aktivieren

Verwenden Sie das cmdlet Edit-EC2NetworkInterfaceAttribute.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -SourceDestCheck $true
```

Example Beispiel: So ändern Sie die Timeouts für die Nachverfolgung von Verbindungen im Leerlauf.

Verwenden Sie das cmdlet Edit-EC2NetworkInterfaceAttribute. Weitere Informationen finden Sie unter Timeout für die Nachverfolgung von Leerlaufverbindungen.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -ConnectionTrackingSpecification_TcpEstablishedTimeout 172800 `
    -ConnectionTrackingSpecification_UdpStreamTimeout 90 `
    -ConnectionTrackingSpecification_UdpTimeout 60
```

Mehrere Netzwerkschnittstellen für Ihre EC2 Amazon-Instances

In den folgenden Fällen ist das Anfügen von mehreren Netzwerkschnittstellen an eine Instance sinnvoll:

- Netzwerkmanagement.
- Netzwerk- und Sicherheits-Appliances.
- Dual-Homed-Instances mit Workloads in verschiedenen Subnetzen oder. VPCs
- Kostengünstigen Hochverfügbarkeitslösungen.

Netzwerkmanagement

In der folgenden Übersicht wird ein Verwaltungsnetzwerk beschrieben, das mit mehreren Netzwerkschnittstellen erstellt wurde.

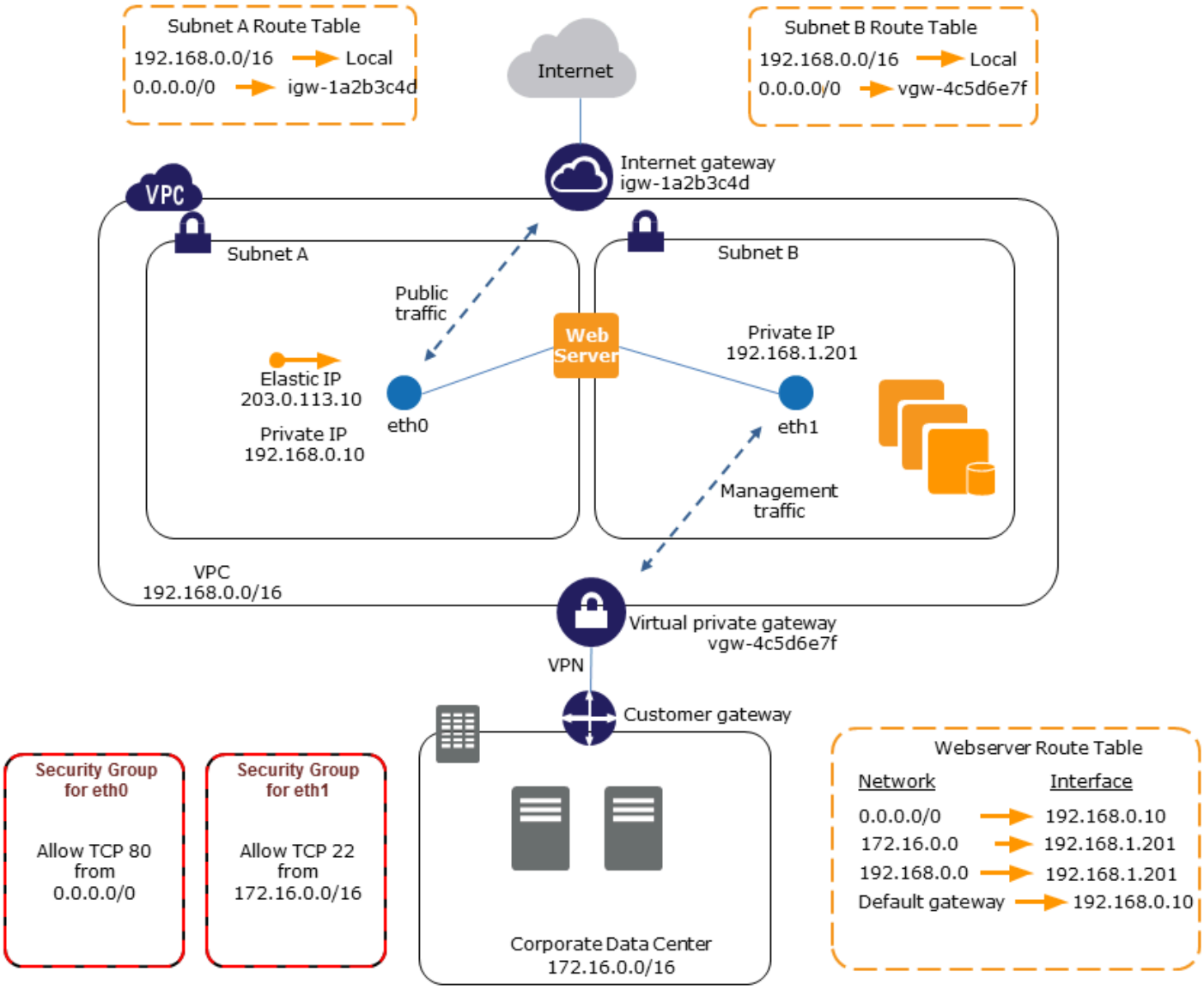
Kriterien

- Die primäre Netzwerkschnittstelle (zum Beispiel eth0) der Instance verarbeitet den öffentlichen Datenverkehr.
- Die sekundäre Netzwerkschnittstelle der Instance (zum Beispiel eth1) verarbeitet den Backend-Verwaltungsverkehr. Sie ist mit einem separaten Subnetz verbunden, das über restriktivere Zugriffskontrollen verfügt und sich in derselben Availability Zone befindet wie die primäre Netzwerkschnittstelle.

Einstellungen

- Die primäre Netzwerkschnittstelle, welche sich möglicherweise hinter einem Load Balancer befindet, verfügt über eine zugeordnete Sicherheitsgruppe, welche den Zugriff auf den Server über das Internet ermöglicht. Erlauben Sie beispielsweise die TCP-Ports 80 und 443 vom 0.0.0.0/0 oder vom Load Balancer.
- Der sekundären Netzwerkschnittstelle ist einer Sicherheitsgruppe zugeordnet, die nur SSH-Zugriff ermöglicht, der von einem der folgenden Standorte aus initiiert wird:
  - Ein zulässiger Bereich von IP-Adressen, entweder innerhalb der VPC oder aus dem Internet.
  - Ein privates Subnetz innerhalb derselben Availability Zone wie die primäre Netzwerkschnittstelle.
  - Ein Virtual Private Gateway.

> **Note**
>
> Um Failover-Fähigkeiten sicherzustellen, sollten Sie erwägen, IPv4 für eingehenden Datenverkehr auf einer Netzwerkschnittstelle ein sekundäres privates System zu verwenden. Falls eine Instanz ausfällt, können Sie die and/or sekundäre private IPv4 Adresse der Schnittstelle in eine Standby-Instance verschieben.



Netzwerk- und Sicherheitsanwendungen

Für einige Netzwerk- und Sicherheitsanwendungen (z. B. Load Balancer, Network Address Translation (NAT)-Server und Proxy-Server) wird die Konfiguration mit mehreren Netzwerkschnittstellen bevorzugt. Sie können sekundäre Netzwerkschnittstellen erstellen und an Instances anfügen, die diese Arten von Anwendungen ausführen und zusätzliche Schnittstellen mit ihren eigenen öffentlichen und privaten IP-Adressen, Sicherheitsgruppen und Quell-/Zielprüfung konfigurieren.

Dual-homed-Instances mit Workloads in verschiedenen Subnetzen

Sie können eine Netzwerkschnittstelle auf jedem Ihrer Webserver einrichten, der mit einem Netzwerk der mittleren Schicht verbunden ist, in dem sich ein Anwendungsserver befindet. Der Anwendungsserver kann auch doppelt mit einem Backend-Netzwerk (Subnetz), in dem sich der Datenbankserver befindet, vernetzt sein. Statt Netzwerkpakete durch die doppelt vernetzten Instances weiterzuleiten, empfängt und verarbeitet jede doppelt vernetzte Instance Anfragen vom Frontend, stellt eine Verbindung zum Backend her und sendet die Anfragen dann an die Server im Backend-Netzwerk.

Dual-Homed-Instances mit unterschiedlichen Workloads VPCs im selben Konto

Sie können eine EC2 Instance in einer VPC starten und eine sekundäre ENI von einer anderen VPC aus anhängen, sofern sich die Netzwerkschnittstelle in derselben Availability Zone wie die Instance befindet. Auf diese Weise können Sie mehrfach vernetzte Instances VPCs mit unterschiedlichen Netzwerk- und Sicherheitskonfigurationen erstellen. Sie können keine mehrfach vernetzten Instanzen in verschiedenen VPCs Konten erstellen. AWS

In den folgenden Anwendungsfällen können Sie doppelt vernetzte VPCs Instanzen verwenden:

- Überwindung von CIDR-Überschneidungen zwischen zwei VPCs , die nicht miteinander verbunden werden können: Sie können ein sekundäres CIDR in einer VPC nutzen und es einer Instance ermöglichen, über zwei nicht überlappende IP-Bereiche zu kommunizieren.
- Connect mehrere VPCs innerhalb eines einzigen Kontos: Ermöglicht die Kommunikation zwischen einzelnen Ressourcen, die normalerweise durch VPC-Grenzen getrennt wären.

Niedrige Budgetlösung mit hoher Verfügbarkeit

Wenn eine Ihrer Instances, die eine bestimmte Funktion erfüllt, ausfällt, besteht folgende Möglichkeit: Die zugehörige Netzwerkschnittstelle kann an eine Ersatz-Instance oder eine Hot Standby-Instance, die für die gleiche Funktion vorkonfiguriert wurde, angefügt werden, um den Service schnell wiederherzustellen. Sie können eine Netzwerkschnittstelle beispielsweise als primäre oder sekundäre Netzwerkschnittstelle für einen kritischen Service wie eine Datenbank- oder NAT-Instance verwenden. Wenn für die Instance ein Fehler auftritt (bzw. für den Code, der für Sie ausgeführt wird), können Sie die Netzwerkschnittstelle an eine Hot Standby-Instance anfügen. Da die Schnittstelle ihre privaten IP-Adressen, Elastic IP-Adressen und MAC-Adressen beibehält, fließt der Netzwerkdatenverkehr zur Standby-Instance, sobald Sie die Netzwerkschnittstelle an die Ersatz-Instance angefügt haben. Zwischen dem Ausfall der Instance und dem Anfügen der

Netzwerkschnittstelle an die Standby-Instance fällt die Verbindung für Benutzer kurzzeitig aus. Es sind jedoch keine Änderungen an der Routing-Tabelle oder an Ihrem DNS-Server erforderlich.

Vom Anforderer verwaltete Netzwerkschnittstellen

Eine vom Anforderer verwaltete Netzwerkschnittstelle ist eine Netzwerkschnittstelle, die ein AWS-Service in Ihrer VPC für Sie erstellt. Die Netzwerkschnittstelle ist mit einer Ressource für einen anderen Dienst verknüpft, z. B. einer DB-Instance von Amazon RDS, einem NAT-Gateway oder einem Schnittstellen-VPC-Endpunkt von AWS PrivateLink.

Überlegungen

- Sie können die vom Anforderer verwalteten Netzwerkschnittstellen in Ihrem Konto anzeigen. Sie können Tags hinzufügen oder entfernen, aber Sie können andere Eigenschaften einer vom Anforderer verwalteten Netzwerkschnittstelle nicht ändern.
- Sie können eine vom Anforderer verwaltete Netzwerkschnittstelle nicht trennen.
- Wenn Sie die Ressource löschen, die einer vom Anforderer verwalteten Netzwerkschnittstelle zugeordnet ist, wird AWS-Service die Netzwerkschnittstelle getrennt und gelöscht. Wenn der Service eine Netzwerkschnittstelle getrennt hat, sie jedoch nicht gelöscht hat, können Sie die getrennte Netzwerkschnittstelle löschen.

Console

So können Sie die vom Anforderer verwaltete Netzwerkschnittstellen anzeigen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich unter Network & Security (Netzwerk und Sicherheit) auf Network Interfaces (Netzwerkschnittstellen).
3. Wählen Sie die ID der Netzwerkschnittstelle aus, um die Detailseite zu öffnen.
4. Im Folgenden finden Sie die Schlüsselfelder, mit denen Sie den Zweck der Netzwerkschnittstelle ermitteln können:
   - Beschreibung: Eine Beschreibung vom AWS -Dienst, der die Schnittstelle erstellt hat. Zum Beispiel: „VPC Endpoint Interface vpce 089f2123488812123“.
   - Vom Antragsteller verwaltet: Gibt an, ob die Netzwerkschnittstelle von verwaltet wird. AWS

- Anforderer-ID: Der Alias oder die AWS Konto-ID des Prinzipals oder Dienstes, der die Netzwerkschnittstelle erstellt hat. Wenn Sie die Netzwerkschnittstelle erstellt haben, ist dies Ihre AWS-Konto ID. Andernfalls hat ein anderer Prinzipal oder Dienst sie erstellt.

AWS CLI

So können Sie die vom Anforderer verwaltete Netzwerkschnittstellen anzeigen

Verwenden Sie den describe-network-interfaces-Befehl wie folgt:

```
aws ec2 describe-network-interfaces \
    --filters "Name=requester-managed,Values=true" \
    --query "NetworkInterfaces[*].[Description, InterfaceType]" \
    --output table
```

Im Folgenden finden Sie eine Beispielausgabe, die die Schlüsselfelder anzeigt, mit denen Sie den Zweck der Netzwerkschnittstelle ermitteln können: `Description` und `InterfaceType`.

```
-------------------------------------------------------------------------
|                        DescribeNetworkInterfaces                      |
+-----------------------------------------------+-----------------------+
|  VPC Endpoint Interface: vpce-0f00567fa8477a1e6  |  interface         |
|  VPC Endpoint Interface vpce-0d8ddce4be80e4474   |  interface         |
|  VPC Endpoint Interface vpce-078221a1e27d1ea5b   |  vpc_endpoint      |
|  Resource Gateway Interface rgw-0bba03f3d56060135 |  interface        |
|  VPC Endpoint Interface: vpce-0cc199f605eaeace7  |  interface         |
|  VPC Endpoint Interface vpce-019b90d6f16d4f958   |  interface         |
+-----------------------------------------------+-----------------------+
```

PowerShell

So können Sie die vom Anforderer verwaltete Netzwerkschnittstellen anzeigen

Verwenden Sie das cmdlet Get-EC2NetworkInterface wie folgt.

```
Get-EC2NetworkInterface -Filter @{Name="requester-managed"; Values="true"} | Select
 Description, InterfaceType
```

Im Folgenden finden Sie eine Beispielausgabe, die die Schlüsselfelder anzeigt, mit denen Sie den Zweck einer Netzwerkschnittstelle ermitteln können: `Description` und `InterfaceType`.

```
Description                                        InterfaceType
-----------                                        -------------
VPC Endpoint Interface: vpce-0f00567fa8477a1e6   interface
VPC Endpoint Interface vpce-0d8ddce4be80e4474    interface
VPC Endpoint Interface vpce-078221a1e27d1ea5b    vpc_endpoint
Resource Gateway Interface rgw-0bba03f3d56060135 interface
VPC Endpoint Interface: vpce-0cc199f605eaeace7   interface
VPC Endpoint Interface vpce-019b90d6f16d4f958    interface
```

Präfix-Delegierung von Amazon-EC2-Netzwerkschnittstellen

Sie können Ihren Netzwerkschnittstellen einen privaten IPv4- oder IPv6-CIDR-Bereich entweder automatisch oder manuell zuweisen. Durch das Zuweisen von Präfixen können Sie die Verwaltung von Anwendungen skalieren und vereinfachen, einschließlich Container- und Netzwerkanwendungen, für die mehrere IP-Adressen in einer Instance erforderlich sind. Weitere Informationen über IPv4- und IPv6-Adressen finden Sie unter IP-Adressierung von Amazon EC2-Instances.

Die folgenden Zuweisungs-Optionen sind verfügbar:

- Automatische Zuweisung – AWS wählt das Präfix aus und weist es Ihrer Netzwerkschnittstelle zu. Wenn das Subnetz für die Netzwerkschnittstelle eine Subnetz-CIDR-Reservierung vom Typ `prefix` hat, wählen wir die Präfixe aus der Subnetz-CIDR-Reservierung aus. Andernfalls wählen wir sie aus dem CIDR-Subnetzbereich aus.
- Manuelle Zuweisung – Sie geben das Präfix an und AWS überprüft, ob das Präfix noch nicht anderen Ressourcen zugewiesen ist, bevor es Ihrer Netzwerkschnittstelle zugewiesen wird.

Die Zuweisung von Präfixen hat folgende Vorteile:

- Erhöhte IP-Adressen auf einer Netzwerkschnittstelle – Wenn Sie ein Präfix verwenden, weisen Sie im Gegensatz zu einzelnen IP-Adressen einen Block von IP-Adressen zu. Dadurch wird die Anzahl der IP-Adressen für eine Netzwerkschnittstelle erhöht.
- Vereinfachte VPC Verwaltung für Container – In Containeranwendungen benötigt jeder Container eine eindeutige IP-Adresse. Das Zuweisen von Präfixen zu Ihrer Instance vereinfacht die Verwaltung Ihrer VPCs, da Sie Container starten und beenden können, ohne Amazon EC2 APIs für individuelle IP-Zuweisungen aufrufen zu müssen.

Inhalt

- Grundlagen
- Überlegungen
- Präfixe für Ihre Netzwerkschnittstellen verwalten
  - Präfixe während der Erstellung der Netzwerkschnittstelle zuweisen
  - Präfixe einer vorhandenen Netzwerkschnittstelle zuweisen
  - Entfernen Sie Präfixe von Ihren Netzwerkschnittstellen

Grundlagen

- Sie können neuen oder vorhandenen Netzwerkschnittstellen ein Präfix zuweisen.
- Wenn Sie Präfixe verwenden möchten, weisen Sie Ihrer Netzwerkschnittstelle ein Präfix zu, fügen die Netzwerkschnittstelle Ihrer Instance an und konfigurieren dann das Betriebssystem.
- Wenn Sie die Option zum Angeben eines Präfix auswählen, muss das Präfix folgende Anforderungen erfüllen:
  - Das IPv4-Präfix, das Sie angeben können, ist `/28`.
  - Das IPv6-Präfix, das Sie angeben können, ist `/80`.
  - Das Präfix befindet sich im Subnetz-CIDR der Netzwerkschnittstelle und überschneidet sich nicht mit anderen Präfixen oder IP-Adressen, die vorhandenen Ressourcen im Subnetz zugewiesen sind.
- Sie können der primären oder sekundären Netzwerkschnittstelle ein Präfix zuweisen.
- Sie können einer Netzwerkschnittstelle eine Elastic IP-Adresse zuweisen, deren ein Präfix zugewiesen ist.
- Sie können dem IP-Adressteil des zugewiesenen Präfix auch eine Elastic-IP-Adresse zuweisen.
- Wir lösen den privaten DNS-Hostname einer Instance zur privaten IPv4-Adresse auf.
- Wir weisen jede private IPv4-Adresse für eine Netzwerkschnittstelle, einschließlich der von Präfixen, mit den folgenden Formaten zu:
  - `us-east-1`-Region

    ```
    ip-private-ipv4-address.ec2.internal
    ```

  - Alle anderen Regionen

    ```
    ip-private-ipv4-address.region.compute.internal
    ```

Überlegungen

Berücksichtigen Sie Folgendes, wenn Sie Präfixe verwenden:

- Netzwerkschnittstellen mit Präfixen werden mit Nitro-basierten Instances unterstützt.
- Präfixe für Netzwerkschnittstellen müssen IPv6- oder private IPv4-Adressen verwenden.
- Die maximale Anzahl der IP-Adressen, die Sie einer Netzwerkschnittstelle zuweisen können, hängt vom Instance-Typ ab. Jedes Präfix, das Sie einer Netzwerkschnittstelle zuweisen, zählt als eine IP-Adresse. Zum Beispiel hat eine `c5.large`-Instance ein Limit von `10` IPv4-Adressen pro Netzwerkschnittstelle. Jede Netzwerkschnittstelle für diese Instance hat eine primäre IPv4-Adresse. Wenn eine Netzwerkschnittstelle keine sekundären IPv4-Adressen hat, können Sie der Netzwerkschnittstelle bis zu 9 Präfixe zuweisen. Für jede weitere IPv4-Adresse, die Sie einer Netzwerkschnittstelle zuweisen, können Sie der Netzwerkschnittstelle ein Präfix weniger zuweisen. Weitere Informationen finden Sie unter Maximale IP-Adressen pro Netzwerkschnittstelle.
- Präfixe sind bei Quell-/Zielprüfungen enthalten.
- Sie müssen Ihr Betriebssystem so konfigurieren, dass es mit Netzwerkschnittstellen mit Präfixen arbeitet. Beachten Sie Folgendes:
  - Einige Amazon-Linux-AMIs enthalten zusätzliche von AWS installierte Skripts, bekannt als `ec2-net-utils`. Mit diesen Skripts kann die Konfiguration Ihrer Netzwerkschnittstellen optional automatisiert werden. Diese Skripts stehen nur für Amazon Linux zur Verfügung.
  - Für Container können Sie ein Container Network Interface (CNI) für das Kubernetes-Plug-in verwenden oder `dockerd`, wenn Sie Docker verwenden, um Ihre Container zu verwalten.

Präfixe für Ihre Netzwerkschnittstellen verwalten

Wenn Sie einer Netzwerkschnittstelle Präfixe zuweisen, können Sie wählen, ob wir die Präfixe automatisch zuweisen sollen oder ob Sie benutzerdefinierte Präfixe angeben möchten. Wenn Sie uns erlauben, automatisch Präfixe zuzuweisen, und das Subnetz für die Netzwerkschnittstelle eine Subnetz-CIDR-Reservierung vom Typ `prefix` hat, wählen wir die Präfixe aus der Subnetz-CIDR-Reservierung aus. Andernfalls wählen wir sie aus dem CIDR-Subnetzbereich aus.

Aufgaben

- Präfixe während der Erstellung der Netzwerkschnittstelle zuweisen
- Präfixe einer vorhandenen Netzwerkschnittstelle zuweisen
- Entfernen Sie Präfixe von Ihren Netzwerkschnittstellen

Präfixe während der Erstellung der Netzwerkschnittstelle zuweisen

Sie können automatische oder benutzerdefinierte Präfixe zuweisen, wenn Sie eine Netzwerkschnittstelle erstellen.

Console

So weisen Sie automatische Präfixe während der Erstellung der Netzwerkschnittstelle zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Klicken Sie auf Create network interface (Netzwerkschnittstellen erstellen).
4. Geben Sie eine Beschreibung für die Netzwerkschnittstelle an, wählen Sie das Subnetz aus, in dem die Netzwerkschnittstelle erstellt werden soll, und konfigurieren Sie die privaten IPv4- und IPv6-Adressen.
5. Erweiterten Sie Advanced settings (Erweiterte Einstellungen).
6. Führen Sie für die IPv4-Präfixdelegierung einen der folgenden Schritte aus:
   - Um ein IPv4-Präfix automatisch zuzuweisen, wählen Sie Automatische Zuweisung. Geben Sie für die Anzahl der IPv4-Präfixe die Anzahl der zuzuweisenden Präfixe an.
   - Um ein bestimmtes IPv4-Präfix zuzuweisen, wählen Sie Benutzerdefiniert aus. Wählen Sie dann Hinzufügen eines Präfix und geben Sie das Präfix ein.
7. Für die IPv6-Präfix-Delegation führen Sie einen der folgenden Schritte aus:
   - Um automatisch ein IPv6-Präfix zuzuweisen, wählen Sie Automatische Zuweisung aus. Geben Sie für die Anzahl der IPv6-Präfixe die Anzahl der zuzuweisenden Präfixe an.
   - Um ein bestimmtes IPv6-Präfix zuzuweisen, wählen Sie Benutzerdefiniert aus. Wählen Sie dann Hinzufügen eines Präfix und geben Sie das Präfix ein.

   > **Note**
   >
   > IPv6-Präfixdelegierung wird nur angezeigt, wenn das ausgewählte Subnetz für IPv6 aktiviert ist.

8. Wählen Sie die Sicherheitsgruppen aus, die der Netzwerkschnittstelle zugeordnet werden sollen, und weisen Sie ggf. Ressourcen-Tags zu.
9. Klicken Sie auf Create network interface (Netzwerkschnittstellen erstellen).

AWS CLI

So weisen Sie während der Erstellung der Netzwerkschnittstelle automatische IPv4-Präfixe zu

Verwenden Sie den Befehl create-network-interface und setzen Sie `--ipv4-prefix-count` auf die Anzahl der IPv4-Präfixe, die AWS zuweisen soll. Im folgenden Beispiel weist AWS ein IPv4-Präfix zu.

```
aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv4 automatic example" \
    --ipv4-prefix-count 1
```

So weisen Sie während der Erstellung der Netzwerkschnittstelle bestimmte IPv4-Präfixe zu

Verwenden Sie den Befehl create-network-interface und setzen Sie `--ipv4-prefixes` auf die Präfixe. AWS wählt IPv4-Adressen aus diesem Bereich aus. Im folgenden Beispiel lautet das Präfix-CIDR 10.0.0.208/28.

```
aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv4 manual example" \
    --ipv4-prefixes Ipv4Prefix=10.0.0.208/28
```

So weisen Sie während der Erstellung der Netzwerkschnittstelle automatische IPv6-Präfixe zu

Verwenden Sie den Befehl create-network-interface und setzen Sie `--ipv6-prefix-count` auf die Anzahl der IPv6-Präfixe, die AWS zuweisen soll. Im folgenden Beispiel weist AWS ein IPv6-Präfix zu.

```
aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv6 automatic example" \
    --ipv6-prefix-count 1
```

So weisen Sie während der Erstellung der Netzwerkschnittstelle bestimmte IPv6-Präfixe zu

Verwenden Sie den Befehl create-network-interface und setzen Sie `--ipv6-prefixes` auf die Präfixe. AWS wählt IPv6-Adressen aus diesem Bereich aus. Im folgenden Beispiel lautet das Präfix-CIDR 2600:1f13:fc2:a700:1768::/80.

```
aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv6 manual example" \
    --ipv6-prefixes Ipv6Prefix=2600:1f13:fc2:a700:1768::/80
```

PowerShell

So weisen Sie während der Erstellung der Netzwerkschnittstelle automatische IPv4-Präfixe zu

Verwenden Sie das cmdlet New-EC2NetworkInterface und setzen Sie `Ipv4PrefixCount` auf die Anzahl der IPv4-Präfixen fest, die AWS zuweisen soll. Im folgenden Beispiel weist AWS ein IPv4-Präfix zu.

```
New-EC2NetworkInterface `
    -SubnetId 'subnet-047cfed18eEXAMPLE' `
    -Description 'IPv4 automatic example' `
    -Ipv4PrefixCount 1
```

So weisen Sie während der Erstellung der Netzwerkschnittstelle bestimmte IPv4-Präfixe zu

Verwenden Sie das cmdlet NEW-EC2NetworkInterface und setzen Sie `Ipv4Prefix` auf die Präfixe. AWS wählt IPv4-Adressen aus diesem Bereich aus. Im folgenden Beispiel lautet das Präfix-CIDR 10.0.0.208/28.

```
Import-Module AWS.Tools.EC2
New-EC2NetworkInterface `
    -SubnetId 'subnet-047cfed18eEXAMPLE' `
    -Description 'IPv4 manual example' `
    -Ipv4Prefix (New-Object `
        -TypeName Amazon.EC2.Model.Ipv4PrefixSpecificationRequest `
        -Property @{Ipv4Prefix = '10.0.0.208/28'})
```

So weisen Sie während der Erstellung der Netzwerkschnittstelle automatische IPv6-Präfixe zu

Verwenden Sie das cmdlet New-EC2NetworkInterface und setzen Sie `Ipv6PrefixCount` auf die Anzahl der IPv6-Präfixen fest, die AWS zuweisen soll. Im folgenden Beispiel weist AWS ein IPv6-Präfix zu.

```
New-EC2NetworkInterface `
    -SubnetId 'subnet-047cfed18eEXAMPLE' `
```

```
    -Description 'IPv6 automatic example' `
    -Ipv6PrefixCount 1
```

So weisen Sie während der Erstellung der Netzwerkschnittstelle bestimmte IPv6-Präfixe zu

Verwenden Sie das cmdlet New-EC2NetworkInterface und setzen Sie `Ipv6Prefixes` auf die Präfixe. AWS wählt IPv6-Adressen aus diesem Bereich aus. Im folgenden Beispiel lautet das Präfix-CIDR 2600:1f13:fc2:a700:1768::/80.

```
Import-Module AWS.Tools.EC2
New-EC2NetworkInterface `
    -SubnetId 'subnet-047cfed18eEXAMPLE' `
    -Description 'IPv6 manual example' `
    -Ipv6Prefix (New-Object `
        -TypeName Amazon.EC2.Model.Ipv6PrefixSpecificationRequest `
        -Property @{Ipv6Prefix = '2600:1f13:fc2:a700:1768::/80'})
```

Präfixe einer vorhandenen Netzwerkschnittstelle zuweisen

Sie können einer vorhandenen Netzwerkschnittstelle automatische oder benutzerdefinierte Präfixe zuweisen.

Console

So weisen Sie einer vorhandenen Netzwerkschnittstelle automatische Präfixe zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces (Netzwerkschnittstellen) aus.
3. Wählen Sie die Netzwerkschnittstelle aus, der Sie die Präfixe zuweisen möchten, und wählen Sie Aktionen, Präfixe verwaltenaus.
4. Führen Sie für die IPv4-Präfixdelegierung einen der folgenden Schritte aus:
   - Um ein IPv4-Präfix automatisch zuzuweisen, wählen Sie Automatische Zuweisung. Geben Sie für die Anzahl der IPv4-Präfixe die Anzahl der zuzuweisenden Präfixe an.
   - Um ein bestimmtes IPv4-Präfix zuzuweisen, wählen Sie Benutzerdefiniert aus. Wählen Sie dann Hinzufügen eines Präfix und geben Sie das Präfix ein.
5. Für die IPv6-Präfix-Delegation führen Sie einen der folgenden Schritte aus:
   - Um automatisch ein IPv6-Präfix zuzuweisen, wählen Sie Automatische Zuweisung aus. Geben Sie für die Anzahl der IPv6-Präfixe die Anzahl der zuzuweisenden Präfixe an.

- Um ein bestimmtes IPv6-Präfix zuzuweisen, wählen Sie Benutzerdefiniert aus. Wählen Sie dann Hinzufügen eines Präfix und geben Sie das Präfix ein.

> **Note**
>
> IPv6-Präfixdelegierung wird nur angezeigt, wenn das ausgewählte Subnetz für IPv6 aktiviert ist.

6. Wählen Sie Speichern.

AWS CLI

Verwenden Sie den Befehl assign-ipv6-addresses nutzen, um IPv6-Präfixe zuzuweisen, und den Befehl assign-private-ip-addresses, um vorhandenen Netzwerkschnittstellen IPv4-Präfixe zuzuweisen.

So weisen Sie einer vorhandenen Netzwerkschnittstelle automatische IPv4-Präfixe zu

Verwenden Sie den Befehl assign-private-ip-addresses und setzen Sie `--ipv4-prefix-count` auf die Anzahl der IPv4-Präfixe, die AWS zuweisen soll. Im folgenden Beispiel weist AWS ein IPv4-Präfix zu.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-id eni-081fbb4095EXAMPLE \
    --ipv4-prefix-count 1
```

Bestimmte IPv4-Präfixe zu einer vorhandenen Netzwerkschnittstelle zuweisen

Verwenden Sie den Befehl assign-private-ip-addresses und stellen Sie `--ipv4-prefixes` auf das Präfix. AWS wählt IPv4-Adressen aus diesem Bereich aus. Im folgenden Beispiel lautet das Präfix-CIDR 10.0.0.208/28.

```
aws ec2 assign-private-ip-addresses \
    --network-interface-id eni-081fbb4095EXAMPLE \
    --ipv4-prefixes 10.0.0.208/28
```

So weisen Sie einer vorhandenen Netzwerkschnittstelle automatische IPv6-Präfixe zu

Verwenden Sie den Befehl assign-ipv6-addresses und setzen Sie `--ipv6-prefix-count` auf die Anzahl der IPv6-Präfixe, die AWS zuweisen soll. Im folgenden Beispiel weist AWS ein IPv6-Präfix zu.

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-00d577338cEXAMPLE \
    --ipv6-prefix-count 1
```

Bestimmte IPv6-Präfixe zu einer vorhandenen Netzwerkschnittstelle zuweisen

Verwenden Sie den Befehl assign-ipv6-addresses und stellen Sie `--ipv6-prefixes` auf das Präfix. AWS wählt IPv6-Adressen aus diesem Bereich aus. Im folgenden Beispiel lautet das Präfix-CIDR 2600:1f13:fc2:a700:18bb::/80.

```
aws ec2 assign-ipv6-addresses \
    --network-interface-id eni-00d577338cEXAMPLE \
    --ipv6-prefixes 2600:1f13:fc2:a700:18bb::/80
```

PowerShell

So weisen Sie einer vorhandenen Netzwerkschnittstelle automatische IPv4-Präfixe zu

Verwenden Sie das cmdlet Register-EC2PrivateIpAddress und setzen Sie `Ipv4PrefixCount` auf die Anzahl der IPv4-Präfixe, die AWS zuweisen soll. Im folgenden Beispiel weist AWS ein IPv4-Präfix zu.

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv4PrefixCount 1
```

Bestimmte IPv4-Präfixe zu einer vorhandenen Netzwerkschnittstelle zuweisen

Verwenden Sie das cmdlet Register-EC2PrivateIpAddress und setzen Sie `Ipv4Prefix` auf das Präfix. AWS wählt IPv4-Adressen aus diesem Bereich aus. Im folgenden Beispiel lautet das Präfix-CIDR 10.0.0.208/28.

```
Register-EC2PrivateIpAddress `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv4Prefix '10.0.0.208/28'
```

So weisen Sie einer vorhandenen Netzwerkschnittstelle automatische IPv6-Präfixe zu

Verwenden Sie das cmdlet Register-EC2Ipv6AddressList und setzen Sie `Ipv6PrefixCount` auf die Anzahl der IPv4-Präfixe, die AWS zuweisen soll. Im folgenden Beispiel weist AWS ein IPv6-Präfix zu.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv6PrefixCount 1
```

Bestimmte IPv6-Präfixe zu einer vorhandenen Netzwerkschnittstelle zuweisen

Verwenden Sie das cmdlet Register-EC2Ipv6AddressList und setzen Sie `Ipv6Prefix` auf das Präfix. AWS wählt IPv6-Adressen aus diesem Bereich aus. Im folgenden Beispiel lautet das Präfix-CIDR 2600:1f13:fc2:a700:18bb::/80.

```
Register-EC2Ipv6AddressList `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv6Prefix '2600:1f13:fc2:a700:18bb::/80'
```

Entfernen Sie Präfixe von Ihren Netzwerkschnittstellen

Sie können Präfixe von einer vorhandenen Netzwerkschnittstelle entfernen.

Console

So entfernen Sie die Präfixe einer Netzwerkschnittstelle

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Wählen Sie die Netzwerkschnittstelle aus.
4. Wählen Sie Aktionen, Präfixe verwalten.
5. Um bei der IPv4-Präfix-Delegierung bestimmte Präfixe zu entfernen, wählen Sie neben den zu entfernenden Präfixen die Option Zuweisung aufheben aus. Um alle Präfixe zu entfernen, wählen Sie Nicht zuweisen aus.
6. Um bei der IPv6-Präfix-Delegierung bestimmte Präfixe zu entfernen, wählen Sie neben den zu entfernenden Präfixen die Option Zuweisung aufheben aus. Um alle Präfixe zu entfernen, wählen Sie Nicht zuweisen aus.

> **Note**
>
> IPv6-Präfixdelegierung wird nur angezeigt, wenn das ausgewählte Subnetz für IPv6 aktiviert ist.

7. Wählen Sie Speichern.

AWS CLI

Sie können den Befehl unassign-ipv6-addresses nutzen, um IPv6-Präfixe zu entfernen und den Befehl unassign-private-ip-addresses, um IPv4-Präfixe aus Ihren vorhandenen Netzwerkschnittstellen zu entfernen.

So entfernen Sie IPv4-Präfixe aus einer Netzwerkschnittstelle

Verwenden Sie den Befehl unassign-private-ip-addresses und setzen Sie `--ipv4-prefix` auf das Präfix-CIDR, das Sie entfernen möchten.

```
aws ec2 unassign-private-ip-addresses \
    --network-interface-id eni-081fbb4095EXAMPLE \
    --ipv4-prefixes 10.0.0.176/28
```

So entfernen Sie IPv6-Präfixe aus einer Netzwerkschnittstelle

Verwenden Sie den Befehl unassign-ipv6-addresses und setzen Sie `--ipv6-prefix` auf das Präfix-CIDR, das Sie entfernen möchten.

```
aws ec2 unassign-ipv6-addresses \
    --network-interface-id eni-00d577338cEXAMPLE \
    --ipv6-prefix 2600:1f13:fc2:a700:18bb::/80
```

PowerShell

So entfernen Sie IPv4-Präfixe aus einer Netzwerkschnittstelle

Verwenden Sie das cmdlet Unregister-EC2PrivateIpAddress und setzen Sie `Ipv4Prefix` auf das Präfix-CIDR fest, das entfernt werden soll.

```
Unregister-EC2PrivateIpAddress `
```

```
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv4Prefix '10.0.0.208/28'
```

So entfernen Sie IPv6-Präfixe aus einer Netzwerkschnittstelle

Verwenden Sie das cmdlet Unregister-EC2Ipv6AddressList und setzen Sie `Ipv6Prefix` auf das Präfix-CIDR fest, das entfernt werden soll.

```
Unregister-EC2Ipv6AddressList `
    -NetworkInterfaceId 'eni-00d577338cEXAMPLE' `
    -Ipv6Prefix '2600:1f13:fc2:a700:18bb::/80'
```

Löschen einer Netzwerkschnittstelle

Durch das Löschen einer Netzwerkschnittstelle werden alle mit der Schnittstelle verknüpften Attribute entfernt und sämtliche privaten IP-Adressen oder Elastic IP-Adressen freigegeben, damit diese von einer anderen Instance verwendet werden können.

Sie können eine verwendete Netzwerkschnittstelle nicht löschen. Zuerst müssen Sie die Netzwerkschnittstelle trennen.

Console

So löschen Sie eine Netzwerkschnittstelle

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle und wählen Sie dann Actions (Aktionen), Delete (Löschen) aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

AWS CLI

So löschen Sie eine Netzwerkschnittstelle

Verwenden Sie den folgenden delete-network-interface-Befehl.

```
aws ec2 delete-network-interface --network-interface-id eni-1234567890abcdef0
```

PowerShell

So löschen Sie eine Netzwerkschnittstelle

Verwenden Sie das cmdlet Remove-EC2NetworkInterface.

```
Remove-EC2NetworkInterface -NetworkInterfaceId eni-1234567890abcdef0
```

Netzwerkbandbreite der EC2 Amazon-Instance

Spezifikationen der Instance-Bandbreite gelten sowohl für eingehenden als auch für ausgehenden Datenverkehr der Instance. Wenn eine Instance beispielsweise eine Bandbreite von bis zu 10 Gbit/s angibt, bedeutet dies, dass sie über eine Bandbreite von bis zu 10 Gbit/s für eingehenden Datenverkehr und gleichzeitig bis zu 10 Gbit/s für ausgehenden Datenverkehr verfügt. Die Netzwerkbandbreite, die einer EC2 Instanz zur Verfügung steht, hängt wie folgt von mehreren Faktoren ab.

Multi-Flow-Datenverkehr

Die Bandbreite für Multi-Flow-Verkehr ist auf 50% der verfügbaren Bandbreite für Datenverkehr begrenzt, der über ein Internet-Gateway oder ein lokales Gateway für Instances mit 32 oder mehr V oder 5 Gbit/s fließtCPUs, je nachdem, welcher Wert größer ist. Für Instances mit weniger als 32 V CPUs ist die Bandbreite auf 5 Gbit/s begrenzt.

Single-Flow-Datenverkehr

Die Basisbandbreite für Datenverkehr mit einem einzelnen Ablauf ist auf 5 Gbit/s begrenzt, wenn sich Instances nicht in der gleichen Cluster-Placement-Gruppe befinden. Um die Latenz zu verringern und die Single-Flow-Bandbreite zu erhöhen, versuchen Sie Folgendes:

- Verwenden Sie eine Cluster-Placement-Gruppe, um eine Bandbreite von bis zu 10 Gbit/s für Instances innerhalb derselben Platzierungsgruppe zu erreichen.
- Richten Sie mehrere Pfade zwischen zwei Endpunkten ein, um mit Multipath TCP (MPTCP) eine höhere Bandbreite zu erreichen.
- Konfigurieren Sie ENA Express für berechtigte Instances innerhalb desselben Subnetzes, um bis zu 25 Gbit/s zwischen diesen Instances zu erreichen.

> **Note**
>
> Ein einzelner Ablauf wird als eindeutiger 5-Tupel-TCP- oder UDP-Ablauf betrachtet. Bei anderen Protokollen, die dem IP-Header folgen, wie z. B. `GRE` oder `IPsec`, wird das 3-Tupel aus Quell-IP, Ziel-IP und nächstem Protokoll verwendet, um einen Ablauf zu definieren.

Verfügbare Instance-Bandbreite

Die verfügbare Netzwerkbandbreite einer Instance hängt von der Anzahl der V abCPUs , die sie hat. Eine `m5.8xlarge` Instance hat beispielsweise eine Netzwerkbandbreite von 32 V CPUs und 10 Gbit/s, und eine `m5.16xlarge` Instance hat eine Netzwerkbandbreite von 64 V CPUs und 20 Gbit/s. Instances erreichen diese Bandbreite jedoch möglicherweise nicht, beispielsweise, wenn sie Netzwerkzuteilungen auf Instance-Ebene überschreiten, z. B. bei den Paketen pro Sekunde oder der Anzahl verfolgter Verbindungen. Wie viel der verfügbaren Bandbreite der Traffic nutzen kann, hängt von der Anzahl von v CPUs und dem Ziel ab. Eine `m5.16xlarge` Instance hat beispielsweise 64 VCPUs, sodass der Datenverkehr zu einer anderen Instance in der Region die gesamte verfügbare Bandbreite (20 Gbit/s) nutzen kann. Der Datenverkehr, der über ein Internet-Gateway oder ein lokales Gateway ausgeführt wird, kann jedoch nur 50 % der verfügbaren Bandbreite (10 Gbit/s) nutzen.

In der Regel wird für Instances mit 16 V CPUs oder weniger (Größe `4xlarge` und kleiner) dokumentiert, dass sie „bis zu“ eine bestimmte Bandbreite haben, zum Beispiel „bis zu 10 Gbit/s“. Diese Instances haben eine Basisbandbreite. Um zusätzlichen Bedarf zu decken, können sie einen Netzwerk-I/O-Guthabenmechanismus nutzen, der ihre Basisbandbreite übersteigt. Instances können Aufteilungsbandbreite für einen begrenzten Zeitraum verwenden, in der Regel zwischen 5 und 60 Minuten, abhängig von der Instancegröße.

Eine Instance erhält beim Start die maximale Anzahl an I/O Netzwerk-Credits. Wenn die Instance ihr I/O Netzwerkguthaben aufgebraucht hat, kehrt sie zu ihrer Basisbandbreite zurück. Eine laufende Instance verdient immer dann I/O Netzwerkguthaben, wenn sie weniger Netzwerkbandbreite als ihre Basisbandbreite verwendet. Für eine gestoppte Instance werden keine I/O Netzwerkguthaben gutgeschrieben. Instance Burst basiert auf bestem Aufwand, selbst wenn für die Instance Credits verfügbar sind, da die Burstbandbreite eine gemeinsam genutzte Ressource ist.

Es gibt separate I/O Netzwerkguthabenbereiche für eingehenden und ausgehenden Datenverkehr.

Basis- und Burst-Netzwerkleistung

Der Amazon EC2 Instance Types Guide beschreibt die Netzwerkleistung für jeden Instance-Typ sowie die Basis-Netzwerkbandbreite, die für Instances verfügbar ist, die Burst-Bandbreite verwenden können. Weitere Informationen finden Sie hier:

- Netzwerkspezifikationen – Allgemeiner Zweck
- Netzwerkspezifikationen – Für Datenverarbeitungsleistung optimiert
- Netzwerkspezifikationen – Arbeitsspeicheroptimiert
- Netzwerkspezifikationen – Speicheroptimiert
- Netzwerkspezifikationen – Beschleunigte Datenverarbeitung
- Netzwerkspezifikationen – Hochleistungs-Datenverarbeitung
- Netzwerkspezifikationen – Vorgängergeneration

Alternativ hierzu können Sie auch ein Befehlszeilen-Tool verwenden, um diese Information zu erhalten. Die EC2 Amazon-Konsole zeigt nicht die Basis-Netzwerkbandbreite eines Instance-Typs an.

AWS CLI

Sie können den describe-instance-typesBefehl verwenden, um Informationen zu einem Instance-Typ anzuzeigen. Im folgenden Beispiel werden Informationen zur Netzwerkleistung für alle C5-Instances angezeigt.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=c5.*" \
    --query "InstanceTypes[].[InstanceType, NetworkInfo.NetworkPerformance,
 NetworkInfo.NetworkCards[0].BaselineBandwidthInGbps] | sort_by(@,&[2])" \
    --output table
```

Es folgt eine Beispielausgabe. Wenn Ihrer Ausgabe die Basisbandbreite fehlt, aktualisieren Sie auf die neueste Version der AWS CLI.

```
-----------------------------------------------
|           DescribeInstanceTypes             |
+--------------+--------------------+---------+
|  c5.large    |  Up to 10 Gigabit  |  0.75   |
|  c5.xlarge   |  Up to 10 Gigabit  |  1.25   |
|  c5.2xlarge  |  Up to 10 Gigabit  |  2.5    |
|  c5.4xlarge  |  Up to 10 Gigabit  |  5.0    |
```

```
|  c5.9xlarge  |  12 Gigabit        |  12.0 |
|  c5.12xlarge |  12 Gigabit        |  12.0 |
|  c5.18xlarge |  25 Gigabit        |  25.0 |
|  c5.24xlarge |  25 Gigabit        |  25.0 |
|  c5.metal    |  25 Gigabit        |  25.0 |
+--------------+--------------------+-------+
```

PowerShell

Sie können den Get-EC2InstanceType PowerShell Befehl verwenden, um Informationen zu einem Instance-Typ anzuzeigen. Im folgenden Beispiel werden Informationen zur Netzwerkleistung für alle C5-Instances angezeigt.

```
Get-EC2InstanceType -Filter @{Name = "instance-type"; Values = "c5.*" } | `
    Select-Object `
    InstanceType,
    @{Name = 'NetworkPerformance'; Expression =
 {($_.Networkinfo.NetworkCards.NetworkPerformance)}},
    @{Name = 'BaselineBandwidthInGbps'; Expression =
 {($_.Networkinfo.NetworkCards.BaselineBandwidthInGbps)}} | `
Format-Table -AutoSize
```

Es folgt eine Beispielausgabe.

```
InstanceType NetworkPerformance BaselineBandwidthInGbps
------------ ------------------ ----------------------
c5.4xlarge   Up to 10 Gigabit                     5.00
c5.xlarge    Up to 10 Gigabit                     1.25
c5.12xlarge  12 Gigabit                          12.00
c5.9xlarge   12 Gigabit                          12.00
c5.24xlarge  25 Gigabit                          25.00
c5.metal     25 Gigabit                          25.00
c5.2xlarge   Up to 10 Gigabit                     2.50
c5.large     Up to 10 Gigabit                     0.75
c5.18xlarge  25 Gigabit                          25.00
```

EC2 Konfiguration der Gewichtung der Instanz-Bandbreite

Einige Instance-Typen unterstützen eine konfigurierbare Bandbreitengewichtung, bei der Sie eine Basis-Bandbreitengewichtung auswählen können, die entweder Netzwerkverarbeitung oder EBS-Vorgänge begünstigt. Die Standardeinstellungen für die Basisbandbreite werden von Ihrem Instance-

Typ bestimmt. Sie können die Bandbreitengewichtung beim Start konfigurieren oder Ihre Instance-Einstellungen mit den folgenden Gewichtungseinstellungen ändern:

- Standard – Diese Option verwendet die Standard-Bandbreitenkonfiguration für Ihren Instance-Typ.
- vpc-1 – Diese Option erhöht die für Netzwerke verfügbare Basisbandbreite und verringert die Basisbandbreite für EBS-Vorgänge.
- vpc-1 – Diese Option erhöht die für EBS-Vorgänge verfügbare Basisbandbreite und verringert die Basisbandbreite für Netzwerke.

Überlegungen zur Bandbreitengewichtung

Im Folgenden sind einige Überlegungen aufgeführt, die sich auf Ihre Strategie zur Bandbreitengewichtung auswirken könnten.

- Die Einstellungen für die Bandbreitengewichtung wirken sich nur auf die Bandbreitenspezifikationen aus Die Spezifikationen für Netzwerkpakete pro Sekunde (PPS) und input/output EBS-Operationen pro Sekunde (IOPS) ändern sich nicht.
- Die kombinierte Bandbreitenspezifikation zwischen Netzwerk und EBS ändert sich nicht. Wenn Sie eine Konfiguration zur Bandbreitengewichtung auswählen, erhöht sich die für die ausgewählte Option verfügbare Basisbandbreite, und die Basisbandbreite für die verbleibende Option wird um denselben absoluten Betrag reduziert. Für alle Instances außer Flex-Instances bleibt die verfügbare Burst-Bandbreite für die gewählte Option gleich und wird für die verbleibende Option reduziert. Bei Flex-Instances bis zu 4xlarge bleibt die Burst-Bandbreite unverändert. Bei Flex-Instances, 8xlarge und größer erhöht sich die Burst-Bandbreite um den gleichen Betrag wie die Basisbandbreite.
- Es ist wichtig zu verstehen, wie sich Änderungen bei der Bandbreitenzuweisung auf die I/O Leistung von EBS auswirken können. Bei EC2 Instances mit `vpc-1` Konfiguration (erhöhte Netzwerkbandbreite) kann es zu niedrigeren IOPS für EBS-Volumes kommen, wenn Sie das EBS-Bandbreitenlimit erreichen, bevor Sie das IOPS-Limit erreicht haben. Dies macht sich bei größeren Größen stärker bemerkbar. I/O

  Wenn Sie beispielsweise bei einem Instance-Typ, der normalerweise 240.000 IOPS mit einer I/O Größe von 16 KiB unterstützt, die `vpc-1` Gewichtung auswählen, kann dies die erreichbaren IOPS aufgrund des angepassten EBS-Basisbandbreitenlimits reduzieren.

  Berücksichtigen Sie bei der Planung Ihrer Arbeitslast Ihre Größe und Muster. I/O Bei kleineren I/O Größen ist die Wahrscheinlichkeit geringer, dass Bandbreitenbeschränkungen Auswirkungen

haben, wohingegen Bandbreitenänderungen bei größeren I/O Größen oder sequentiellen Workloads größere Auswirkungen haben können. Testen Sie immer Ihren spezifischen Workload, um eine optimale Leistung mit der von Ihnen gewählten Konfiguration sicherzustellen.

- Die Netzwerk-Bandbreitenspezifikation für Datenverkehr mit mehreren Abläufen, der über ein Internet-Gateway oder ein lokales Gateway geleitet wird, wird auf 50 % der Basisbandbreite der konfigurierten Option oder, falls zutreffend, auf 5 Gbit/s angepasst. Weitere Informationen finden Sie unter Netzwerkbandbreite der EC2 Amazon-Instance.

  Das folgende Beispiel basiert auf einem Instance-Typ mit einer Standard-Basisbandbreite von 40 Gbit/s und einer Standard-Grenzbandbreite von 20 Gbit/s. Wenn Sie die `vpc-1`-Bandbreitengewichtung für diese Instance wählen, ändert sich die gewichtete Basisbandbreite auf 50 Gbit/s und die Grenzbandbreite auf 25 Gbit/s.
- Diese Funktion ist in allen Handelsregionen verfügbar und richtet sich nach der Verfügbarkeit und dem Support der EC2 Instances.
- Durch diese Funktion fallen für Ihre Instance keine zusätzlichen Kosten an. EC2

Unterstützte Instance-Typen für die Bandbreitengewichtung

Instance-Typen in den folgenden Instance-Familien unterstützen eine konfigurierbare Bandbreitengewichtung.

- Allzweck: M8a, M8g, M8gd, M8i, M8i-flex
- Für die Datenverarbeitung optimiert: C8a, C8g, C8GD, C8i, C8i-Flex
- Speicheroptimiert: R8a, R8g, R8gd, R8i, R8i-Flex, X8g, X8AEDZ

Die aktuellen Bandbreiteneinstellungen überprüfen

Um die aktuellen Bandbreiteneinstellungen für Ihre Instance anzuzeigen, wählen Sie eine der Registerkarten aus, um Anweisungen zu erhalten.

Console

So rufen Sie die Bandbreiteneinstellung für eine Instance ab

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.

3. Wählen Sie die Instance, die Sie überprüfen möchten, aus der Liste aus und navigieren Sie zur Registerkarte Netzwerk. Ihre aktuelle Einstellung wird im Feld Konfigurierte Bandbreite angezeigt. Amazon EC2 verwendet Standardeinstellungen für Ihren Instance-Typ, wenn die Bandbreite nicht auf einen bestimmten Wert festgelegt ist.

AWS CLI

So rufen Sie die Bandbreiteneinstellung für eine Instance ab

Verwenden Sie den Befehl describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].NetworkPerformanceOptions.BandwidthWeighting
 \
    --output text
```

Es folgt eine Beispielausgabe.

```
default
```

In diesem Beispiel werden alle Ihre Instances aufgeführt, bei denen die Einstellung der Bandbreitengewichtung für eine höhere Netzwerkbandbreite auf `vpc-1` gesetzt ist.

```
aws ec2 describe-instances \
    --filters "Name=network-performance-options.bandwidth-weighting,Values=vpc-1" \
    --query Reservations[].Instances[].InstanceId \
    --output text
```

PowerShell

So rufen Sie die Bandbreiteneinstellung für eine Instance ab

Verwenden Sie das cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -
InstanceId i-1234567890abcdef0).Instances.NetworkPerformanceOptions.BandwidthWeighting.Value
```

Es folgt eine Beispielausgabe.

```
default
```

In diesem Beispiel werden alle Ihre Instances aufgeführt, bei denen die Einstellung der Bandbreitengewichtung für eine höhere Netzwerkbandbreite auf `vpc-1` gesetzt ist.

```
(Get-EC2Instance `
    -Filter @{Name="network-performance-options.bandwidth-
weighting";Values="vpc-1"}).Instances.InstanceId
```

Die Bandbreitengewichtung für Ihre Instance konfigurieren

Sie können die Bandbreitengewichtung entweder beim Start oder durch Ändern vorhandener Instances über die EC2 Konsole API/SDKs oder CLI konfigurieren.

Die Bandbreitengewichtung konfigurieren, wenn Sie eine Instance starten

Um die Bandbreiteneinstellungen beim Starten einer Instance zu konfigurieren, wählen Sie eine der Registerkarten aus, um Anweisungen zu erhalten.

Sie können die Bandbreitengewichtung auch in einer Startvorlage angeben. Informationen dazu, wie Sie eine Startvorlage erstellen, finden Sie unter Erstellen Sie eine EC2 Amazon-Startvorlage. Der festzulegende Parameter befindet sich an derselben Stelle wie wenn Sie eine Instance direkt von der Konsole aus starten. Erweitern Sie den Abschnitt Erweiterte Details und legen Sie die Konfiguration der Instance-Bandbreite fest.

Informationen zum Starten einer Instance mit einer Startvorlage finden Sie unter Starten Sie EC2 Instances mithilfe einer Startvorlage.

Console

So starten Sie eine Instance mit konfigurierbarer Bandbreitengewichtung

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie Launch Instances aus. Das Dialogfeld Eine Instance starten wird geöffnet. Je nach Wunsch gibt es mehrere zusätzliche Möglichkeiten, wie Sie zum Start-Dialogfeld gelangen können. Sie können eine Instance beispielsweise direkt über ein AMI oder über das EC2 Amazon-Dashboard selbst starten.

4. Das Amazon Machine Image (AMI), von dem aus Sie starten, muss auf der `Arm`-Architektur basieren. Viele Quick-Start-Images unterstützen sowohl `x86`- und `Arm`-Architekturen. Nachdem Sie das Betriebssystem für Ihre Instance ausgewählt haben, wählen Sie die Option `Arm` aus der Architekturliste aus.
5. Der Instance-Typ muss einer der Unterstützte Instance-Typen für dieses Feature sein.
6. Wenn Sie den Abschnitt Erweiterte Details erweitern, können Sie nach unten scrollen, um die Einstellungen für die Konfiguration der Instance-Bandbreite zu finden. Wählen Sie die Option zur Bandbreitenkonfiguration für Ihre Instance aus.
7. Konfigurieren Sie alle anderen Einstellungen für Ihre Instance wie gewohnt und wählen Sie Instance starten.

AWS CLI

So starten Sie eine Instance mit konfigurierbarer Bandbreitengewichtung

Verwenden Sie den Befehl run-instances mit der folgenden Option, um Instances zu starten, die für eine höhere Gewichtung der Netzwerkbandbreite konfiguriert sind.

```
--network-performance-options BandwidthWeighting=vpc-1
```

Verwenden Sie den Befehl run-instances mit der folgenden Option, um Instances zu starten, die für eine höhere Gewichtung der EBS-Bandbreite konfiguriert sind.

```
--network-performance-options BandwidthWeighting=ebs-1
```

PowerShell

So starten Sie eine Instance mit konfigurierbarer Bandbreitengewichtung

Verwenden Sie das New-EC2InstanceCmdlet mit dem folgenden Parameter, um Instances zu starten, die für eine höhere Gewichtung der Netzwerkbandbreite konfiguriert sind.

```
-NetworkPerformanceOptions_BandwidthWeighting vpc-1
```

Verwenden Sie das New-EC2InstanceCmdlet mit dem folgenden Parameter, um Instances zu starten, die für eine höhere EBS-Bandbreitengewichtung konfiguriert sind.

```
-NetworkPerformanceOptions_BandwidthWeighting ebs-1
```

Die Bandbreitengewichtung für eine vorhandene Instance aktualisieren

Um die Bandbreitengewichtung für eine vorhandene Instance zu aktualisieren, muss sich Ihre Instance im Status `Stopped` befinden.

Console

So aktualisieren Sie die Bandbreitengewichtung

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus der Liste aus, die Sie aktualisieren möchten.
4. Bevor Sie die Bandbreitenkonfiguration ändern, muss sich Ihre Instance in einem `Stopped`-Status befinden. Wenn Ihre Instance ausgeführt wird, wählen Sie im Menü Instance-Status die Option Instance anhalten aus.
5. Wählen Sie im Menü Aktionen > Netzwerk die Option Bandbreite verwalten. Dadurch wird das Dialogfeld Bandbreite verwalten geöffnet.

   > **Note**
   >
   > Wenn Ihr Instance-Typ die Konfiguration für die Bandbreitengewichtung nicht unterstützt, ist dieser Menüpunkt deaktiviert.

6. Wählen Sie die Option zum Aktualisieren Ihrer Instance aus und wählen Sie Ändern, um Ihre Einstellungen zu speichern.

AWS CLI

So aktualisieren Sie die Bandbreitengewichtung

Verwenden Sie den Befehl modify-instance-network-performance-options, um eine höhere Gewichtung der Netzwerkbandbreite für die angegebene Instance zu konfigurieren.

```
aws ec2 modify-instance-network-performance-options \
    --instance-id i-1234567890abcdef0 \
    --bandwidth-weighting=vpc-1
```

Im folgenden Beispiel wird eine höhere EBS-Bandbreitengewichtung für die angegebene Instance konfiguriert.

```
aws ec2 modify-instance-network-performance-options \
    --instance-id i-1234567890abcdef0 \
    --bandwidth-weighting=ebs-1
```

PowerShell

So aktualisieren Sie die Bandbreitengewichtung

Verwenden Sie das Edit-EC2InstanceNetworkPerformanceOptionCmdlet, um eine höhere Gewichtung der Netzwerkbandbreite für die angegebene Instanz zu konfigurieren.

```
Edit-EC2InstanceNetworkPerformanceOption `
    -InstanceId i-1234567890abcdef0 `
    -BandwidthWeighting vpc-1
```

Im folgenden Beispiel wird eine höhere EBS-Bandbreitengewichtung für die angegebene Instance konfiguriert.

```
Edit-EC2InstanceNetworkPerformanceOption `
    -InstanceId i-1234567890abcdef0 `
    -BandwidthWeighting ebs-1
```

Netzwerkleistung

Die folgende Tabelle zeigt die Netzwerkleistung in Gbit/s, die mit den Konfigurationen `default`, `vpc-1` und `ebs-1` erreicht werden kann.

Instance-Typ	**`default`** (Basisbandbreite/Spitzenlast)	**`vpc-1`** (Basisbandbreite/Spitzenlast)	**`ebs-1`** (Basisbandbreite/Spitzenlast)
c8a.medium	0,52 / 12,5	0,65 / 12,5	0,438 / 10,0
c8a. groß	0,937 / 12,5	1,172 / 12,5	0,774 / 10,0
c8a.x groß	1,875 / 12,5	2,344 / 12,5	1,562 / 10,0
c8a.2 x groß	3,75 / 15,0	4,688 / 15,0	3,125 / 12,5

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
c8a.4x groß	7,5 / 15,0	9,375 / 15,0	6,25 / 12,5
c8a.8 x groß	15,0	18,75	12,5
ca. 8 x 12 x groß	22,5	28,125	18,75
ca. 8 x 16 x groß	30.0	37,5	25.0
c8a.24x groß	40,0	50.0	32,5
ca. 8 x 48 x groß	75.0	93,75	60,0
c8a.metall-24xl	40,0	50.0	32,5
c8a.metal-48xl	75.0	93,75	60,0
c8g.medium	0,52 / 12,5	0,65 / 12,5	0,441 / 10,0
c8g.large	0,937 / 12,5	1,171 / 12,5	0,779 / 10,0
c8g.xlarge	1,875 / 12,5	2,344 / 12,5	1,562 / 10,0
c8g.2xlarge	3,75 / 15,0	4,688 / 15,0	3,125 / 12,5
c8 g, 4 x groß	7,5 / 15,0	9,375 / 15,0	6,25 / 12,5
c8g.8xgroß	15,0	18,75	12,5
cm 8 g, 12 x groß	22,5	28,125	18,75
cm 8 g, 16 x groß	30.0	37,5	25.0
c8g.24xlarge	40,0	50.0	32,5
c8g.48xlarge	50.0	62,5	40,0

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
c8g.metal-24xl	40,0	50.0	32,5
c8g.metal-48xl	50.0	62,5	40,0
c8gd.medium	0,52 / 12,5	0,65 / 12,5	0,441 / 10,0
c8gd.large	0,937 / 12,5	1,171 / 12,5	0,779 / 10,0
c8gd.xlarge	1,875 / 12,5	2,344 / 12,5	1,562 / 10,0
c8gd.2 x groß	3,75 / 15,0	4,688 / 15,0	3,125 / 12,5
c8gd.4x groß	7,5 / 15,0	9,375 / 15,0	6,25 / 12,5
c8gd.8xgroß	15,0	18,75	12,5
c 8 g, 12 x groß	22,5	28,125	18,75
c8gd.16x groß	30.0	37,5	25.0
c8gd.24xlarge	40,0	50.0	32,5
c8gd.48xlarge	50.0	62,5	40,0
c8gd.metal-24xl	40,0	50.0	32,5
c8gd.metal-48xl	50.0	62,5	40,0
c8i.large	0,937 / 12,5	1,172 / 12,5	0,774 / 10,0
c8i.xlarge	1,875 / 12,5	2,344 / 12,5	1,562 / 10,0
c8i.2 x groß	3,75 / 15,0	4,688 / 15,0	3,125 / 12,5
c8i.4x groß	7,5 / 15,0	9,375 / 15,0	6,25 / 12,5

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
c8i.8 x groß	15,0	18,75	12,5
c8i.12x groß	22,5	28,125	18,75
c8i.16x groß	30.0	37,5	25.0
c8i.24x groß	40,0	50.0	32,5
c8i.32x groß	50.0	62,5	40,0
c8i.48x groß	75.0	93,75	60,0
c8i.96xlarge	100.0	125,0	80,0
c8i.metall-48xl	75.0	93,75	60,0
c8i.metal-96xl	100.0	125,0	80,0
c8i-flex. groß	0,468 / 12,5	0,585 / 12,5	0,389 / 10,0
c8i-flex.xgroß	0,937 / 12,5	1,172 / 12,5	0,779 / 10,0
c8i-flex.2 x groß	1,875 / 15,0	2,344 / 15,0	1,562 / 12,5
c8i-flex.4x groß	3,75 / 15,0	4,688 / 15,0	3,125 / 12,5
c8i-flex.8 x groß	7,5 / 15,0	9,375 / 18,75	6,25 / 12,5
c8i-flex.12x groß	11,25 / 22,5	14,063 / 28,125	9,375 / 18,75
c8i-flex.16x groß	15,0 / 30,0	18,75 / 37,5	12,5 / 25,0
m8a.medium	0,52 / 12,5	0,65 / 12,5	0,438 / 10,0
m8a.large	0,937 / 12,5	1,172 / 12,5	0,774 / 10,0

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
m8a.xlarge	1,875 / 12,5	2,344 / 12,5	1,562 / 10,0
m8a.2 x groß	3,75 / 15,0	4,688 / 15,0	3,125 / 12,5
m8a.4x groß	7,5 / 15,0	9,375 / 15,0	6,25 / 12,5
m8a.8xgroß	15,0	18,75	12,5
m8a.12x groß	22,5	28,125	18,75
m8a.16x groß	30.0	37,5	25.0
m8a.24x groß	40,0	50.0	32,5
m8a.48x groß	75.0	93,75	60,0
m8a.metal-24xl	40,0	50.0	32,5
8 mm, Metall, 48 XL	75.0	93,75	60,0
m8g.medium	0,52 / 12,5	0,65 / 12,5	0,441 / 10,0
m8g.large	0,937 / 12,5	1,171 / 12,5	0,779 / 10,0
m8g.xlarge	1,875 / 12,5	2,344 / 12,5	1,562 / 10,0
m8g.2xlarge	3,75 / 15,0	4,688 / 15,0	3,125 / 12,5
8 g, 4 x groß	7,5 / 15,0	9,375 / 15,0	6,25 / 12,5
8 g, 8 x groß	15,0	18,75	12,5
8 mg, 12 x groß	22,5	28,125	18,75
8 mg, 16 x groß	30.0	37,5	25.0

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
m8g.24xlarge	40,0	50.0	32,5
m8g.48xlarge	50.0	62,5	40,0
m8g.metal-24xl	40,0	50.0	32,5
m8g.metal-48xl	50.0	62,5	40,0
m8gd.medium	0,52 / 12,5	0,65 / 12,5	0,441 / 10,0
m8gd.large	0,937 / 12,5	1,171 / 12,5	0,779 / 10,0
m8gd.xlarge	1,875 / 12,5	2,344 / 12,5	1,562 / 10,0
8 g, 2 x groß	3,75 / 15,0	4,688 / 15,0	3,125 / 12,5
m8 gd.4 x groß	7,5 / 15,0	9,375 / 15,0	6,25 / 12,5
m 8 g d 8 x groß	15,0	18,75	12,5
8 m g, 12 x groß	22,5	28,125	18,75
8 m g. 16 x groß	30.0	37,5	25.0
m8gd.24xlarge	40,0	50.0	32,5
m8gd.48xlarge	50.0	62,5	40,0
m8gd.metal-24xl	40,0	50.0	32,5
m8gd.metal-48xl	50.0	62,5	40,0
m8i.large	0,937 / 12,5	1,172 / 12,5	0,774 / 10,0
m8i.xlarge	1,875 / 12,5	2,344 / 12,5	1,562 / 10,0

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
m 8i, 2 x groß	3,75 / 15,0	4,688 / 15,0	3,125 / 12,5
m8i.4x groß	7,5 / 15,0	9,375 / 15,0	6,25 / 12,5
m8i.8 x groß	15,0	18,75	12,5
m 8i. 12 x groß	22,5	28,125	18,75
m 8i. 16x groß	30.0	37,5	25.0
m8i.24x groß	40,0	50.0	32,5
m 8i. 32 x groß	50.0	62,5	40,0
m 8i. 48x groß	75.0	93,75	60,0
m8i.96xlarge	100.0	125,0	80,0
m8i.metal-48xl	75.0	93,75	60,0
m8i.metal-96xl	100.0	125,0	80,0
m8i-flex. groß	0,468 / 12,5	0,585 / 12,5	0,389 / 10,0
m8i-flex.xgroß	0,937 / 12,5	1,172 / 12,5	0,779 / 10,0
m8i-flex.2 x groß	1,875 / 15,0	2,344 / 15,0	1,562 / 12,5
m8i-flex.4 x groß	3,75 / 15,0	4,688 / 15,0	3,125 / 12,5
m8i-flex.8 x groß	7,5 / 15,0	9,375 / 18,75	6,25 / 12,5
m8i-flex.12x groß	11,25 / 22,5	14,063 / 28,125	9,375 / 18,75
m8i-flex.16x groß	15,0 / 30,0	18,75 / 37,5	12,5 / 25,0

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
r8a.medium	0,52 / 12,5	0,65 / 12,5	0,438 / 10,0
r8a.large	0,937 / 12,5	1,172 / 12,5	0,774 / 10,0
r8a.xlarge	1,875 / 12,5	2,344 / 12,5	1,562 / 10,0
r8a.2 x groß	3,75 / 15,0	4,688 / 15,0	3,125 / 12,5
r8a.4x groß	7,5 / 15,0	9,375 / 15,0	6,25 / 12,5
r8a.8 x groß	15,0	18,75	12,5
r8a.12x groß	22,5	28,125	18,75
r8a.16x groß	30.0	37,5	25.0
r8a.24x groß	40,0	50.0	32,5
r8a.48x groß	75.0	93,75	60,0
r8a.metal-24xl	40,0	50.0	32,5
r8a.metal-48xl	75.0	93,75	60,0
r8g.medium	0,52 / 12,5	0,65 / 12,5	0,441 / 10,0
r8g.large	0,937 / 12,5	1,171 / 12,5	0,779 / 10,0
r8g.xlarge	1,875 / 12,5	2,344 / 12,5	1,562 / 10,0
r 8 g, 2 x groß	3,75 / 15,0	4,688 / 15,0	3,125 / 12,5
r8g.4x groß	7,5 / 15,0	9,375 / 15,0	6,25 / 12,5
r8g.8xgroß	15,0	18,75	12,5

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
r8g.12x groß	22,5	28,125	18,75
R8 G. 16 x groß	30.0	37,5	25.0
r8g.24xlarge	40,0	50.0	32,5
r8g.48xlarge	50.0	62,5	40,0
r8g.metal-24xl	40,0	50.0	32,5
r8g.metal-48xl	50.0	62,5	40,0
r8gd.medium	0,52 / 12,5	0,65 / 12,5	0,441 / 10,0
r8gd.large	0,937 / 12,5	1,171 / 12,5	0,779 / 10,0
r8gd.xlarge	1,875 / 12,5	2,344 / 12,5	1,562 / 10,0
r8gd.2xlarge	3,75 / 15,0	4,688 / 15,0	3,125 / 12,5
r 8 g d.4 x groß	7,5 / 15,0	9,375 / 15,0	6,25 / 12,5
r8gd.8xgroß	15,0	18,75	12,5
r 8 g d. 12 x groß	22,5	28,125	18,75
r 8 g d. 16 x groß	30.0	37,5	25.0
r8gd.24xlarge	40,0	50.0	32,5
r8gd.48xlarge	50.0	62,5	40,0
r8gd.metal-24xl	40,0	50.0	32,5
r8gd.metal-48xl	50.0	62,5	40,0

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
r8i.large	0,937 / 12,5	1,172 / 12,5	0,774 / 10,0
r8i.xlarge	1,875 / 12,5	2,344 / 12,5	1,562 / 10,0
r8i.2 x groß	3,75 / 15,0	4,688 / 15,0	3,125 / 12,5
r8i.4x groß	7,5 / 15,0	9,375 / 15,0	6,25 / 12,5
r8i.8 x groß	15,0	18,75	12,5
r8i.12x groß	22,5	28,125	18,75
r8i.16x groß	30.0	37,5	25.0
r8i.24x groß	40,0	50.0	32,5
r8i.32x groß	50.0	62,5	40,0
r8i.48x groß	75.0	93,75	60,0
r8i.96xlarge	100.0	125,0	80,0
r8i.metall-48xl	75.0	93,75	60,0
r8i.metal-96xl	100.0	125,0	80,0
r8i-flex.large	0,468 / 12,5	0,585 / 12,5	0,389 / 10,0
r8i-flex.xlarge	0,937 / 12,5	1,172 / 12,5	0,779 / 10,0
r8i-flex.2xlarge	1,875 / 15,0	2,344 / 15,0	1,562 / 12,5
r8i-flex.4xlarge	3,75 / 15,0	4,688 / 15,0	3,125 / 12,5
r8i-flex.8xlarge	7,5 / 15,0	9,375 / 18,75	6,25 / 12,5

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
r8i-flex.12xlarge	11,25 / 22,5	14,063 / 28,125	9,375 / 18,75
r8i-flex.16xlarge	15,0 / 30,0	18,75 / 37,5	12,5 / 25,0
x8g.medium	0,52 / 12,5	0,65 / 12,5	0,441 / 10,0
x8g.large	0,937 / 12,5	1,171 / 12,5	0,779 / 10,0
x8g.xlarge	1,875 / 12,5	2,344 / 12,5	1,562 / 10,0
x8g.2xlarge	3,75 / 15,0	4,688 / 15,0	3,125 / 12,5
x8g.4xlarge	7,5 / 15,0	9,375 / 15,0	6,25 / 12,5
x8g.8xlarge	15,0	18,75	12,5
x8g.12xlarge	22,5	28,125	18,75
x8g.16xlarge	30.0	37,5	25.0
x8g.24xlarge	40,0	50.0	32,5
x8g.48xlarge	50.0	62,5	40,0
x8g.metal-24xl	40,0	50.0	32,5
x8g.metal-48xl	50.0	62,5	40,0
x8aedz. groß	1,562/18,75	1,953/18,75	1,249/15,0
x8aedz.x groß	3,125/18,75	3,907/18,75	2,5/15,0
x8aedz.3x groß	9,375 / 18,75	11,719/18,75	7,5 / 15,0
x8aedz.6x groß	18,75	23,438	15,0

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
x8aedz.12x groß	37,5	46,875	30.0
x8aedz.24x groß	75.0	93,75	60,0
x8aedz.metall-12xl	37,5	46,875	30.0
x8aedz.metall-24xl	75.0	93,75	60,0

Amazon-EBS-Leistung

Die folgende Tabelle zeigt die Amazon-EBS-Leistung in Gbit/s, die mit den Konfigurationen `default`, `vpc-1` und `ebs-1` erreicht werden kann.

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
c8a. mittel	0,325 / 10,0	0,195 / 6,25	0,407 / 10,0
c8a. groß	0,65 / 10,0	0,415 / 6,25	0,813 / 10,0
c8a.x groß	1,25 / 10,0	0,781 / 6,25	1,563 / 10,0
c8a.2 x groß	2,5 / 10,0	1,562 / 6,25	3,125 / 10,0
c8a.4x groß	5,0 / 10,0	3,125 / 6,25	6,25 / 10,0
c8a.8 x groß	10.0	6,25	12,5
ca. 8 x 12 x groß	15,0	9,375	18,75
ca. 8 x 16 x groß	20.0	12,5	25.0

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
c8a.24x groß	30.0	20.0	37,5
c8a.48x groß	60,0	41,25	75.0
c8a.metall-24xl	30.0	20.0	37,5
c8a.metall-48xl	60,0	41,25	75.0
c8g.medium	0,315 / 10,0	0,185 / 6,25	0,394 / 10,0
c8g.large	0,63 / 10,0	0,396 / 6,25	0,788 / 10,0
c8g.xlarge	1,25 / 10,0	0,781 / 6,25	1,563 / 10,0
c8g.2xlarge	2,5 / 10,0	1,562 / 6,25	3,125 / 10,0
c8 g, 4 x groß	5,0 / 10,0	3,125 / 6,25	6,25 / 10,0
c8g.8xgroß	10.0	6,25	12,5
cm 8 g, 12 x groß	15,0	9,375	18,75
cm 8 g, 16 x groß	20.0	12,5	25.0
c8g.24xlarge	30.0	20.0	37,5
c8g.48xlarge	40,0	27,5	50.0
c8g.metal-24xl	30.0	20.0	37,5
c8g.metal-48xl	40,0	27,5	50.0
c8gd.medium	0,315 / 10,0	0,185 / 6,25	0,394 / 10,0
c8gd.large	0,63 / 10,0	0,396 / 6,25	0,788 / 10,0

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
c8gd.xlarge	1,25 / 10,0	0,781 / 6,25	1,563 / 10,0
c8gd.2xgroß	2,5 / 10,0	1,562 / 6,25	3,125 / 10,0
c8gd.4x groß	5,0 / 10,0	3,125 / 6,25	6,25 / 10,0
c8gd.8xgroß	10.0	6,25	12,5
c 8 g, 12 x groß	15,0	9,375	18,75
c8gd.16x groß	20.0	12,5	25.0
c8gd.24xlarge	30.0	20.0	37,5
c8gd.48xlarge	40,0	27,5	50.0
c8gd.metal-24xl	30.0	20.0	37,5
c8gd.metal-48xl	40,0	27,5	50.0
c8i.large	0,65 / 10,0	0,415 / 6,25	0,813 / 10,0
c8i.xlarge	1,25 / 10,0	0,781 / 6,25	1,563 / 10,0
c8i.2 x groß	2,5 / 10,0	1,562 / 6,25	3,125 / 10,0
c8i.4x groß	5,0 / 10,0	3,125 / 6,25	6,25 / 10,0
c8i.8 x groß	10.0	6,25	12,5
c8i.12x groß	15,0	9,375	18,75
c8i.16x groß	20.0	12,5	25.0
c8i.24x groß	30.0	20.0	37,5

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
c8i.32x groß	40,0	27,5	50.0
c8i.48x groß	60,0	41,25	75.0
c8i.96xlarge	80,0	55,0	100.0
c8i.metall-48xl	60,0	41,25	75.0
c8i.metal-96xl	80,0	55,0	100.0
c8i-flex. groß	0,315 / 10,0	0,198 / 6,25	0,394 / 10,0
c8i-flex.xgroß	0,63 / 10,0	0,395 / 6,25	0,788 / 10,0
c8i-flex.2 x groß	1,25 / 10,0	0,781 / 6,25	1,563 / 10,0
c8i-flex.4x groß	2,5 / 10,0	1,562 / 6,25	3,125 / 10,0
c8i-flex.8 x groß	5,0 / 10,0	3,125 / 6,25	6,25 / 12,5
c8i-flex.12x groß	7,5 / 15,0	4,687 / 9,375	9,375 / 18,75
c8i-flex.16x groß	10,0 / 20,0	6,25 / 12,5	12,5 / 25,0
m8a.medium	0,325 / 10,0	0,195 / 6,25	0,407 / 10,0
m8a.large	0,65 / 10,0	0,415 / 6,25	0,813 / 10,0
m8a.xlarge	1,25 / 10,0	0,781 / 6,25	1,563 / 10,0
m8a.2 x groß	2,5 / 10,0	1,562 / 6,25	3,125 / 10,0
m8a.4x groß	5,0 / 10,0	3,125 / 6,25	6,25 / 10,0
m8a.8xgroß	10.0	6,25	12,5

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
8 m x 12 x groß	15,0	9,375	18,75
m8a.16x groß	20.0	12,5	25.0
m8a.24x groß	30.0	20.0	37,5
m8a.48x groß	60,0	41,25	75.0
m8a.metal-24xl	30.0	20.0	37,5
8 mm, Metall, 48 XL	60,0	41,25	75.0
m8g.medium	0,315 / 10,0	0,185 / 6,25	0,394 / 10,0
m8g.large	0,63 / 10,0	0,396 / 6,25	0,788 / 10,0
m8g.xlarge	1,25 / 10,0	0,781 / 6,25	1,563 / 10,0
m8g.2xlarge	2,5 / 10,0	1,562 / 6,25	3,125 / 10,0
8 g, 4 x groß	5,0 / 10,0	3,125 / 6,25	6,25 / 10,0
8 g, 8 x groß	10.0	6,25	12,5
8 mg, 12 x groß	15,0	9,375	18,75
8 mg, 16 x groß	20.0	12,5	25.0
m8g.24xlarge	30.0	20.0	37,5
m8g.48xlarge	40,0	27,5	50.0
m8g.metal-24xl	30.0	20.0	37,5
m8g.metal-48xl	40,0	27,5	50.0

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
m8gd.medium	0,315 / 10,0	0,185 / 6,25	0,394 / 10,0
m8gd.large	0,63 / 10,0	0,396 / 6,25	0,788 / 10,0
m8gd.xlarge	1,25 / 10,0	0,781 / 6,25	1,563 / 10,0
8 g, 2 x groß	2,5 / 10,0	1,562 / 6,25	3,125 / 10,0
m8 gd.4 x groß	5,0 / 10,0	3,125 / 6,25	6,25 / 10,0
m 8 g d 8 x groß	10.0	6,25	12,5
8 m g, 12 x groß	15,0	9,375	18,75
8 m g. 16 x groß	20.0	12,5	25.0
m8gd.24xlarge	30.0	20.0	37,5
m8gd.48xlarge	40,0	27,5	50.0
m8gd.metal-24xl	30.0	20.0	37,5
m8gd.metal-48xl	40,0	27,5	50.0
m8i.large	0,65 / 10,0	0,415 / 6,25	0,813 / 10,0
m8i.xlarge	1,25 / 10,0	0,781 / 6,25	1,563 / 10,0
m 8i, 2 x groß	2,5 / 10,0	1,562 / 6,25	3,125 / 10,0
m8i.4x groß	5,0 / 10,0	3,125 / 6,25	6,25 / 10,0
m8i.8 x groß	10.0	6,25	12,5
m 8i. 12 x groß	15,0	9,375	18,75

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
m 8i. 16x groß	20.0	12,5	25.0
m8i.24x groß	30.0	20.0	37,5
m8i.32x groß	40,0	27,5	50.0
m 8i. 48x groß	60,0	41,25	75.0
m8i.96xlarge	80,0	55,0	100.0
m8i.metal-48xl	60,0	41,25	75.0
m8i.metal-96xl	80,0	55,0	100.0
m8i-flex. groß	0,315 / 10,0	0,198 / 6,25	0,394 / 10,0
m8i-flex.xgroß	0,63 / 10,0	0,395 / 6,25	0,788 / 10,0
m8i-flex.2 x groß	1,25 / 10,0	0,781 / 6,25	1,563 / 10,0
m8i-flex.4 x groß	2,5 / 10,0	1,562 / 6,25	3,125 / 10,0
m8i-flex.8 x groß	5,0 / 10,0	3,125 / 6,25	6,25 / 12,5
m8i-flex.12x groß	7,5 / 15,0	4,687 / 9,375	9,375 / 18,75
m8i-flex.16x groß	10,0 / 20,0	6,25 / 12,5	12,5 / 25,0
r8a.medium	0,325 / 10,0	0,195 / 6,25	0,407 / 10,0
r8a.large	0,65 / 10,0	0,415 / 6,25	0,813 / 10,0
r8a.xlarge	1,25 / 10,0	0,781 / 6,25	1,563 / 10,0
r8a.2 x groß	2,5 / 10,0	1,562 / 6,25	3,125 / 10,0

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
r8a.4x groß	5,0 / 10,0	3,125 / 6,25	6,25 / 10,0
r8a.8 x groß	10.0	6,25	12,5
r8a.12x groß	15,0	9,375	18,75
r8a.16x groß	20.0	12,5	25.0
r8a.24x groß	30.0	20.0	37,5
r8a.48x groß	60,0	41,25	75.0
r8a.metal-24xl	30.0	20.0	37,5
r8a.metal-48xl	60,0	41,25	75.0
r8g.medium	0,315 / 10,0	0,185 / 6,25	0,394 / 10,0
r8g.large	0,63 / 10,0	0,396 / 6,25	0,788 / 10,0
r8g.xlarge	1,25 / 10,0	0,781 / 6,25	1,563 / 10,0
r 8 g, 2 x groß	2,5 / 10,0	1,562 / 6,25	3,125 / 10,0
r8g.4x groß	5,0 / 10,0	3,125 / 6,25	6,25 / 10,0
r8g.8xgroß	10.0	6,25	12,5
r8 g, 12 x groß	15,0	9,375	18,75
R8 G. 16 x groß	20.0	12,5	25.0
r8g.24xlarge	30.0	20.0	37,5
r8g.48xlarge	40,0	27,5	50.0

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
r8g.metal-24xl	30.0	20.0	37,5
r8g.metal-48xl	40,0	27,5	50.0
r8gd.medium	0,315 / 10,0	0,185 / 6,25	0,394 / 10,0
r8gd.large	0,63 / 10,0	0,396 / 6,25	0,788 / 10,0
r8gd.xlarge	1,25 / 10,0	0,781 / 6,25	1,563 / 10,0
r8gd.2xlarge	2,5 / 10,0	1,562 / 6,25	3,125 / 10,0
r 8 g d.4 x groß	5,0 / 10,0	3,125 / 6,25	6,25 / 10,0
r8gd.8xgroß	10.0	6,25	12,5
r 8 g d. 12 x groß	15,0	9,375	18,75
r 8 g d. 16 x groß	20.0	12,5	25.0
r8gd.24xlarge	30.0	20.0	37,5
r8gd.48xlarge	40,0	27,5	50.0
r8gd.metal-24xl	30.0	20.0	37,5
r8gd.metal-48xl	40,0	27,5	50.0
r8i.large	0,65 / 10,0	0,415 / 6,25	0,813 / 10,0
r8i.xlarge	1,25 / 10,0	0,781 / 6,25	1,563 / 10,0
r8i.2 x groß	2,5 / 10,0	1,562 / 6,25	3,125 / 10,0
r8i.4x groß	5,0 / 10,0	3,125 / 6,25	6,25 / 10,0

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
r8i.8 x groß	10.0	6,25	12,5
r8i.12x groß	15,0	9,375	18,75
r8i.16x groß	20.0	12,5	25.0
r8i.24x groß	30.0	20.0	37,5
r8i.32x groß	40,0	27,5	50.0
r8i.48x groß	60,0	41,25	75.0
r8i.96xlarge	80,0	55,0	100.0
r8i.metall-48xl	60,0	41,25	75.0
r8i.metal-96xl	80,0	55,0	100.0
r8i-flex.large	0,315 / 10,0	0,198 / 6,25	0,394 / 10,0
r8i-flex.xlarge	0,63 / 10,0	0,395 / 6,25	0,788 / 10,0
r8i-flex.2xlarge	1,25 / 10,0	0,781 / 6,25	1,563 / 10,0
r8i-flex.4xlarge	2,5 / 10,0	1,562 / 6,25	3,125 / 10,0
r8i-flex.8xlarge	5,0 / 10,0	3,125 / 6,25	6,25 / 12,5
r8i-flex.12xlarge	7,5 / 15,0	4,687 / 9,375	9,375 / 18,75
r8i-flex.16xlarge	10,0 / 20,0	6,25 / 12,5	12,5 / 25,0
x8g.medium	0,315 / 10,0	0,185 / 6,25	0,394 / 10,0
x8g.large	0,63 / 10,0	0,396 / 6,25	0,788 / 10,0

Instance-Typ	**default** (Basisbandbreite/Spitzenlast)	**vpc-1** (Basisbandbreite/Spitzenlast)	**ebs-1** (Basisbandbreite/Spitzenlast)
x8g.xlarge	1,25 / 10,0	0,781 / 6,25	1,563 / 10,0
x8g.2xlarge	2,5 / 10,0	1,562 / 6,25	3,125 / 10,0
x8g.4xlarge	5,0 / 10,0	3,125 / 6,25	6,25 / 10,0
x8g.8xlarge	10.0	6,25	12,5
x8g.12xlarge	15,0	9,375	18,75
x8g.16xlarge	20.0	12,5	25.0
x8g.24xlarge	30.0	20.0	37,5
x8g.48xlarge	40,0	27,5	50.0
x8g.metal-24xl	30.0	20.0	37,5
x8g.metal-48xl	40,0	27,5	50.0
x8aedz. groß	1,25/15,0	0,859/10,312	1,563/15,0
x8aedz.x groß	2,5/15,0	1,718/10,312	3,125/15,0
x8aedz.3x groß	7,5 / 15,0	5,156/10,312	9,375 / 15,0
x8aedz.6x groß	15,0	10,312	18,75
x8aedz.12x groß	30.0	20,625	37,5
x8aedz.24x groß	60,0	41,25	75.0
x8aedz.metall-12xl	30.0	20,625	37,5
x8aedz.metall-24xl	60,0	41,25	75.0

Überwachen der Instance-Bandbreite

Sie können CloudWatch Metriken verwenden, um die Netzwerkbandbreite der Instance und die gesendeten und empfangenen Pakete zu überwachen. Sie können die vom Elastic Network Adapter (ENA) -Treiber bereitgestellten Netzwerkleistungsmetriken verwenden, um zu überwachen, wann der Datenverkehr die von Amazon auf Instance-Ebene EC2 definierten Netzwerkberechtigungen überschreitet.

Sie können konfigurieren, ob Amazon Metrikdaten für die Instance in Zeiträumen CloudWatch von einer Minute oder fünf Minuten EC2 sendet. Es ist möglich, dass die Netzwerkleistungsmetriken zeigen, dass eine zulässige Menge überschritten wurde und Pakete verworfen wurden, während dies bei den CloudWatch Instance-Metriken nicht der Fall ist. Dies kann passieren, wenn die Instance einen kurzen Anstieg der Nachfrage nach Netzwerkressourcen (bekannt als Microburst) hat, die CloudWatch Metriken aber nicht detailliert genug sind, um diese Mikrosekundenspitzen widerzuspiegeln.

Weitere Informationen

- Instance-Metriken
- Überwachen der Netzwerkleistung

Erweitertes Netzwerk in Amazon-EC2-Instances

Enhanced Networking verwendet Single Root I/O Virtualization (SR-IOV), um Hochleistungsnetzwerk-Funktionen in unterstützten Instance-Typen bereitzustellen. SR-IOV ist eine Methode zur Gerätevirtualisierung, die im Vergleich zu herkömmlichen virtualisierten Netzwerkschnittstellen eine höhere I/O-Leistung bei niedrigerer CPU-Auslastung bietet. Erweitertes Netzwerk ermöglicht eine größere Bandbreite, mehr Pakete pro Sekunde (PPS) und konstant niedrigere Latenzzeiten zwischen Instances. Für die Nutzung von Enhanced Networking fallen keine zusätzlichen Gebühren an.

Weitere Informationen zur unterstützten Netzwerkgeschwindigkeit für die einzelnen Instance-Typen finden Sie unter Amazon EC2-Instance-Typen.

Sie können das Enhanced Networking mit einem der folgenden Mechanismen aktivieren:

Elastic Network Adapter (ENA)

Der Elastic Network Adapter (ENA) unterstützt Netzwerkgeschwindigkeiten von bis zu 100 Gbit/s für unterstützte Instance-Typen.

Alle Nitro-basierten Instances verwenden ENA für Erweitertes Netzwerk. Darüber hinaus verwenden die folgenden Xen-Instance-Typen ENA: H1, I3, G3, `m4.16xlarge`, P2, P3, P3dn und R4.

Weitere Informationen finden Sie unter Ermöglichen Sie Enhanced Networking mit ENA auf Ihren EC2 Instances.

Intel 82599 Virtual Function-Schnittstelle (VF

Die Intel 82599 Virtual Function-Schnittstelle unterstützt Netzwerkgeschwindigkeiten von bis zu 10 Gbit/s für unterstützte Instance-Typen.

Die folgenden Instance-Typen verwenden die Intel-82599-VF-Schnittstelle für erweiterte Netzwerke: C3, C4, D2, I2, M4 (ausgenommen m4.16xlarge) und R3.

Weitere Informationen finden Sie unter Erweitertes Netzwerk mit der Intel 82599 VF-Schnittstelle.

Inhalt

- Ermöglichen Sie Enhanced Networking mit ENA auf Ihren EC2 Instances
- Verbessern Sie die Netzwerkleistung zwischen EC2 Instanzen mit ENA Express
- Erweitertes Netzwerk mit der Intel 82599 VF-Schnittstelle
- Netzwerkleistung für ENA-Einstellungen auf Ihrer EC2-Instance überwachen
- Verbessern Sie die Netzwerklatenz für Linux-basierte EC2-Instances
- Überlegungen zum Nitro-System für die Leistungsoptimierung
- Die Netzwerkleistung in EC2-Windows-Instances optimieren

Ermöglichen Sie Enhanced Networking mit ENA auf Ihren EC2 Instances

Amazon EC2 bietet erweiterte Netzwerkfunktionen über den Elastic Network Adapter (ENA). Um erweitertes Netzwerk nutzen zu können, müssen Sie ein AMI verwenden, das den erforderlichen ENA-Treiber enthält, oder ihn manuell installieren. Dann können Sie die ENA-Unterstützung in Ihrer Instance aktivieren.

Die Versionshinweise oder Installationsanweisungen für einen ENA-Treiber finden Sie auf der Registerkarte, die der Betriebssystemplattform Ihrer Instance entspricht.

Linux

Sie können die folgende Dokumentation lesen unter GitHub:

- Lesen Sie die Versionshinweise zum ENA-Linux-Kerneltreiber unter GitHub.
- Eine Übersicht über den ENA-Linux-Kerneltreiber, einschließlich Installationsanweisungen, finden Sie unter Linux-Kerneltreiber für die Elastic Network Adapter (ENA) -Familie unter GitHub.

Windows

Sie können die folgende Dokumentation im Abschnitt Gerätetreiber verwalten dieses Handbuchs nachlesen:

- NA-Windows-Treiber-Versionen verfolgen.
- ENA-Treiber auf EC2-Windows-Instances installieren.

Bei Nitro-basierten Instances variieren die erweiterten Netzwerkfunktionen je nach der Nitro-Version, die der Instance-Typ implementiert.

Um die Netzwerkspezifikationen für Ihre Instance zu überprüfen, wählen Sie den Link zur Instance-Familie für Ihren Instance-Typ. Wenn Sie sich nicht sicher sind, welche Instance-Familie gilt, finden Sie weitere Informationen unter Benennungskonventionen im EC2 Amazon-Instanztypen-Leitfaden.

- Netzwerkspezifikationen für beschleunigte Computing-Instances
- Netzwerkspezifikationen für Datenverarbeitung optimierte Instances
- Netzwerkspezifikationen für Allzweck-Instances
- Netzwerkspezifikationen für Hochleistungs-Computing-Instances
- Netzwerkspezifikationen für arbeitsspeicheroptimierte Instances
- Netzwerkspezifikationen für speicheroptimierte Instances

Inhalt

- Voraussetzungen für erweiterte Netzwerke mit ENA
- Testen, ob Enhanced Networking aktiviert ist
- Aktivieren von Enhanced Networking auf Ihrer Instance
- ENA-Warteschlangen

- Problembehandlung beim ENA-Kernel-Treiber in Linux
- Fehlerbehebung beim Windows-Treiber von Elastic Network Adapter

Voraussetzungen für erweiterte Netzwerke mit ENA

Zur Vorbereitung für Enhanced Networking mit ENA sollten Sie Ihre Instance wie folgt einrichten:

- Starten Sie eine Nitro-basierte Instance.
- Überprüfen Sie, ob der Instance eine Verbindung zum Internet fehlt.
- Wenn Sie wichtige Daten auf der Instance gespeichert haben, die Sie erhalten möchten, sollten Sie diese Daten jetzt sichern, indem Sie ein AMI von Ihrer Instance erstellen. Die Aktualisierung des ENA-Kernel-Treibers und die Aktivierung des Attributs `enaSupport` kann dazu führen, dass inkompatible Instances oder Betriebssysteme nicht mehr erreicht werden können. Wenn Sie über ein aktuelles Backup verfügen, gehen die Daten nicht verloren, falls das geschieht.
- Linux-Instances – Starten Sie die Instance mit einer unterstützten Version des Linux-Kernels sowie einer unterstützten Distribution, um ENA Enhanced Networking für Ihre Instance automatisch zu aktivieren. Weitere Informationen finden Sie unter ENA Linux Kernel Driver Release Notes.
- Windows-Instances — Wenn auf der Instance Windows Server 2008 R2 ausgeführt wird, stellen Sie sicher SP1, dass sie über das Update zur Unterstützung der SHA-2-Codesignatur verfügt.
- Verwenden Sie AWS CloudShelldas AWS-Managementkonsole oder installieren und konfigurieren Sie das AWS CLIoder AWS Tools for Windows PowerShellauf einem beliebigen Computer Ihrer Wahl, vorzugsweise auf Ihrem lokalen Desktop oder Laptop. Weitere Informationen finden Sie unter Zugriff auf Amazon EC2 oder im AWS CloudShell -Benutzerhandbuch. Enhanced Networking kann nicht von der EC2 Amazon-Konsole aus verwaltet werden.

Testen, ob Enhanced Networking aktiviert ist

Sie können testen, ob Enhanced Networking in Ihren oder Ihren Instances aktiviert ist AMIs.

Instance-Attribut

Überprüfen Sie den Wert des Instance-Attributs `enaSupport`.

AWS CLI

Verwenden Sie den Befehl describe-instances.

```
aws ec2 describe-instances \
```

```
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[].Instances[].EnaSupport"
```

Wenn Enhanced Networking aktiviert ist, sieht die Ausgabe wie folgt aus.

```
[
    true
]
```

PowerShell

Verwenden Sie das cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.EnaSupport
```

Wenn Enhanced Networking aktiviert ist, sieht die Ausgabe wie folgt aus.

```
True
```

Image-Attribut

Überprüfen Sie den Wert des Image-Attributs `enaSupport`.

AWS CLI

Verwenden Sie den Befehl describe-images.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query "Images[].EnaSupport"
```

Wenn Enhanced Networking aktiviert ist, sieht die Ausgabe wie folgt aus.

```
[
    true
]
```

PowerShell

Verwenden Sie das cmdlet Get-EC2Image.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).EnaSupport
```

Wenn Enhanced Networking aktiviert ist, sieht die Ausgabe wie folgt aus.

```
True
```

Linux-Netzwerkschnittstellentreiber

Prüfen Sie mit dem folgenden Befehl, ob der `ena`-Kernel-Treiber aktuell an einer bestimmten Schnittstelle verwendet wird; setzen Sie dabei den Namen der Schnittstelle ein, die Sie überprüfen möchten. Wenn Sie eine einzige Schnittstelle verwenden (der Standard), lautet der Name `eth0`. Wenn Ihre Linux-Distribution vorhersagbare Netzwerknamen unterstützt, könnte der Name `ens5` lauten. Weitere Informationen erhalten Sie, indem Sie den Abschnitt für RHEL, SUSE und CentOS in Aktivieren von Enhanced Networking auf Ihrer Instance erweitern.

Im folgenden Beispiel wird der `ena`-Kernel-Treiber nicht geladen, da als Treiber `vif` angezeigt wird.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

In diesem Beispiel wurde der `ena`-Kernel-Treiber bereits geladen und liegt in der empfohlenen Mindestversion vor. In dieser Instance wurde Enhanced Networking richtig konfiguriert.

```
[ec2-user ~]$ ethtool -i eth0
driver: ena
version: 1.5.0g
firmware-version:
expansion-rom-version:
bus-info: 0000:00:05.0
supports-statistics: yes
supports-test: no
```

```
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Aktivieren von Enhanced Networking auf Ihrer Instance

Welches Verfahren Sie verwenden, hängt vom Betriebssystem der Instance ab.

Amazon Linux

Die AMIs für Amazon Linux enthalten den Kernel-Treiber, der für Enhanced Networking erforderlich ist, wenn ENA installiert ist und die ENA-Unterstützung aktiviert ist. Wenn Sie eine Instance mit einer HVM-Version von Amazon Linux auf einem unterstützten Instance-Typ starten, ist Enhanced Networking für Ihre Instance bereits aktiviert. Weitere Informationen finden Sie unter Testen, ob Enhanced Networking aktiviert ist.

Ubuntu

Die neuesten HVMs von Ubuntu AMIs enthalten den Kernel-Treiber, der für erweiterte Netzwerke erforderlich ist, wenn ENA installiert ist, und die ENA-Unterstützung ist aktiviert. Wenn Sie also eine Instance mit dem aktuellen Ubuntu HVM-AMI auf einem unterstützten Instance-Typ starten, ist Enhanced Networking bereits für Ihre Instance aktiviert. Weitere Informationen finden Sie unter Testen, ob Enhanced Networking aktiviert ist.

Wenn Sie Ihre Instance aus einem älteren AMI gestartet haben und Enhanced Networking noch nicht aktiviert wurde, können Sie das Kernel-Paket `linux-aws` installieren, um die aktuellen Enhanced Networking-Treiber zu erhalten und das erforderliche Attribut zu aktualisieren.

`linux-aws`-Kernel-Paket (Ubuntu 16.04 oder höher) installieren

Ubuntu 16.04 und 18.04 werden mit dem benutzerdefinierten Ubuntu-Kernel geliefert (`linux-aws`-Kernel-Paket). Um einen anderen Kernel zu verwenden, wenden Sie sich an Support.

`linux-aws`-Kernel-Paket (Ubuntu Trusty 14.04) installieren

1. Verbinden Sie sich mit der Instance.
2. Aktualisieren Sie den Cache der Paketverwaltung und die einzelnen Pakete.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

> **Important**
>
> Wenn Sie während des Aktualisierungsvorgangs aufgefordert werden, `grub` zu installieren, verwenden Sie `/dev/xvda` für die Installation von `grub` und wählen Sie anschließend aus, dass die aktuelle Version von `/boot/grub/menu.lst` beibehalten werden soll.

3. [EBS-gestützte Instance] Stoppen Sie die Instance von Ihrem lokalen Computer aus mithilfe der EC2 Amazon-Konsole oder mit einem der folgenden Befehle: stop-instances(AWS CLI) oder Stop-EC2Instance(AWS Tools for Windows PowerShell).

   [In einem Instance-Speicher gesicherte Instance] Sie können die Instance nicht anhalten, um das Attribut zu ändern. Gehen Sie stattdessen wie folgt vor: So aktivieren Sie Enhanced Networking unter Ubuntu (Instance Store-Backed Instances).

4. Aktivieren Sie auf Ihrem lokalen Computer das Enhanced Networking-Attribut mit einem der folgenden Befehle:

   - modify-instance-attribute (AWS CLI)

     ```
     aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --ena-support
     ```

   - Edit-EC2InstanceAttribute(Tools für Windows) PowerShell

     ```
     Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -EnaSupport $true
     ```

5. (Optional) Erstellen Sie ein AMI von der Instance, wie unter Ein Amazon-EBS-gestütztes AMI erstellen beschrieben. Das AMI erbt das Enhanced Networking-Attribut `enaSupport` von der Instance. D. h. Sie können mit diesem AMI eine andere Instance starten, in der Enhanced Networking standardmäßig aktiviert ist.
6. Starten Sie die Instance von Ihrem lokalen Computer aus mit der EC2 Amazon-Konsole oder einem der folgenden Befehle: start-instances(AWS CLI) oder Start-EC2Instance(AWS Tools for Windows PowerShell).

So aktivieren Sie Enhanced Networking unter Ubuntu (Instance Store-Backed Instances)

Führen Sie die Schritte aus dem vorherigen Verfahren durch bis zu dem Schritt, in dem die Instance angehalten wird. Erstellen Sie ein neues AMI, wie in Ein Amazon-S3-gestütztes AMI erstellen

beschreiben, um sicherzustellen, dass Sie das Enhanced Networking-Attribut aktivieren, wenn Sie das AMI registrieren.

- register-image (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

RHEL, SUSE, CentOS

Die neuesten Versionen AMIs für Red Hat Enterprise Linux, SUSE Linux Enterprise Server und CentOS enthalten den Kernel-Treiber, der für Enhanced Networking mit ENA erforderlich ist, und haben ENA-Unterstützung aktiviert. Wenn Sie also eine Instance mit dem aktuellen AMI auf einem unterstützten Instance-Typ starten, ist Enhanced Networking bereits für Ihre Instance aktiviert. Weitere Informationen finden Sie unter Testen, ob Enhanced Networking aktiviert ist.

In der folgenden Anleitung werden die Schritte beschrieben, die Sie für die Aktivierung von Enhanced Networking unter einer anderen Linux-Distribution als Amazon Linux AMI oder Ubuntu ausführen müssen. Weitere Informationen, z. B. hinsichtlich der genauen Syntax für Befehle, der Speicherorte von Dateien oder der Unterstützung von einzelnen Paketen bzw. Tools, finden Sie in der Dokumentation zu der jeweiligen Linux-Distribution.

Aktivieren von Enhanced Networking in Linux

1. Verbinden Sie sich mit der Instance.
2. Klonen Sie den Quellcode für den `ena` Kernel-Treiber auf Ihrer Instance von GitHub at. https://github.com/amzn/amzn-drivers (SUSE Linux Enterprise Server 12 SP2 und höher enthalten standardmäßig ENA 2.02, sodass Sie den ENA-Treiber nicht herunterladen und kompilieren müssen. Für SUSE Linux Enterprise Server 12 SP2 und höher sollten Sie eine Anfrage stellen, um die gewünschte Treiberversion zum Standardkernel hinzuzufügen).

   ```
   git clone https://github.com/amzn/amzn-drivers
   ```

3. Kompilieren und installieren Sie den `ena`-Kernel-Treiber in Ihrer Instance. Diese Schritte hängen von der Linux-Distribution ab. Weitere Informationen zur Kompilierung des Kernel-Treibers auf

Red Hat Enterprise Linux finden Sie unter Wie installiere ich den neuesten ENS-Treiber für erweiterte Netzwerkunterstützung auf einer EC2 Amazon-Instance, die RHEL ausführt?

4. Führen Sie den Befehl sudo depmod aus, um die Abhängigkeiten für das Modul zu aktualisieren.
5. Aktualisieren Sie `initramfs` in Ihrer Instance, um sicherzustellen, dass der neue Kernel-Treiber während des Bootvorgangs geladen wird. Wenn die Verteilung beispielsweise dracut unterstützt, können Sie den folgenden Befehl verwenden.

```
dracut -f -v
```

6. Ermitteln Sie, ob Ihr System standardmäßig transparente Netzwerkschnittstellennamen verwendet. Systeme, die systemd- oder udev-Versionen ab 197 verwenden, können Ethernet-Geräte umbenennen, d. h. die einzige Netzwerkschnittstelle in einem solchen System wird nicht zwingend als `eth0` bezeichnet. Dieses Verhalten kann Probleme bei der Verbindung mit Ihrer Instance verursachen. Weitere Informationen und andere Konfigurationsoptionen finden Sie unter Predictable Network Interface Names auf der freedesktop.org-Website.

   a. Sie können die systemd- und udev-Versionen auf RPM-basierten Systemen mit dem folgenden Befehl überprüfen.

   ```
   rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
   systemd-208-11.el7_0.2.x86_64
   ```

   In dem Red Hat Enterprise Linux 7-Beispiel oben lautet die systemd-Version 208, d. h. transparente Netzwerkschnittstellennamen müssen deaktiviert werden.

   b. Sie können transparente Netzwerkschnittstellennamen deaktivieren, indem Sie in der Zeile `net.ifnames=0` in der Datei `GRUB_CMDLINE_LINUX` die Option `/etc/default/grub` hinzufügen.

   ```
   sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /etc/default/
   grub
   ```

   c. Erstellen Sie die neue Grub-Konfigurationsdatei.

   ```
   sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

7. [EBS-gestützte Instance] Stoppen Sie die Instance von Ihrem lokalen Computer aus mithilfe der EC2 Amazon-Konsole oder mit einem der folgenden Befehle: stop-instances(AWS CLI), Stop-EC2Instance(AWS Tools for Windows PowerShell).

[In einem Instance-Speicher gesicherte Instance] Sie können die Instance nicht anhalten, um das Attribut zu ändern. Gehen Sie stattdessen wie folgt vor: So aktivieren Sie Enhanced Networking unter Linux (Instance-Speicher-gestützte Instances):.

8. Aktivieren Sie auf Ihrem lokalen Computer das Enhanced Networking-Attribut `enaSupport` mit einem der folgenden Befehle:

   - modify-instance-attribute (AWS CLI)

     ```
     aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --ena-support
     ```

   - Edit-EC2InstanceAttribute(Tools für Windows) PowerShell

     ```
     Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -EnaSupport $true
     ```

9. (Optional) Erstellen Sie ein AMI von der Instance, wie unter Ein Amazon-EBS-gestütztes AMI erstellen beschrieben. Das AMI erbt das Enhanced Networking-Attribut `enaSupport` von der Instance. D. h. Sie können mit diesem AMI eine andere Instance starten, in der Enhanced Networking standardmäßig aktiviert ist.

   Wenn Ihr Instance-Betriebssystem eine `/etc/udev/rules.d/70-persistent-net.rules`-Datei enthält, müssen Sie diese vor der Erstellung des AMI löschen. Diese Datei enthält die MAC-Adresse des Ethernet-Adapters in der ursprünglichen Instance. Wenn eine andere Instance mit dieser Datei gestartet wird, kann das Betriebssystem das Gerät nicht finden und von `eth0` schlägt möglicherweise fehl, was zu Problemen beim Start führt. Diese Datei wird während des nächsten Bootvorgangs neu generiert, und jede aus dem AMI gestartete Instance erstellt eine eigene Version der Datei.

10. Starten Sie die Instance von Ihrem lokalen Computer aus mit der EC2 Amazon-Konsole oder einem der folgenden Befehle: start-instances(AWS CLI) oder Start-EC2Instance(AWS Tools for Windows PowerShell).

11. (Optional) Stellen Sie eine Verbindung mit Ihrer Instance her und überprüfen Sie, ob der Kernel-Treiber installiert wurde.

    Wenn Sie nach der Aktivierung von Enhanced Networking keine Verbindung zu Ihrer Instance herstellen können, informieren Sie sich unter Problembehandlung beim ENA-Kernel-Treiber in Linux.

So aktivieren Sie Enhanced Networking unter Linux (Instance-Speicher-gestützte Instances):

Führen Sie die Schritte aus dem vorherigen Verfahren durch bis zu dem Schritt, in dem die Instance angehalten wird. Erstellen Sie ein neues AMI, wie in Ein Amazon-S3-gestütztes AMI erstellen beschreiben, um sicherzustellen, dass Sie das Enhanced Networking-Attribut aktivieren, wenn Sie das AMI registrieren.

- register-image (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport ...
```

Ubuntu mit DKMS

Diese Methode ist nur für Test- und Feedbackzwecke. Sie ist nicht für die Nutzung mit Produktionsbereitstellungen gedacht. Für Produktionsbereitstellungen siehe Ubuntu.

> **Important**
>
> Bei Verwendung von DKMS wird die Supportvereinbarung für Ihr Abonnement unwirksam. Es sollte nicht für Produktionsbereitstellungen verwendet werden.

So aktivieren Sie Enhanced Networking mit ENA unter Ubuntu (EBS-gestützte Instances)

1. Führen Sie die Schritte 1 und 2 unter Ubuntu aus.
2. Installieren Sie die `build-essential`-Pakete zum Kompilieren des Kernel-Treibers und das `dkms`-Paket, damit Ihr `ena`-Modul bei jeder Aktualisierung des Kernels neu erstellt wird.

   ```
   ubuntu:~$ sudo apt-get install -y build-essential dkms
   ```

3. Klonen Sie die Quelle für den `ena` Kernel-Treiber auf Ihrer Instance von GitHub at aushttps://github.com/amzn/amzn-drivers.

   ```
   ubuntu:~$ git clone https://github.com/amzn/amzn-drivers
   ```

4. Verschieben Sie das `amzn-drivers`-Paket in das Verzeichnis `/usr/src/`, sodass es von DKMS gefunden und bei jedem Kernel-Update neu erstellt wird. Fügen Sie die Versionsnummer des Quellcodes an den Verzeichnisnamen an (Sie finden die aktuelle Versionsnummer in den Versionshinweisen). Im folgenden Beispiel wird Version `1.0.0` angezeigt.

```
ubuntu:~$ sudo mv amzn-drivers /usr/src/amzn-drivers-1.0.0
```

5. Erstellen Sie eine DKMS-Konfigurationsdatei mit den folgenden Werten. Geben Sie dabei Ihre `ena`-Version an.

   Erstellen Sie die Datei.

```
ubuntu:~$ sudo touch /usr/src/amzn-drivers-1.0.0/dkms.conf
```

   Öffnen Sie die Datei und fügen Sie die folgenden Werte hinzu.

```
ubuntu:~$ sudo vim /usr/src/amzn-drivers-1.0.0/dkms.conf
PACKAGE_NAME="ena"
PACKAGE_VERSION="1.0.0"
CLEAN="make -C kernel/linux/ena clean"
MAKE="make -C kernel/linux/ena/ BUILD_KERNEL=${kernelver}"
BUILT_MODULE_NAME[0]="ena"
BUILT_MODULE_LOCATION="kernel/linux/ena"
DEST_MODULE_LOCATION[0]="/updates"
DEST_MODULE_NAME[0]="ena"
AUTOINSTALL="yes"
```

6. Verwenden Sie DKMS, um den `ena`-Kernel-Treiber in der Instance hinzuzufügen, zu erstellen und zu installieren.

   Den Kernel-Treiber DKMS hinzufügen.

```
ubuntu:~$ sudo dkms add -m amzn-drivers -v 1.0.0
```

   Erstellen Sie den Kernel-Treiber mit dem dkms-Befehl.

```
ubuntu:~$ sudo dkms build -m amzn-drivers -v 1.0.0
```

   Installieren Sie den Kernel-Treiber mit dkms.

```
ubuntu:~$ sudo dkms install -m amzn-drivers -v 1.0.0
```

7. Erstellen Sie `initramfs` neu, damit der richtige Kernel-Treiber während des Bootvorgangs geladen wird.

```
ubuntu:~$ sudo update-initramfs -u -k all
```

8. Stellen Sie sicher, dass der `ena`-Kernel-Treiber installiert ist. Verwenden Sie dafür den Befehl „modinfo ena“ von Testen, ob Enhanced Networking aktiviert ist.

```
ubuntu:~$ modinfo ena
filename:    /lib/modules/3.13.0-74-generic/updates/dkms/ena.ko
version:  1.0.0
license:  GPL
description: Elastic Network Adapter (ENA)
author:   Amazon.com, Inc. or its affiliates
srcversion:  9693C876C54CA64AE48F0CA
alias:    pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
vermagic:    3.13.0-74-generic SMP mod_unload modversions
parm:     debug:Debug level (0=none,...,16=all) (int)
parm:     push_mode:Descriptor / header push mode (0=automatic,1=disable,3=enable)
    0 - Automatically choose according to device capability (default)
    1 - Don't push anything to device memory
    3 - Push descriptors and header buffer to device memory (int)
parm:     enable_wd:Enable keepalive watchdog (0=disable,1=enable,default=1) (int)
parm:     enable_missing_tx_detection:Enable missing Tx completions. (default=1)
 (int)
parm:     numa_node_override_array:Numa node override map
(array of int)
parm:     numa_node_override:Enable/Disable numa node override (0=disable)
(int)
```

9. Fahren Sie mit Schritt 3 in Ubuntu fort.

Aktivieren von Enhanced Networking unter Windows

Wenn Sie Ihre Instance gestartet haben und Enhanced Networking noch nicht aktiviert wurde, müssen Sie den erforderlichen Netzwerkadaptertreiber herunterladen und in der Instance installieren sowie anschließend das `enaSupport`-Instance-Attribut setzen, um die optimierte Netzwerkleistung zu erzielen.

Aktivieren von Enhanced Networking

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
2. [Nur Windows Server 2016 und 2019] Führen Sie das folgende EC2 PowerShell Startskript aus, um die Instanz zu konfigurieren, nachdem der Treiber installiert wurde.

   ```
   PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
   ```

3. Installieren Sie den Treiber in der Instance, indem Sie wie folgt vorgehen:

   a. Laden Sie den aktuellen Treiber in die Instance herunter.

   b. Extrahieren Sie die ZIP-Datei.

   c. Installieren Sie den Treiber, indem Sie das `install.ps1` PowerShell Skript ausführen.

   > **Note**
   >
   > Wenn ein Fehler der Ausführungsrichtlinie gemeldet wird, weisen Sie der Richtlinie `Unrestricted` zu (standardmäßig ist `Restricted` oder `RemoteSigned` zugewiesen). Führen Sie das `install.ps1` PowerShell Skript in einer Befehlszeile aus`Set-ExecutionPolicy -ExecutionPolicy Unrestricted`, und führen Sie es dann erneut aus.

4. Stoppen Sie die Instance auf Ihrem lokalen Computer mithilfe der EC2 Amazon-Konsole oder mit einem der folgenden Befehle: stop-instances(AWS CLI) oder Stop-EC2Instance(AWS Tools for Windows PowerShell).
5. Aktivieren Sie die ENA-Unterstützung in Ihrer Instance wie folgt:

   a. Überprüfen Sie von Ihrem lokalen Computer aus das EC2 ENA-Supportattribut der Instance auf Ihrer Instance, indem Sie einen der folgenden Befehle ausführen. Wenn das

Attribut nicht aktiviert ist, wird „[]" oder ein leeres Feld zurückgegeben. `EnaSupport` ist standardmäßig auf `false` festgelegt.

- describe-instances (AWS CLI)

```
aws ec2 describe-instances --instance-ids i-1234567890abcdef0 --query
 "Reservations[].Instances[].EnaSupport"
```

- Get-EC2Instance(Tools für Windows PowerShell)

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.EnaSupport
```

b. Führen Sie zur Aktivierung der ENA-Unterstützung einen der folgenden Befehle aus:

- modify-instance-attribute (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --ena-
support
```

- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -EnaSupport $true
```

Wenn beim Neustarten der Instance Probleme auftreten, können Sie die ENA-Unterstützung auch über einen der folgenden Befehle deaktivieren:

- modify-instance-attribute (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --no-ena-
support
```

- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -EnaSupport $false
```

c. Stellen Sie sicher, dass das Attribut auf `true` gesetzt wurde, indem Sie den Befehl describe-instances oder Get-EC2Instance wie oben gezeigt ausführen. Die Ausgabe sollte hetzt folgendermaßen aussehen:

```
[
```

```
 true
]
```

6. Starten Sie die Instance von Ihrem lokalen Computer aus mit der EC2 Amazon-Konsole oder einem der folgenden Befehle: start-instances(AWS CLI) oder Start-EC2Instance(AWS Tools for Windows PowerShell).
7. Prüfen Sie auf der Instance, wie folgt ob der ENA-Treiber installiert und aktiviert ist:
   a. Klicken Sie mit der rechten Maustaste auf das Netzwerksymbol und wählen Sie Open Network and Sharing Center aus.
   b. Wählen Sie den Ethernet-Adapter aus (z. B. Ethernet 2).
   c. Wählen Sie Details aus. Prüfen Sie unter Network Connection Details, ob Description den Wert Amazon Elastic Network Adapter hat.
8. (Optional) Erstellen Sie aus der Instance ein AMI. Das AMI übernimmt das `enaSupport`-Attribute von der Instance. D. h. Sie können mit diesem AMI eine andere Instance starten, in der ENA standardmäßig aktiviert ist.

ENA-Warteschlangen

ENA-Warteschlangen werden Netzwerkschnittstellen mit standardmäßigen statischen Grenzwerten zugewiesen, die auf dem Instance-Typ und der Größe der Instance basieren. Bei unterstützten Instance-Typen können Sie diese Warteschlangen dynamisch den Elastic Network Interfaces zuweisen ()ENIs. Die Gesamtzahl der Warteschlangen pro Instance hängt zwar von ihrem Typ und ihrer Größe ab, Sie können jedoch mehrere ENIs mit ENA-Warteschlangen konfigurieren, bis Sie die maximale Warteschlangenanzahl für die ENI und die Instance erreicht haben.

Die flexible ENA-Warteschlangenzuweisung optimiert die Ressourcenverteilung und ermöglicht so eine maximale vCPU-Auslastung. Workloads mit hoher Netzwerkleistung erfordern in der Regel mehrere ENA-Warteschlangen. Sie können die Netzwerkleistung und die Pakete pro Sekunde (PPS) optimieren, indem Sie die Anzahl der Warteschlangen an Ihre spezifischen Workload-Anforderungen anpassen. Beispielsweise benötigen netzwerkintensive Anwendungen möglicherweise mehr Warteschlangen als CPU-intensive Anwendungen.

Topics

- Unterstützte Instances
- Die Anzahl der Warteschlangen ändern

Unterstützte Instances

Die folgenden Instances unterstützen die dynamische Zuweisung mehrerer ENA-Warteschlangen.

Allgemeine Zwecke

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
	M6i		
m6i.large	2	2	6
m6i.xlarge	4	4	16
m6i.2xlarge	8	8	32
m6i.4xlarge	8	16	64
m6i.8xlarge	8	32	64
m6i.12xlarge	8	32	64
m6i.16xlarge	8	32	120
m6i.24xlarge	8	32	120
m6i.32xlarge	8	32	120
	M6 ID		
m6id.large	2	2	6
m6id.xlarge	4	4	16
m6id.2xlarge	8	8	32
m6id.4xlarge	8	16	64
m6id.8xlarge	8	32	64

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
m6id.12xlarge	8	32	64
m6id.16xlarge	8	32	120
m6id.24xlarge	8	32	120
m6id.32xlarge	8	32	120
M6 IDN			
m6idn.large	2	2	6
m6idn.xlarge	4	4	16
m6idn.2xlarge	8	8	32
m6idn.4xlarge	8	16	64
m6idn.8xlarge	16	32	128
m6idn.12xlarge	16	32	128
m6idn.16xlarge	16	32	240
m6idn.24xlarge	32	32	480
m6idn.32xlarge	32	32	512 *
M 6 Zoll			
m6in.large	2	2	6
m6in.xlarge	4	4	16
m6in.2xlarge	8	8	32
m6in.4xlarge	8	16	64

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
m6in.8xlarge	16	32	128
m6in.12xlarge	16	32	128
m6in.16xlarge	16	32	240
m6in.24xlarge	32	32	480
m6in.32xlarge	32	32	512 *
M8a			
m8a.medium	1	1	3
m8a.large	2	2	6
m8a.xlarge	4	4	16
m8a.2xlarge	8	8	32
m8a.4xlarge	8	16	64
m8a.8xlarge	8	32	128
m8a.12xlarge	16	64	192
m8a.16xlarge	16	64	256
m8a.24xlarge	16	128	384
m8a.48xlarge	32	128	768
m8a.metal-24xl	16	128	384
m8a.metal-48xl	32	128	768
M8i			

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
m8i.large	2	2	6
m8i.xlarge	4	4	16
m8i.2xlarge	8	8	32
m8i.4xlarge	8	16	64
m8i.8xlarge	8	32	128
m8i.12xlarge	16	64	192
m8i.16xlarge	16	64	256
m8i.24xlarge	16	128	384
m8i.32xlarge	16	128	512
m8i.48xlarge	32	128	768
m8i.96xlarge	32	128	1536
m8i.metal-48xl	32	128	768
m8i.metal-96xl	32	128	1536
M8 i-Flex			
m8i-flex.large	1	1	3
m8i-flex.xlarge	2	2	8
m8i-flex.2xlarge	4	4	16
m8i-flex.4xlarge	4	8	32
m8i-flex.8xlarge	4	16	64

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
m8i-flex.12xlarge	8	32	96
m8i-flex.16xlarge	8	32	128

> **Note**
>
> * Diese Instance-Typen verfügen über mehrere Netzwerkkarten. Andere Instance-Typen verfügen über eine einzelne Netzwerkkarte. Weitere Informationen finden Sie unter Netzwerkkarten.

Für Datenverarbeitung optimiert

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
	C6i		
c6i.large	2	2	6
c6i.xlarge	4	4	16
c6i.2xlarge	8	8	32
c6i.4xlarge	8	16	64
c6i.8xlarge	8	32	64
c6i.12xlarge	8	32	64
c6i.16xlarge	8	32	120
c6i.24xlarge	8	32	120

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
c6i.32xlarge	8	32	120
C6id			
c6id.large	2	2	6
c6id.xlarge	4	4	16
c6id.2xlarge	8	8	32
c6id.4xlarge	8	16	64
c6id.8xlarge	8	32	64
c6id.12xlarge	8	32	64
c6id.16xlarge	8	32	120
c6id.24xlarge	8	32	120
c6id.32xlarge	8	32	120
C6 Zoll			
c6in.large	2	2	6
c6in.xlarge	4	4	16
c6in.2xlarge	8	8	32
c6in.4xlarge	8	16	64
c6in.8xlarge	16	32	128
c6in.12xlarge	16	32	128
c6in.16xlarge	16	32	240

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
c6in.24xlarge	32	32	480
c6in.32xlarge	32	32	512 *
C8a			
c8a.medium	1	1	3
c8a.large	2	2	6
c8a.xlarge	4	4	16
c8a.2xlarge	8	8	32
c8a.4xlarge	8	16	64
c8a.8xlarge	8	32	128
c8a.12xlarge	16	64	192
c8a.16xlarge	16	64	256
c8a.24xlarge	16	128	384
c8a.48xlarge	32	128	768
c8a.metal-24xl	16	128	384
c8a.metal-48xl	32	128	768
C 8 GB			
c8gb.medium	1	1	2
c8gb.large	2	2	6
c8gb.xlarge	4	4	16

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
c8gb.2xlarge	8	8	32
c8gb.4xlarge	8	16	64
c8gb.8xlarge	8	32	128
c8gb.12xlarge	16	64	192
c8gb.16xlarge	16	64	256
c8gb.24xlarge	16	128	384
c8gb.metal-24xl	32	128	768
C8gn			
c8gn.medium	1	1	2
c8gn.large	2	2	6
c8gn.xlarge	4	4	16
c8gn.2xlarge	8	8	32
c8gn.4xlarge	8	16	64
c8gn.8xlarge	8	32	128
c8gn.12xlarge	16	64	192
c8gn.16xlarge	16	64	256
c8gn.24xlarge	16	128	384
c8gn.48xlarge	32	128	768 *
c8gn.metal-24xl	32	128	768

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
c8gn.metal-48xl	32	128	768 *
C8i			
c8i.large	2	2	6
c8i.xlarge	4	4	16
c8i.2xlarge	8	8	32
c8i.4xlarge	8	16	64
c8i.8xlarge	8	32	128
c8i.12xlarge	16	64	192
c8i.16xlarge	16	64	256
c8i.24xlarge	16	128	384
c8i.32xlarge	16	128	512
c8i.48xlarge	32	128	768
c8i.96xlarge	32	128	1536
c8i.metal-48xl	32	128	768
c8i.metal-96xl	32	128	1536
C8i-flex			
c8i-flex.large	1	1	3
c8i-flex.xlarge	2	2	8
c8i-flex.2xlarge	4	4	16

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
c8i-flex.4xlarge	4	8	32
c8i-flex.8xlarge	4	16	64
c8i-flex.12xlarge	8	32	96
c8i-flex.16xlarge	8	32	128

> **Note**
>
> * Diese Instance-Typen verfügen über mehrere Netzwerkkarten. Andere Instance-Typen verfügen über eine einzelne Netzwerkkarte. Weitere Informationen finden Sie unter Netzwerkkarten.

Arbeitsspeicher optimiert

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
	R6i		
r6i.large	2	2	6
r6i.xlarge	4	4	16
r6i.2xlarge	8	8	32
r6i.4xlarge	8	16	64
r6i.8xlarge	8	32	64
r6i.12xlarge	8	32	64

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
r6i.16xlarge	8	32	120
r6i.24xlarge	8	32	120
r6i.32xlarge	8	32	120
R6id			
r6id.large	2	2	6
r6id.xlarge	4	4	16
r6id.2xlarge	8	8	32
r6id.4xlarge	8	16	64
r6id.8xlarge	8	32	64
r6id.12xlarge	8	32	64
r6id.16xlarge	8	32	120
r6id.24xlarge	8	32	120
r6id.32xlarge	8	32	120
R 6 i DN			
r6idn.large	2	2	6
r6idn.xlarge	4	4	16
r6idn.2xlarge	8	8	32
r6idn.4xlarge	8	16	64
r6idn.8xlarge	16	32	128

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
r6idn.12xlarge	16	32	128
r6idn.16xlarge	16	32	240
r6idn.24xlarge	32	32	480
r6idn.32xlarge	32	32	512 *
R 6 Zoll			
r6in.large	2	2	6
r6in.xlarge	4	4	16
r6in.2xlarge	8	8	32
r6in.4xlarge	8	16	64
r6in.8xlarge	16	32	128
r6in.12xlarge	16	32	128
r6in.16xlarge	16	32	240
r6in.24xlarge	32	32	480
r6in.32xlarge	32	32	512 *
R8a			
r8a.medium	1	1	3
r8a.large	2	2	6
r8a.xlarge	4	4	16
r8a.2xlarge	8	8	32

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
r8a.4xlarge	8	16	64
r8a.8xlarge	8	32	128
r8a.12xlarge	16	64	192
r8a.16xlarge	16	64	256
r8a.24xlarge	16	128	384
r8a.48xlarge	32	128	768
r8a.metal-24xl	16	128	384
r8a.metal-48xl	32	128	768
R8gb			
r8gb.medium	1	1	2
r8gb.large	2	2	6
r8gb.xlarge	4	4	16
r8gb.2xlarge	8	8	32
r8gb.4xlarge	8	16	64
r8gb.8xlarge	8	32	128
r8gb.12xlarge	16	64	192
r8gb.16xlarge	16	64	256
r8gb.24xlarge	16	128	384
r8gb.metal-24xl	32	128	768

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
R8gn			
r8gn.medium	1	1	2
r8gn.large	2	2	6
r8gn.xlarge	4	4	16
r8gn.2xlarge	8	8	32
r8gn.4xlarge	8	16	64
r8gn.8xlarge	8	32	128
r8gn.12xlarge	16	64	192
r8gn.16xlarge	16	64	256
r8gn.24xlarge	16	128	384
r8gn.48xlarge	32	128	768 *
r8gn.metal-24xl	32	128	768
r8gn.metal-48xl	32	128	768 *
R8i			
r8i.large	2	2	6
r8i.xlarge	4	4	16
r8i.2xlarge	8	8	32
r8i.4xlarge	8	16	64
r8i.8xlarge	8	32	128

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
r8i.12xlarge	16	64	192
r8i.16xlarge	16	64	256
r8i.24xlarge	16	128	384
r8i.32xlarge	16	128	512
r8i.48xlarge	32	128	768
r8i.96xlarge	32	128	1536
r8i.metal-48xl	32	128	768
r8i.metal-96xl	32	128	1536
R8i-flex			
r8i-flex.large	1	1	3
r8i-flex.xlarge	2	2	8
r8i-flex.2xlarge	4	4	16
r8i-flex.4xlarge	4	8	32
r8i-flex.8xlarge	4	16	64
r8i-flex.12xlarge	8	32	96
r8i-flex.16xlarge	8	32	128
x 8 AEDZ			
x8aedz.large	2	2	8
x8aedz.xlarge	4	4	16

Instance-Typ	Standard-ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Schnittstelle	Maximale ENA-Warteschlangen pro Instance
x8aedz.3xlarge	4	16	48
x8aedz.6xlarge	8	32	96
x8aedz.12xlarge	8	64	192
x8aedz.24xlarge	16	128	384
x8aedz.metal-12xl	8	64	192
x8aedz.metal-24xl	16	128	384

Note

* Diese Instance-Typen verfügen über mehrere Netzwerkkarten. Andere Instance-Typen verfügen über eine einzelne Netzwerkkarte. Weitere Informationen finden Sie unter Netzwerkkarten.

Die Anzahl der Warteschlangen ändern

Sie können die Anzahl der ENA-Warteschlangen mit oder ändern. AWS-Managementkonsole AWS CLI In der AWS-Managementkonsole ist die ENA-Warteschlangenkonfiguration unter jeder Netzwerkschnittstellen-Einstellung verfügbar.

Verwenden Sie einen der folgenden Befehle AWS CLI, um die Anzahl der ENA-Warteschlangen mithilfe von zu ändern. Bevor Sie die Anzahl der Warteschlangen ändern, überprüfen Sie mit dem folgenden Befehl Ihre aktuelle Warteschlangenanzahl.

```
aws ec2 describe-instances --instance-id i-1234567890abcdef0
```

> **Note**
>
> - Ihre Instance muss angehalten werden, damit die Anzahl der ENA-Warteschlangen geändert werden kann.
> - Der Wert für ENA-Warteschlangen muss eine Zweierpotenz sein, z. B. 1, 2, 4, 8, 16, 32 usw.
> - Die Anzahl der Warteschlangen, die einer einzelnen ENI zugewiesen sind, darf die Anzahl der auf Ihrer Instance CPUs verfügbaren v nicht überschreiten.

attach-network-interface

Im folgenden Beispiel sind 32 ENA-Warteschlangen auf einer ENI konfiguriert.

```
aws ec2 attach-network-interface \
  --network-interface-id eni-001aa1bb223cdd4e4 \
  --instance-id i-1234567890abcdef0 \
  --device-index 1 \
  --ena-queue-count 32
```

run-instances

Im folgenden Beispiel sind jeweils 2 ENA-Warteschlangen auf 3 konfiguriert. ENIs

```
aws ec2 run-instances \
  --image-id ami-12ab3c30 \
  --instance-type c6i.large \
  --min-count 1 \
  --max-count 1 \
  --network-interfaces \
    "[{\"DeviceIndex\":0,\"SubnetId\":\"subnet-123456789012a345a\",\"EnaQueueCount
\":2},
      {\"DeviceIndex\":1,\"SubnetId\":\"subnet-123456789012a345a\",\"EnaQueueCount
\":2},
      {\"DeviceIndex\":2,\"SubnetId\":\"subnet-123456789012a345a\",\"EnaQueueCount
\":2}]"
```

modify-network-interface-attribute

Im folgenden Beispiel sind 32 ENA-Warteschlangen auf einer ENI konfiguriert.

```
aws ec2 modify-network-interface-attribute \
--network-interface-id eni-1234567890abcdef0 \
--attachment AttachmentId=eni-attach-12345678,EnaQueueCount=32
```

Im folgenden Beispiel wird die ENA-Anzahl auf den Standardwert zurückgesetzt.

```
aws ec2 modify-network-interface-attribute \
--network-interface-id eni-1234567890abcdef0 \
--attachment AttachmentId=eni-attach-12345678,DefaultEnaQueueCount=true
```

Problembehandlung beim ENA-Kernel-Treiber in Linux

Der Elastic Network Adapter (ENA) soll die Integrität des Betriebssystems verbessern und mögliche langfristige Störungen aufgrund von unerwartetem Hardwareverhalten oder Fehlern verringern. In der ENA-Architektur bleiben Geräte- oder Treiberfehler für das System weitestgehend transparent. Dieses Thema enthält Informationen zur Fehlerbehebung für ENA.

Beginnen Sie mit Abschnitt Fehlerbehebung bei Verbindungsproblemen, wenn Sie keine Verbindung mit Ihrer Instance herstellen können.

Wenn Sie nach der Migration auf einen Instance-Typ der sechsten Generation eine Leistungsverschlechterung feststellen, lesen Sie den Artikel Was muss ich tun, bevor ich meine EC2-Instance auf eine Instance der sechsten Generation migriere, um sicherzustellen, dass ich die maximale Netzwerkleistung erhalte?

Wenn Sie eine Verbindung mit Ihrer Instance herstellen können, können Sie mithilfe der Fehlererkennungs- und Wiederherstellungsmechanismen Diagnose-Informationen sammeln. Ausführliche Informationen zu diesen Mechanismen finden Sie in den weiteren Abschnitten dieses Themas.

Inhalt

- Fehlerbehebung bei Verbindungsproblemen
- Keep-Alive-Mechanismus
- Timeout für Registerlesevorgänge
- Statistiken
- Treiberfehlerprotokolle im syslog
- Benachrichtigungen zur suboptimalen Konfiguration

Fehlerbehebung bei Verbindungsproblemen

Wenn die Verbindung bei der Aktivierung des Enhanced Networking verloren geht, ist das `ena`-Modul u. U. nicht mit der Kernelversion Ihrer Instance kompatibel. Dies geschieht z .B. dann, wenn Sie das Modul für eine bestimmte Kernelversion (ohne Befehl dkms oder mit einer falsch konfigurierten dkms.conf-Datei) installieren und Ihr Instance-Kernel anschließend aktualisiert wird. Wenn der beim Start geladene Instance-Kernel nicht über ein richtig installiertes `ena`-Modul verfügt, erkennt Ihre Instance den Netzwerkadapter nicht und Ihre Instance ist nicht erreichbar.

Wenn Sie Enhanced Networking für eine PV-Instance oder ein AMI aktivieren, kann es ebenfalls vorkommen, dass Ihre Instance nicht erreichbar ist.

Wenn Ihre Instance nach dem Aktivieren von Enhanced Networking mit ENA nicht erreichbar ist, können Sie das Attribut `enaSupport` für Ihre Instance deaktivieren, damit diese wieder den üblichen Netzwerkadapter nutzt.

So deaktivieren Sie Enhanced Networking mit ENA (EBS-gestützte Instances)

1. Halten Sie die Instance auf Ihrem lokalen Computer an, indem Sie die Amazon-EC2-Konsole, den Befehl stop-instances (AWS CLI) oder das cmdlet Stop-EC2Instance (AWS -Tools für PowerShell) verwenden.
2. Deaktivieren Sie auf Ihrem lokalen Computer das erweiterte Netzwerkattribut, indem Sie den Befehl modify-instance-attribute mit der Option `--no-ena-support` oder das cmdlet Edit-EC2InstanceAttribute mit dem Parameter `-EnaSupport $false` verwenden.
3. Starten Sie die Instance auf Ihrem lokalen Computer, indem Sie die Amazon-EC2-Konsole, den Befehl start-instances oder das cmdlet Start-EC2Instance verwenden.
4. (Optional) Stellen Sie eine Verbindung mit Ihrer Instance her und versuchen Sie, das Modul `ena` erneut mit Ihrer aktuellen Kernelversion zu installieren, indem Sie die entsprechenden Schritte unter Ermöglichen Sie Enhanced Networking mit ENA auf Ihren EC2 Instances ausführen.

So deaktivieren Sie Enhanced Networking mit ENA (Instance Store-Backed Instances)

1. Erstellen Sie ein neues AMI, wie unter Ein Amazon-S3-gestütztes AMI erstellen beschrieben.
2. Achten Sie bei der Registrierung des AMI darauf, die Option `--no-ena-support` in den Befehl stop-instances (AWS CLI) oder den `-EnaSupport $false`-Parameter in das cmdlet Register-EC2Image aufzunehmen.

Keep-Alive-Mechanismus

Das ENA-Gerät sendet Keep-Alive-Ereignisse in einem bestimmten Zeitintervall (i. d. R. einmal pro Sekunde). Der ENA-Treiber implementiert einen Überwachungsmechanismus, der regelmäßig nach allen Keep-Alive-Nachrichten sucht. Wenn eine oder mehrere Nachrichten vorhanden sind, wird der Überwachungsmechanismus wieder aktiviert. Andernfalls geht der Treiber davon aus, dass ein Gerätefehler vorliegt, und ergreift folgende Maßnahmen:

- Er legt seine aktuellen Statistiken unter syslog ab.
- Er setzt das ENA-Gerät zurück.
- Er setzt den ENA-Treiberstatus zurück.

Der obige Zurücksetzungsvorgang kann kurzzeitig zu einem Traffic-Verlust führen (TCP-Verbindungen können i. d. R. wiederhergestellt werden), der aber keine weiteren Auswirkungen für den Benutzer haben sollte.

Das ENA-Gerät fordert u. U. indirekt eine Gerätezurücksetzung an, indem keine Keep-Alive-Benachrichtigung gesendet wird, z. B. wenn das ENA-Gerät nach dem Laden einer nicht wiederherstellbaren Konfiguration in einen unbekannten Status versetzt wird.

Das folgende Beispiel zeigt den Vorgang des Zurücksetzens:

```
[18509.800135] ena 0000:00:07.0 eth1: Keep alive watchdog timeout. // The watchdog
 process initiates a reset
[18509.815244] ena 0000:00:07.0 eth1: Trigger reset is on
[18509.825589] ena 0000:00:07.0 eth1: tx_timeout: 0 // The driver logs the current
 statistics
[18509.834253] ena 0000:00:07.0 eth1: io_suspend: 0
[18509.842674] ena 0000:00:07.0 eth1: io_resume: 0
[18509.850275] ena 0000:00:07.0 eth1: wd_expired: 1
[18509.857855] ena 0000:00:07.0 eth1: interface_up: 1
[18509.865415] ena 0000:00:07.0 eth1: interface_down: 0
[18509.873468] ena 0000:00:07.0 eth1: admin_q_pause: 0
[18509.881075] ena 0000:00:07.0 eth1: queue_0_tx_cnt: 0
[18509.888629] ena 0000:00:07.0 eth1: queue_0_tx_bytes: 0
[18509.895286] ena 0000:00:07.0 eth1: queue_0_tx_queue_stop: 0
.......
........
[18511.280972] ena 0000:00:07.0 eth1: free uncompleted tx skb qid 3 idx 0x7 // At the
 end of the down process, the driver discards incomplete packets.
```

```
[18511.420112] [ENA_COM: ena_com_validate_version] ena device version: 0.10 //The
 driver begins its up process
[18511.420119] [ENA_COM: ena_com_validate_version] ena controller version: 0.0.1
 implementation version 1
[18511.420127] [ENA_COM: ena_com_admin_init] ena_defs : Version:[b9692e8] Build date
 [Wed Apr  6 09:54:21 IDT 2016]
[18512.252108] ena 0000:00:07.0: Device watchdog is Enabled
[18512.674877] ena 0000:00:07.0: irq 46 for MSI/MSI-X
[18512.674933] ena 0000:00:07.0: irq 47 for MSI/MSI-X
[18512.674990] ena 0000:00:07.0: irq 48 for MSI/MSI-X
[18512.675037] ena 0000:00:07.0: irq 49 for MSI/MSI-X
[18512.675085] ena 0000:00:07.0: irq 50 for MSI/MSI-X
[18512.675141] ena 0000:00:07.0: irq 51 for MSI/MSI-X
[18512.675188] ena 0000:00:07.0: irq 52 for MSI/MSI-X
[18512.675233] ena 0000:00:07.0: irq 53 for MSI/MSI-X
[18512.675279] ena 0000:00:07.0: irq 54 for MSI/MSI-X
[18512.772641] [ENA_COM: ena_com_set_hash_function] Feature 10 isn't supported
[18512.772647] [ENA_COM: ena_com_set_hash_ctrl] Feature 18 isn't supported
[18512.775945] ena 0000:00:07.0: Device reset completed successfully // The reset
 process is complete
```

Timeout für Registerlesevorgänge

Bei der ENA-Architektur kommt es nur zu einer begrenzten Nutzung von im Speicher abgebildeten I/O-Lesevorgängen (MMIO). Der ENA-Treiber greift nur während seines Initialisierungsvorgangs auf MMIO-Register zu.

Wenn die Treiberprotokolle (verfügbar in der dmesg-Ausgabe) Fehler bei Lesevorgängen ausgeben, kann die Ursache ein nicht kompatibler oder falsch kompilierter Treiber, ein ausgelastetes Hardwaregerät oder einen Hardwarefehler sein.

Intermittierende Protokolleinträge, die auf Fehler bei Lesevorgängen hinweisen, stellen i. d. R. kein Problem dar. Der Treiber führt dafür in diesem Fall einen neuen Versuch durch. Eine Reihe von Protokolleinträgen mit Lesefehlern deuten jedoch auf ein Treiber- oder Hardwareproblem hin.

Nachfolgend finden Sie ein Beispiel für einen Treiber-Protokolleintrag, der auf einen Lesevorgangsfehler aufgrund eines Timeouts hindeutet:

```
[ 47.113698] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[1] offset[88] actual: req id[57006] offset[0]
[ 47.333715] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[2] offset[8] actual: req id[57007] offset[0]
```

```
[ 47.346221] [ENA_COM: ena_com_dev_reset] Reg read32 timeout occurred
```

Statistiken

Falls eine unzureichende Netzwerkleistung oder Latenzprobleme auftreten, sollten Sie die Gerätestatistiken aufrufen und überprüfen. Diese Statistiken können Sie mithilfe von ethtool wie folgt aufrufen.

```
[ec2-user ~]$ ethtool -S ethN
NIC statistics:
 tx_timeout: 0
 suspend: 0
 resume: 0
 wd_expired: 0
 interface_up: 1
 interface_down: 0
 admin_q_pause: 0
 bw_in_allowance_exceeded: 0
 bw_out_allowance_exceeded: 0
 pps_allowance_exceeded: 0
 conntrack_allowance_available: 450878
 conntrack_allowance_exceeded: 0
 linklocal_allowance_exceeded: 0
 queue_0_tx_cnt: 4329
 queue_0_tx_bytes: 1075749
 queue_0_tx_queue_stop: 0
 ...
```

Unten sind die folgenden Befehlsausgabeparameter beschrieben:

`tx_timeout`: *N*

Gibt an, wie oft der Netdev-Überwachungsmechanismus aktiviert wurde.

`suspend`: *N*

Gibt an, wie oft der Treiber eine Aussetzung durchgeführt hat.

`resume`: *N*

Gibt an, wie oft der Treiber eine Wiederaufnahme durchgeführt hat.

`wd_expired`: *N*

Gibt an, wie oft der Treiber in den letzten drei Sekunden kein Keep-Alive-Ereignis empfangen hat.

`interface_up`: *N*

Gibt an, wie oft die ENA-Schnittstelle aufgerufen wurde.

`interface_down`: *N*

Gibt an, wie oft die ENA-Schnittstelle heruntergefahren wurde.

`admin_q_pause`: *N*

Gibt an, wie oft die Admin-Warteschlange nicht in einem laufenden Zustand gefunden wurde.

`bw_in_allowance_exceeded`: *N*

Die Anzahl der Pakete, die in die Warteschlange gestellt oder verworfen wurden, da die eingehende aggregierte Bandbreite das Maximum für die Instance überschritten hat.

`bw_out_allowance_exceeded`: *N*

Die Anzahl der Pakete, die in die Warteschlange gestellt oder verworfen wurden, weil die ausgehende aggregierte Bandbreite das Maximum für die Instance überschritten hat.

`pps_allowance_exceeded`: *N*

Die Anzahl der Pakete, die in die Warteschlange gestellt oder verworfen wurden, weil die bidirektionale PPS das Maximum für die Instance überschritten hat. *

`conntrack_allowance_available`: *N*

Die Anzahl der nachverfolgten Verbindungen, die von der Instance hergestellt werden können, bevor die zulässige Anzahl nachverfolgter Verbindungen dieses Instance-Typs erreicht wird. Nur für Nitro-basierte Instances verfügbar. Wird mit FreeBSD-Instances oder DPDK-Umgebungen nicht unterstützt.

`conntrack_allowance_exceeded`: *N*

Die Anzahl der verworfenen Pakete, weil die Verbindungsverfolgung das Maximum für die Instance überschritten hat und keine neuen Verbindungen hergestellt werden konnten. Dies kann zu einem Paketverlust für den Datenverkehr zur oder von der Instance führen.

`linklocal_allowance_exceeded`: *N*

Die Anzahl der verworfenen Pakete, weil das PPS des Datenverkehrs zu lokalen Proxy-Diensten das Maximum für die Netzwerkschnittstelle überschritten hat. Dies wirkt sich auf den Datenverkehr zum Amazon-DNS-Service, zum Instance Metadata Service und zum Amazon Time Sync Service aus, hat jedoch keine Auswirkung auf den Datenverkehr an benutzerdefinierte DNS-Resolver.

`queue_N_tx_cnt`: *N*

Gibt die Anzahl der übertragenen Pakete für diese Warteschlange an.

`queue_N_tx_bytes`: *N*

Gibt die Anzahl von übertragenen Bytes für diese Warteschlange an.

`queue_N_tx_queue_stop`: *N*

Gibt an, wie oft die Warteschlange *N* vollständig gefüllt war und angehalten wurde.

`queue_N_tx_queue_wakeup`: *N*

Gibt an, wie oft die Warteschlange *N* nach dem Anhalten wieder gestartet wurde.

`queue_N_tx_dma_mapping_err`: *N*

Fehleranzahl für direkten Speicherzugriff. Wenn dieser Wert nicht 0 ist, weist dies auf einen niedrigen Stand der Systemressourcen hin.

`queue_N_tx_linearize`: *N*

Gibt an, wie oft die SKB-Linearisierung für diese Warteschlange versucht wurde.

`queue_N_tx_linearize_failed`: *N*

Gibt an, wie oft die SKB-Linearisierung für diese Warteschlange fehlgeschlagen ist.

`queue_N_tx_napi_comp`: *N*

Gibt an, wie oft der `napi`-Handler `napi_complete` für diese Warteschlange aufgerufen hat.

`queue_N_tx_tx_poll`: *N*

Gibt an, wie oft der `napi`-Handler für diese Warteschlange geplant war.

`queue_N_tx_doorbells`: *N*

Gibt die Anzahl der Übertragungs-Doorbells für diese Warteschlange an.

`queue_N_tx_prepare_ctx_err`: *N*

Gibt an, wie oft `ena_com_prepare_tx` für diese Warteschlange fehlgeschlagen ist.

`queue_N_tx_bad_req_id`: *N*

Ungültige `req_id` für diese Warteschlange. Die gültige `req_id` ist 0, minus `queue_size` und minus 1.

`queue_N_tx_llq_buffer_copy: N`

Die Anzahl der Pakete, deren Header-Größe größer ist als der llq-Eintrag für diese Warteschlange.

`queue_N_tx_missed_tx: N`

Gibt die Anzahl der nicht abgeschlossenen Pakete für diese Warteschlange an.

`queue_N_tx_unmask_interrupt: N`

Gibt an, wie oft der tx-Interrupt für diese Warteschlange entlarvt wurde.

`queue_N_rx_cnt: N`

Anzahl der empfangenen Pakete für diese Warteschlange.

`queue_N_rx_bytes: N`

Anzahl der empfangenen Bytes für diese Warteschlange.

`queue_N_rx_rx_copybreak_pkt: N`

Gibt an, wie oft die rx-Warteschlange ein Paket erhalten hat, das kleiner als die rx_copybreak-Paketgröße für diese Warteschlange ist.

`queue_N_rx_csum_good: N`

Gibt an, wie oft die rx-Warteschlange ein Paket erhalten hat, in dem die Prüfsumme überprüft wurde und für diese Warteschlange korrekt war.

`queue_N_rx_refil_partial: N`

Gibt an, wie oft der Treiber erfolglos versucht hat, den leeren Teil der rx-Warteschlange mit den Puffern für diese Warteschlange wieder aufzufüllen. Ist dieser Wert nicht 0, weist dies auf einen niedrigen Stand der Speicherressourcen hin.

`queue_N_rx_bad_csum: N`

Gibt an, wie oft die Warteschlange `rx` eine fehlerhafte Prüfsumme für diese Warteschlange ermittelt hat (nur wenn rx-Prüfsummenabladung unterstützt wird).

`queue_N_rx_page_alloc_fail: N`

Gibt an, wie oft die Seitenzuordnung für diese Warteschlange fehlgeschlagen ist. Ist dieser Wert nicht 0, weist dies auf einen niedrigen Stand der Speicherressourcen hin.

`queue_N_rx_skb_alloc_fail`: *N*

Gibt an, wie oft die SKB-Zuordnung für diese Warteschlange fehlgeschlagen ist. Wenn dieser Wert nicht 0 ist, weist dies auf einen niedrigen Stand der Systemressourcen hin.

`queue_N_rx_dma_mapping_err`: *N*

Fehleranzahl für direkten Speicherzugriff. Wenn dieser Wert nicht 0 ist, weist dies auf einen niedrigen Stand der Systemressourcen hin.

`queue_N_rx_bad_desc_num`: *N*

Zu viele Puffer pro Paket. Wenn dieser Wert nicht 0 ist, weist dies auf die Verwendung von sehr kleinen Puffern hin.

`queue_N_rx_bad_req_id`: *N*

Die req_id für diese Warteschlange ist nicht gültig. Die gültige req_id stammt von [0, queue_size - 1].

`queue_N_rx_empty_rx_ring`: *N*

Gibt an, wie oft die rx-Warteschlange für diese Warteschlange leer war.

`queue_N_rx_csum_unchecked`: *N*

Gibt an, wie oft die rx-Warteschlange ein Paket erhalten hat, dessen Prüfsumme nicht für diese Warteschlange überprüft wurde.

`queue_N_rx_xdp_aborted`: *N*

Gibt an, wie oft ein XDP-Paket als XDP_ABORT klassifiziert wurde.

`queue_N_rx_xdp_drop`: *N*

Gibt an, wie oft ein XDP-Paket als XDP_DROP klassifiziert wurde.

`queue_N_rx_xdp_pass`: *N*

Gibt an, wie oft ein XDP-Paket als XDP_PASS klassifiziert wurde.

`queue_N_rx_xdp_tx`: *N*

Gibt an, wie oft ein XDP-Paket als XDP_TX klassifiziert wurde.

`queue_N_rx_xdp_invalid`: *N*

Gibt an, wie oft der XDP-Rückgabecode für das Paket ungültig war.

`queue_N_rx_xdp_redirect: N`

Gibt an, wie oft ein XDP-Paket als XDP_REDIRECT klassifiziert wurde.

`queue_N_xdp_tx_cnt: N`

Gibt die Anzahl der übertragenen Pakete für diese Warteschlange an.

`queue_N_xdp_tx_bytes: N`

Gibt die Anzahl von übertragenen Bytes für diese Warteschlange an.

`queue_N_xdp_tx_queue_stop: N`

Gibt an, wie oft diese Warteschlange vollständig gefüllt war und angehalten wurde.

`queue_N_xdp_tx_queue_wakeup: N`

Gibt an, wie oft diese Warteschlange nach dem Anhalten wieder gestartet wurde.

`queue_N_xdp_tx_dma_mapping_err: N`

Fehleranzahl für direkten Speicherzugriff. Wenn dieser Wert nicht 0 ist, weist dies auf einen niedrigen Stand der Systemressourcen hin.

`queue_N_xdp_tx_linearize: N`

Gibt an, wie oft die XDP-Puffer-Linearisierung für diese Warteschlange versucht wurde.

`queue_N_xdp_tx_linearize_failed: N`

Gibt an, wie oft die XDP-Puffer-Linearisierung für diese Warteschlange fehlgeschlagen ist.

`queue_N_xdp_tx_napi_comp: N`

Gibt an, wie oft der Napi-Handler napi_complete für diese Warteschlange aufgerufen hat.

`queue_N_xdp_tx_tx_poll: N`

Gibt an, wie oft der Napi-Handler für diese Warteschlange geplant war.

`queue_N_xdp_tx_doorbells: N`

Gibt die Anzahl der Übertragungs-Doorbells für diese Warteschlange an.

`queue_N_xdp_tx_prepare_ctx_err: N`

Gibt an, wie oft der ena_com_prepare_tx für diese Warteschlange fehlgeschlagen ist. Dieser Wert sollte immer 0 sein. Überprüfen Sie die Treiberprotokolle, wenn dies nicht der Fall ist.

`queue_N_xdp_tx_bad_req_id: N`

Die req_id für diese Warteschlange ist nicht gültig. Die gültige req_id stammt von [0, queue_size - 1].

`queue_N_xdp_tx_llq_buffer_copy: N`

Die Anzahl der Pakete, deren Header mit LLQ-Pufferkopie für diese Warteschlange kopiert wurden.

`queue_N_xdp_tx_missed_tx: N`

Gibt an, wie oft ein tx-Warteschlangeneintrag ein Abschluss-Timeout für diese Warteschlange verpasst hat.

`queue_N_xdp_tx_unmask_interrupt: N`

Gibt an, wie oft der tx-Interrupt für diese Warteschlange entlarvt wurde.

`ena_admin_q_aborted_cmd: N`

Gibt die Anzahl der abgebrochenen Admin-Befehle an. Dies passiert normalerweise während des automatischen Wiederherstellungsverfahrens.

`ena_admin_q_submitted_cmd: N`

Gibt die Anzahl der Doorbells für die Admin-Warteschlange an.

`ena_admin_q_completed_cmd: N`

Gibt die Anzahl der Abschlüsse für die Admin-Warteschlange an.

`ena_admin_q_out_of_space: N`

Gibt an, wie oft der Treiber versucht hat, einen neuen Admin-Befehl zu senden, während die Warteschlange ausgelastet war.

`ena_admin_q_no_completion: N`

Gibt an, wie oft der Treiber für einen Befehl keinen Admin-Abschluss erhalten hat.

Treiberfehlerprotokolle im syslog

Der ENA-Treiber schreibt während des Systemstarts Protokollnachrichten in das syslog. Wenn Sie entsprechende Probleme feststellen, können Sie diese Protokolle auf Fehler überprüfen. Nachfolgend finden Sie ein Beispiel für Informationen, die vom ENA-Treiber während des Systemstarts im syslog protokolliert wurden, sowie einige Anmerkungen zu ausgewählten Nachrichten.

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.416939] [ENA_COM:
 ena_com_validate_version] ena device version: 0.10
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.420915] [ENA_COM:
 ena_com_validate_version] ena controller version: 0.0.1 implementation version 1
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.256831] ena 0000:00:03.0: Device
 watchdog is Enabled
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.672947] ena 0000:00:03.0: creating 8 io
 queues. queue size: 1024
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.680885] [ENA_COM:
 ena_com_init_interrupt_moderation] Feature 20 isn't supported  // Interrupt moderation
 is not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.691609] [ENA_COM:
 ena_com_get_feature_ex] Feature 10 isn't supported // RSS HASH function configuration
 is not supported by the
 device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.694583] [ENA_COM:
 ena_com_get_feature_ex] Feature 18 isn't supported //RSS HASH input source
 configuration is not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.697433] [ENA_COM:
 ena_com_set_host_attributes] Set host attribute isn't supported
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.701064] ena 0000:00:03.0 (unnamed
 net_device) (uninitialized): Cannot set host attributes
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.704917] ena 0000:00:03.0: Elastic
 Network Adapter (ENA) found at mem f3000000, mac addr 02:8a:3c:1e:13:b5 Queues 8
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  480.805037] EXT4-fs (xvda1): re-mounted.
 Opts: (null)
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  481.025842] NET: Registered protocol family
 10
```

Welche Fehler kann ich ignorieren?

Folgende Warnungen, die u. U. in den Fehlerprotokollen Ihres Systems auftauchen, können für den Elastic Network Adapter ignoriert werden:

Das Festlegen des Hostattributs wird nicht unterstützt

> Host-Attribute werden für dieses Gerät nicht unterstützt.

Es konnte kein Puffer für die Empfangswarteschlange reserviert werden

> Dies ist ein umkehrbarer Fehler, der darauf hinweist, dass beim Auslösen des Fehlers eine starke Speicherbelastung vorgelegen hat.

Feature *X* wird nicht unterstützt

Das angegebene Feature wird vom Elastic Network Adapter nicht unterstützt. Mögliche Werte für *X* sind:

- 10: Konfiguration der RSS Hash-Funktion wird für dieses Gerät nicht unterstützt.
- 12: Konfiguration der RSS Indirection-Tabelle wird für dieses Gerät nicht unterstützt.
- 18: RSS-Hash-Input-Konfiguration wird für dieses Gerät nicht unterstützt.
- 20: Interrupt Moderation wird für dieses Gerät nicht unterstützt.
- 27: Der Elastic -Network-Adapter-Treiber unterstützt keine Abfrage der Ethernet-Kapazitäten von snmpd.

AENQ konnte nicht konfiguriert werden

Der Elastic Network Adapter unterstützt keine AENQ-Konfiguration.

Es wird versucht, nicht unterstützte AENQ-Ereignisse festzulegen

Dieser Fehler weist darauf hin, dass versucht wurde, eine AENQ-Ereignisgruppe festzulegen, die vom Elastic Network Adapter nicht unterstützt wird.

Benachrichtigungen zur suboptimalen Konfiguration

Das ENA-Gerät erkennt suboptimale Konfigurationseinstellungen im Treiber, die Sie ändern können. Das Gerät benachrichtigt den ENA-Treiber und protokolliert eine Warnung zur Konsole. Das folgende Beispiel zeigt das Format der Warnmeldung.

```
Sub-optimal configuration notification code: 1. Refer to AWS ENA documentation for
 additional details and mitigation options.
```

Die folgende Liste enthält Details zum Benachrichtigungscode und empfohlene Maßnahmen für suboptimale Konfigurationserkenntnisse.

- Code 1: ENA Express mit umfassender LLQ-Konfiguration wird nicht empfohlen

  ENA Express ENI ist mit umfassenden LLQ konfiguriert. Diese Konfiguration ist suboptimal und könnte die Leistung von ENA Express beeinträchtigen. Wir empfehlen, die umfassenden LLQ-Einstellungen wie folgt zu deaktivieren, wenn Sie ENA Express ENIs verwenden.

  ```
  sudo rmmod ena && sudo modprobe ena force_large_llq_header=0
  ```

Weitere Informationen zur optimalen Konfiguration für ENA Express finden Sie unter Verbessern Sie die Netzwerkleistung zwischen EC2 Instanzen mit ENA Express.

- Code 2: ENA Express ENI mit suboptimaler Tx-Warteschlangentiefe wird nicht empfohlen

  ENA Express ENI ist mit einer suboptimalen Tx-Warteschlangentiefe konfiguriert. Diese Konfiguration beeinträchtigt möglicherweise die Leistung von ENA Express. Wir empfehlen, bei Verwendung von ENA Express alle Tx-Warteschlangen wie folgt auf den maximalen Wert für die Netzwerkschnittstelle zu vergrößern.

  Sie können die folgenden ethtool-Befehle ausführen, um die LLQ-Größe anzupassen. Weitere Informationen zur Steuerung, Abfrage und Aktivierung von Wide-LLQ finden Sie im Thema Große Warteschlange mit niedriger Latenzzeit (Large Low-Latency Queue – Large LLQ) der Dokumentation zum Linux-Kernel-Treiber für ENA im Amazon-Treiber-GitHub-Repository.

  ```
  ethtool -g interface
  ```

  Stellen Sie Ihre Tx-Warteschlangen auf die maximale Tiefe ein:

  ```
  ethtool -G interface tx depth
  ```

  Weitere Informationen zur optimalen Konfiguration für ENA Express finden Sie unter Verbessern Sie die Netzwerkleistung zwischen EC2 Instanzen mit ENA Express.

- Code 3: ENA mit regulärer LLQ-Größe und Tx-Paketverkehr überschreitet die maximale unterstützte Header-Größe

  Standardmäßig unterstützt ENA LLQ eine Tx-Paket-Header-Größe von bis zu 96 Byte. Wenn die Größe des Paket-Headers mehr als 96 Byte beträgt, wird das Paket verworfen. Um dieses Problem zu beheben, empfehlen wir, Wide-LLQ zu aktivieren, wodurch die unterstützte Tx-Paket-Header-Größe auf maximal 224 Byte erhöht wird.

  Wenn Sie Wide-LLQ aktivieren, wird die maximale Tx-Ringgröße jedoch von 1 000 auf 512 Einträge reduziert. Wide-LLQ ist standardmäßig für alle Instance-Typen von Nitro v4 und höher aktiviert.

  - Nitro-v4-Instance-Typen haben standardmäßig eine maximale Wide-LLQ-Tx-Ringgröße von 512 Einträgen, die nicht geändert werden kann.

- Nitro-v5-Instance-Typen haben standardmäßig eine maximale Wide-LLQ-Tx-Ringgröße von 512 Einträgen, die Sie auf 1 000 Einträge erhöhen können.

Sie können die folgenden ethtool-Befehle ausführen, um die LLQ-Größe anzupassen. Weitere Informationen zur Steuerung, Abfrage und Aktivierung von Wide-LLQ finden Sie im Thema Große Warteschlange mit niedriger Latenzzeit (Large Low-Latency Queue – Large LLQ) der Dokumentation zum Linux-Kernel-Treiber für ENA im Amazon-Treiber-GitHub-Repository.

Finden Sie die maximale Tiefe für Ihre Tx-Warteschlangen heraus:

```
ethtool -g interface
```

Stellen Sie Ihre Tx-Warteschlangen auf die maximale Tiefe ein:

```
ethtool -G interface tx depth
```

Fehlerbehebung beim Windows-Treiber von Elastic Network Adapter

Der Elastic Network Adapter (ENA) wurde entwickelt, um den Zustand des Betriebssystems zu verbessern und unerwartetes Hardwareverhalten oder -ausfälle zu reduzieren, die den Betrieb Ihrer Windows-Instance stören können. In der ENA-Architektur bleiben Geräte- oder Treiberfehler für das Betriebssystem weitestgehend transparent.

Sammeln von Diagnoseinformationen über die Instance

Die Schritte zum Öffnen der Tools des Windows-Betriebssystems variieren je nachdem, welche Version des Betriebssystems auf Ihrer Instance installiert ist. In den folgenden Abschnitten verwenden wir das Dialogfeld Run (Ausführen) zum Öffnen der Tools, das in allen Betriebssystemversionen gleich funktioniert. Sie können jedoch mit jeder beliebigen Methode auf diese Tools zugreifen.

Zugriff auf das Dialogfeld „Run“ (Ausführen)

- Mit der Windows-Logo-Tastenkombination: `Windows` + `R`
- Über die Suchleiste:
  - Geben Sie im Suchfeld `run` ein.
  - Wählen Sie die Anwendung Run (Ausführen) aus den Suchergebnissen aus.

Einige Schritte erfordern das Kontextmenü, um auf Eigenschaften oder kontextsensitive Aktionen zuzugreifen. Dazu gibt es je nach Betriebssystemversion und Hardware verschiedene Möglichkeiten.

Zugriff auf das Kontextmenü

- Mit der Maus: Klicken Sie mit der rechten Maustaste auf ein Element, um das Kontextmenü aufzurufen.
- Mit der Tastatur:
  - Verwenden Sie je nach Betriebssystemversion `Shift` + `F10` oder `Ctrl` + `Shift` + `F10`.
  - Wenn Sie die Kontexttaste auf Ihrer Tastatur haben (drei horizontale Linien in einem Feld), wählen Sie das gewünschte Element aus und drücken Sie dann die Kontexttaste.

Wenn Sie eine Verbindung mit Ihrer Instance herstellen können, verwenden Sie die folgenden Techniken, um Diagnoseinformationen zur Fehlerbehebung zu sammeln.

Überprüfen des ENA-Gerätestatus

Gehen Sie folgendermaßen vor, um den Status Ihres ENA-Windows-Treibers mit dem Windows-Geräte-Manager zu überprüfen:

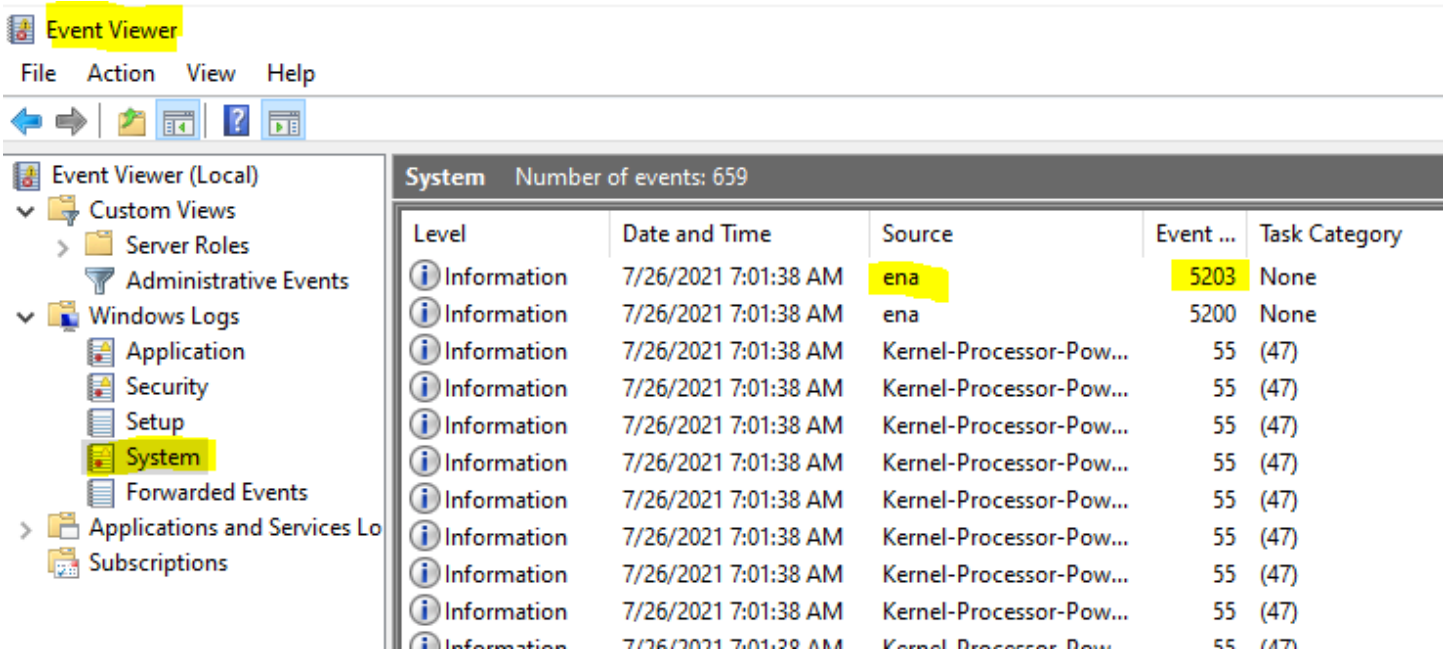
1. Öffnen Sie das Dialogfeld Run (Ausführen) mit einer der im vorherigen Abschnitt beschriebenen Methoden.
2. Zum Aufrufen des Windows-Geräte-Managers geben Sie `devmgmt.msc` im Feld Run (Ausführen) ein.
3. Wählen Sie OK aus. Dadurch wird das Fenster „Device Manager“ (Geräte-Manager) geöffnet.
4. Wählen Sie den Pfeil links neben Network adapters (Netzwerkadapter) aus, um die Liste zu erweitern.
5. Wählen Sie den Namen aus oder öffnen Sie das Kontextmenü für den Amazon Elastic Network Adapter und wählen Sie dann Properties (Eigenschaften) aus. Dadurch wird das Dialogfeld mit den Eigenschaften des Amazon Elastic Network Adapters geöffnet.
6. Vergewissern Sie sich, dass auf der Registerkarte Allgemein die Meldung „Dieses Gerät funktioniert ordnungsgemäß“ erscheint.

Untersuchen von Treiberereignismeldungen

Gehen Sie folgendermaßen vor, um die Ereignisprotokolle des ENA-Windows-Treibers mit der Windows-Ereignisanzeige zu überprüfen:

1. Öffnen Sie das Dialogfeld Run (Ausführen) mit einer der im vorherigen Abschnitt beschriebenen Methoden.
2. Zum Aufrufen der Windows-Ereignisanzeige geben Sie `eventvwr.msc` im Feld Ausführen ein.
3. Wählen Sie OK aus. Dadurch wird das Fenster „Ereignisanzeige“ geöffnet.
4. Erweitern Sie das Menü Windows Logs (Windows--Protokolle) und wählen Sie dann System (System) aus.
5. Wählen Sie unter Actions (Aktionen) im oberen rechten Bereich Filter Current Log (Aktuelles Protokoll filtern) aus. Daraufhin wird das Filterdialogfeld angezeigt.
6. Geben Sie im Feld Event sources (Ereignisquellen) `ena` ein. Dies beschränkt die Ergebnisse auf Ereignisse, die vom ENA-Windows-Treiber generiert wurden.
7. Wählen Sie OK aus. Daraufhin werden gefilterte Ereignisprotokollergebnisse in den Detailabschnitten des Fensters angezeigt.
8. Um die Details ausführlicher anzuzeigen, wählen Sie eine Ereignismeldung in der Liste aus.

Das folgende Beispiel zeigt ein ENA-Treiberereignis in der Systemereignisliste der Windows-Ereignisanzeige:



Zusammenfassung der Ereignismeldung

Die folgende Tabelle zeigt Ereignismeldungen, die der ENA-Windows-Treiber generiert.

Eingabe

Ereignis-ID	Beschreibung des ENA-Treiberereignisses	Typ
5001	Hardware hat keine Ressourcen mehr.	Fehler
5002	Adapter hat einen Hardwarefehler erkannt.	Fehler
5005	Für den Adapter ist bei einem NDIS-Vorgang, der nicht rechtzeitig abgeschlossen wurde, eine Zeitüberschreitung aufgetreten.	Fehler
5032	Adapter konnte das Gerät nicht zurücksetzen.	Fehler
5200	Adapter wurde initialisiert.	Informativ
5201	Adapter wurde unterbrochen.	Informativ
5202	Adapter wurde angehalten.	Informativ
5203	Adapter wurde neu gestartet.	Informativ
5204	Adapter wurde heruntergefahren.	Informativ
5205	Adapter wurde zurückgesetzt.	Fehler
5206	Adapter wurde überraschend entfernt.	Fehler
5208	Initialisierungsroutine des Adapters ist fehlgeschlagen.	Fehler

Ereignis-ID	Beschreibung des ENA-Treibereignisses	Typ
5210	Adapter ist auf ein internes Problem gestoßen und hat erfolgreich wiederhergestellt.	Fehler

Leistungsmetriken überprüfen

Der ENA-Windows-Treiber veröffentlicht Netzwerkleistungsmetriken der Instances, für die sie aktiviert sind. Sie können Metriken für die Instance mit der nativen Leistungsmonitoranwendung anzeigen und aktivieren. Weitere Informationen zu den Metriken, die der ENA-Windows-Treiber erstellt, finden Sie unter Netzwerkleistung für ENA-Einstellungen auf Ihrer EC2-Instance überwachen.

Auf Instances, auf denen ENA-Metriken aktiviert sind und der Amazon-CloudWatch-Agent installiert ist, sammelt CloudWatch die Metriken, die mit den Zählern im Windows-Leistungsmonitor verbunden sind, sowie einige erweiterte Metriken für ENA. Diese Metriken werden zusätzlich zu den Metriken erfasst, die auf EC2-Instances standardmäßig aktiviert sind. Weitere Informationen zu diesen Metriken finden Sie unter Vom Amazon-CloudWatch-Agenten erfasste Metriken im Benutzerhandbuch von Amazon CloudWatch.

> **Note**
>
> Leistungsmetriken stehen ab der ENA-Treiberversion 2.4.0 (sowie für die Version 2.2.3) zur Verfügung. Die ENA-Treiberversion 2.2.4 wurde aufgrund einer möglichen Leistungsverschlechterung bei EC2-Instances der sechsten Generation zurückgesetzt. Wir empfehlen, ein Upgrade auf die aktuelle Version des Treibers durchzuführen, um sicherzustellen, dass Sie über die neuesten Updates verfügen.

Zu den Möglichkeiten, wie Sie Leistungsmetriken verwenden können, gehören:

- Beheben von Problemen mit der Instance-Leistung
- Auswählen der richtigen Instance-Größe für eine Workload
- Proaktives Planen von Skalierungsaktivitäten
- Benchmarking von Anwendungen, um festzustellen, ob sie die auf einer Instance verfügbare Leistung maximieren

Aktualisierungsrate

Standardmäßig aktualisiert der Treiber Metriken in einem Intervall von 1 Sekunde. Die Anwendung, die die Metriken abruft, verwendet jedoch möglicherweise ein anderes Intervall für die Abfrage. Sie können das Aktualisierungsintervall im Geräte-Manager mithilfe der erweiterten Eigenschaften für den Treiber ändern.

Gehen Sie folgendermaßen vor, um das Aktualisierungsintervall für den ENA-Windows-Treiber zu ändern:

1. Öffnen Sie das Dialogfeld Run (Ausführen) mit einer der im vorherigen Abschnitt beschriebenen Methoden.
2. Zum Aufrufen des Windows-Geräte-Managers geben Sie `devmgmt.msc` im Feld Run (Ausführen) ein.
3. Wählen Sie OK aus. Dadurch wird das Fenster „Device Manager“ (Geräte-Manager) geöffnet.
4. Wählen Sie den Pfeil links neben Network adapters (Netzwerkadapter) aus, um die Liste zu erweitern.
5. Wählen Sie den Namen aus oder öffnen Sie das Kontextmenü für den Amazon Elastic Network Adapter und wählen Sie dann Properties (Eigenschaften) aus. Dadurch wird das Dialogfeld mit den Eigenschaften des Amazon Elastic Network Adapters geöffnet.
6. Öffnen Sie die Registerkarte Advanced (Erweitert) im Popup-Fenster.
7. Wählen Sie in der Liste Property (Eigenschaft) Metrics Refresh Interval (Aktualisierungsintervall für Metriken) aus, um den Wert zu ändern.
8. Wählen Sie OK aus, wenn Sie damit fertig sind.

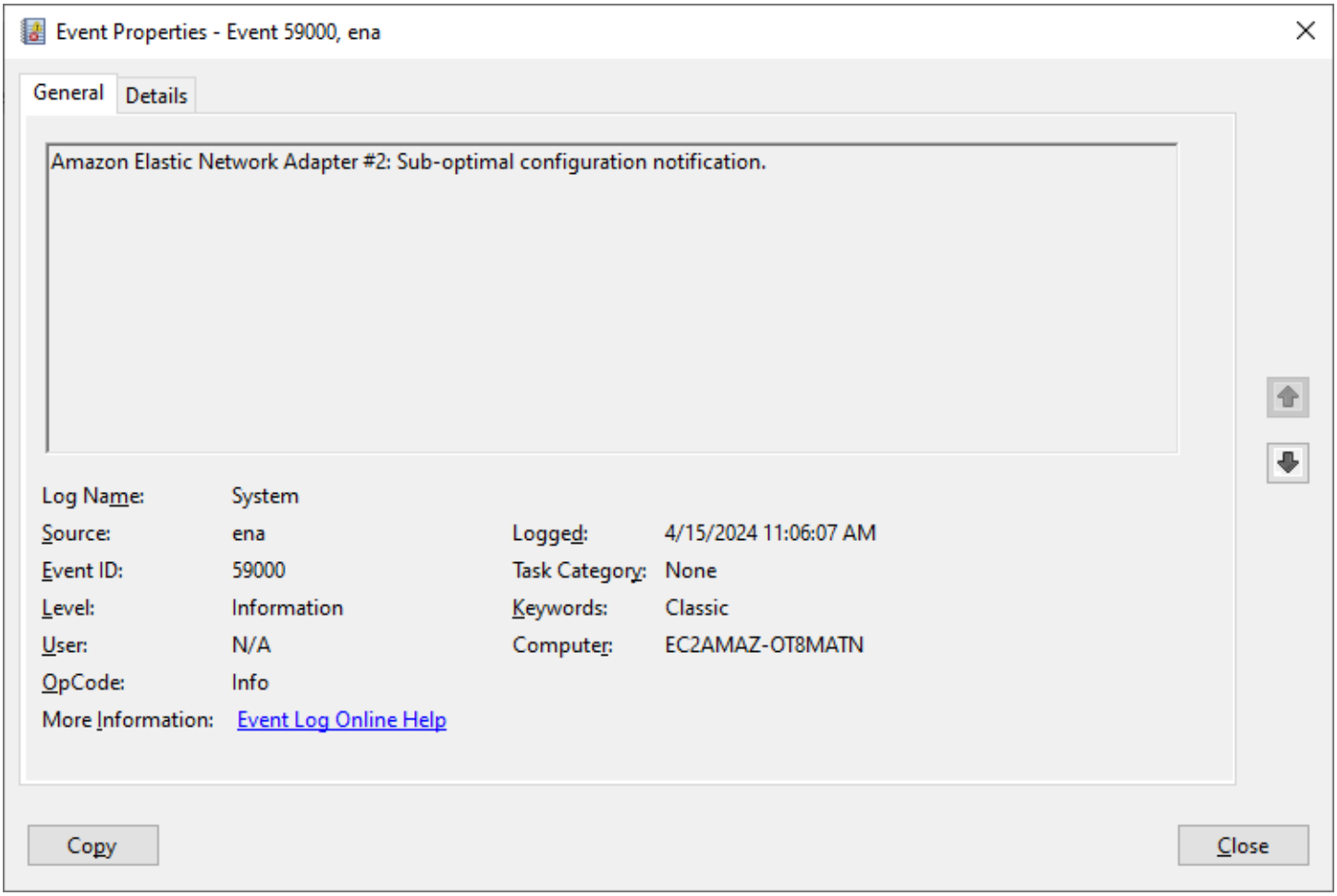
Benachrichtigungen zur suboptimalen Konfiguration untersuchen

Das ENA-Gerät erkennt suboptimale Konfigurationseinstellungen im Treiber, die Sie ändern können. Das Gerät benachrichtigt den ENA-Treiber und protokolliert eine Ereignisbenachrichtigung. So überprüfen Sie suboptimale Ereignisse in der Windows-Ereignisanzeige

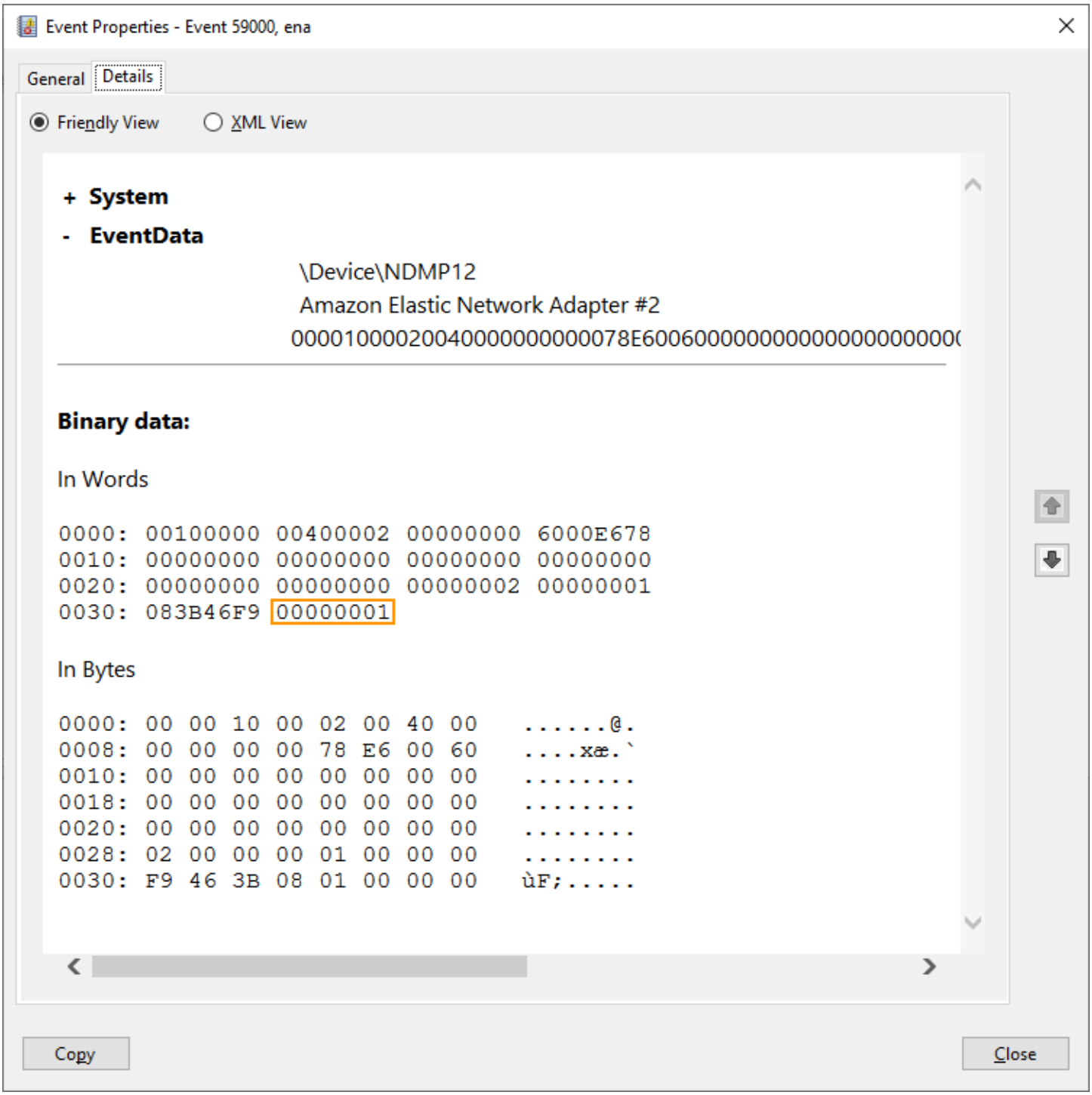
1. Öffnen Sie das Dialogfeld Run (Ausführen) mit einer der im vorherigen Abschnitt beschriebenen Methoden.
2. Zum Aufrufen der Windows-Ereignisanzeige geben Sie `eventvwr.msc` im Feld Ausführen ein.
3. Wählen Sie OK aus. Dadurch wird das Fenster „Ereignisanzeige“ geöffnet.

4. Erweitern Sie das Menü Windows Logs (Windows--Protokolle) und wählen Sie dann System (System) aus.
5. Wählen Sie unter Actions (Aktionen) im oberen rechten Bereich Filter Current Log (Aktuelles Protokoll filtern) aus. Daraufhin wird das Filterdialogfeld angezeigt.
6. Geben Sie im Feld Event sources (Ereignisquellen) `ena` ein. Dies beschränkt die Ergebnisse auf Ereignisse, die vom ENA-Windows-Treiber generiert wurden.
7. Wählen Sie OK aus. Daraufhin werden gefilterte Ereignisprotokollergebnisse in den Detailabschnitten des Fensters angezeigt.

Ereignisse mit ID `59000` informieren Sie über suboptimale Konfigurations-Erkenntnisse. Klicken Sie mit der rechten Maustaste auf ein Ereignis und wählen Sie Ereigniseigenschaften, um eine detaillierte Ansicht zu öffnen, oder wählen Sie im Menü Ansicht die Option Vorschaufenster, um dasselbe Detail anzuzeigen.



Öffnen Sie die Registerkarte Details, um den Ereignis-Code anzuzeigen. Im Abschnitt Binärdaten: In Worten ist das letzte Wort der Code.



Die folgende Liste enthält Details zum Benachrichtigungscode und empfohlene Maßnahmen für suboptimale Konfigurationserkenntnisse.

- Code **1**: ENA Express mit umfassender LLQ-Konfiguration wird nicht empfohlen

ENA Express ENI ist mit umfassenden LLQ konfiguriert. Diese Konfiguration ist suboptimal und könnte die Leistung von ENA Express beeinträchtigen. Wir empfehlen, die umfassenden LLQ-Einstellungen wie folgt zu deaktivieren, wenn Sie ENA Express ENIs verwenden.

1. Zum Aufrufen des Windows-Geräte-Managers geben Sie `devmgmt.msc` im Feld Run (Ausführen) ein.
2. Wählen Sie OK aus. Dadurch wird das Fenster „Device Manager“ (Geräte-Manager) geöffnet.
3. Wählen Sie den Pfeil links neben Network adapters (Netzwerkadapter) aus, um die Liste zu erweitern.
4. Öffnen Sie die Eigenschaften für den `Amazon Elastic Network Adapter`.
5. Öffnen Sie von dort die Registerkarte Erweitert, um Ihre Änderungen vorzunehmen.
6. Wählen Sie die Eigenschaft LLQ Header Size Policy aus und legen Sie ihren Wert auf `Normal (128 Bytes)` fest.
7. Wählen Sie OK aus, um Ihre Änderungen zu speichern.

- Code **2**: ENA Express ENI mit suboptimaler Tx-Warteschlangentiefe wird nicht empfohlen.

  ENA Express ENI ist mit einer suboptimalen Tx-Warteschlangentiefe konfiguriert. Diese Konfiguration beeinträchtigt möglicherweise die Leistung von ENA Express. Wir empfehlen, bei Verwendung von ENA Express alle Tx-Warteschlangen wie folgt auf den maximalen Wert für die Netzwerkschnittstelle zu vergrößern.

  Folgen Sie diesen Schritten, um die Tx-Warteschlangen auf die maximale Tiefe zu vergrößern:

  1. Zum Aufrufen des Windows-Geräte-Managers geben Sie `devmgmt.msc` im Feld Run (Ausführen) ein.
  2. Wählen Sie OK aus. Dadurch wird das Fenster „Device Manager“ (Geräte-Manager) geöffnet.
  3. Wählen Sie den Pfeil links neben Network adapters (Netzwerkadapter) aus, um die Liste zu erweitern.
  4. Öffnen Sie die Eigenschaften für den `Amazon Elastic Network Adapter`.
  5. Öffnen Sie von dort die Registerkarte Erweitert, um Ihre Änderungen vorzunehmen.
  6. Wählen Sie die Eigenschaft Übertragungspuffer aus und legen Sie ihren Wert auf den maximal unterstützten Wert fest.
  7. Wählen Sie OK aus, um Ihre Änderungen zu speichern.

Zurücksetzen des ENA-Adapters

Der Zurücksetzungsprozess startet, wenn der ENA-Windows-Treiber einen Fehler an einem Adapter feststellt und den Adapter als fehlerhaft markiert. Der Treiber kann sich nicht selbst zurücksetzen, daher ist es die Aufgabe des Betriebssystems, den Zustand des Adapters zu überprüfen und den Rücksetz-Handle für den ENA-Windows-Treiber aufzurufen. Beim Zurücksetzen kann es zu einer kurzen Zeitspanne kommen, in der der Datenverkehr unterbrochen ist. TCP-Verbindungen sollten jedoch wiederhergestellt werden können.

Der ENA-Adapter fordert möglicherweise auch indirekt eine Prozedur zum Zurücksetzen des Geräts an, indem er keine Keep-Alive-Benachrichtigung sendet. Wenn der ENA-Adapter beispielsweise nach dem Laden einer nicht wiederherstellbaren Konfiguration in einen unbekannten Status versetzt wird, sendet er möglicherweise keine Keep-Alive-Benachrichtigungen mehr.

Häufige Ursachen für das Zurücksetzen des ENA-Adapters

- Keep-Alive-Nachrichten fehlen.

  Der ENA-Adapter sendet Keep-Alive-Ereignisse in einem bestimmten Zeitintervall (i. d. R. einmal pro Sekunde). Der ENA-Windows-Treiber implementiert einen Überwachungsmechanismus, der regelmäßig auf das Vorhandensein von Keep-Alive-Nachrichten überprüft. Wenn er seit der letzten Überprüfung eine oder mehrere neue Nachrichten erkennt, zeichnet er ein erfolgreiches Ergebnis auf. Andernfalls kommt der Treiber zu dem Schluss, dass das Gerät einen Fehler festgestellt hat, und leitet eine Zurücksetzungssequenz ein.
- Pakete stecken in Übertragungswarteschlangen fest.

  Der ENA-Adapter überprüft, ob Pakete wie erwartet durch die Übertragungswarteschlangen fließen. Der ENA-Windows-Treiber erkennt, ob Pakete hängen bleiben, und leitet eine Zurücksetzungssequenz ein, wenn dies der Fall ist.
- Timeout beim Lesen für MMIO-Register (Memory Mapped I/O)

  Um die im Speicher abgebildeten I/O-Lesevorgänge (MMIO) einzuschränken, greift der ENA-Windows-Treiber nur während der Initialisierungs- und Zurücksetzungsprozesse auf MMIO-Register zu. Wenn der Treiber ein Timeout erkennt, führt er je nachdem, welcher Prozess ausgeführt wurde, eine der folgenden Aktionen aus:

  - Wenn während der Initialisierung ein Timeout erkannt wird, schlägt der Datenfluss fehl, was dazu führt, dass der Treiber ein gelbes Ausrufezeichen des ENA-Adapters im Windows-Geräte-Manager anzeigt.

- Wenn beim Zurücksetzen ein Timeout erkannt wird, schlägt der Datenfluss fehl. Das Betriebssystem leitet dann ein überraschendes Entfernen des ENA-Adapters ein und stellt ihn wieder her, indem es den entfernten Adapter anhält und startet. Weitere Informationen zum überraschenden Entfernen einer Network Interface Card (NIC, Netzwerkschnittstellenkarte) finden Sie unter Behandeln des überraschenden Entfernens einer NIC in der Dokumentation für Microsoft Windows-Hardwareentwickler.

Fehlerbehebungsszenarien

Die folgenden Szenarien können Ihnen bei der Behebung von Problemen helfen, die beim ENA-Windows-Treiber möglicherweise auftreten. Wir empfehlen Ihnen, mit dem Upgrade Ihres ENA-Treibers zu beginnen, wenn Sie nicht über die aktuelle Version verfügen. Den aktuellen Treiber für Ihre Windows-Betriebssystemversion finden Sie unter NA-Windows-Treiber-Versionen verfolgen.

Unerwartete ENA-Treiberversion installiert

Beschreibung

Nachdem Sie die Schritte zur Installation einer bestimmten Version des ENA-Treibers ausgeführt haben, zeigt der Windows-Geräte-Manager an, dass Windows eine andere Version des ENA-Treibers installiert hat.

Ursache

Wenn Sie die Installation für ein Treiberpaket ausführen, ordnet Windows alle Treiberpakete, die für das angegebene Gerät gültig sind, im lokalen Treiberspeicher ein, bevor es beginnt. Dann wird das Paket mit dem niedrigsten Rangwert als das am besten passende Paket ausgewählt. Dies kann sich von dem Paket unterscheiden, das Sie installieren wollten. Weitere Informationen zur Auswahl von Gerätetreiberpaketen finden Sie auf der Microsoft-Dokumentationswebsite unter So wählt Windows ein Treiberpaket für ein Gerät aus.

Lösung

Um sicherzustellen, dass Windows die von Ihnen gewählte Treiberpaketversion installiert, können Sie mit dem PnPUtil-Befehlszeilentool Treiberpakete mit niedrigerem Rang aus dem Treiberspeicher entfernen.

Gehen Sie folgendermaßen vor, um den ENA-Treiber zu aktualisieren:

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
2. Öffnen Sie das Eigenschaftenfenster des Geräte-Managers, wie im Abschnitt Überprüfen des ENA-Gerätestatus beschrieben. Dadurch wird die Registerkarte Allgemein des Fensters Eigenschaften zu Amazon Elastic Network Adapter geöffnet.
3. Öffnen Sie die Registerkarte Driver (Treiber).
4. Wählen Sie Update Driver (Treiber aktualisieren) aus. Dadurch wird das Dialogfeld Treibersoftware aktualisieren – Amazon Elastic Network Adapter geöffnet.
   a. Auf der Seite Wie wollen Sie nach Treibersoftware suchen? wählen Sie Meinen Computer nach Treibersoftware durchsuchen.
   b. Wählen Sie auf der Seite Nach Treibersoftware auf Ihrem Computer suchen die Option Lassen Sie mich aus einer Liste von Gerätetreibern auf meinem Computer auswählen, die sich unter der Suchleiste befindet.
   c. Wählen Sie auf der Seite Wählen Sie den Gerätetreiber aus, den Sie für diese Hardware installieren möchten, die Option Hat Festplatte ... .
   d. Wählen Sie im Fenster Von Festplatte installieren die Option Durchsuchen ... , neben dem Verzeichnis der Datei aus der Dropdown-Liste.
   e. Navigieren Sie zu dem Verzeichnis, in das Sie das ENA-Treiberpaket heruntergeladen haben. Wählen Sie die Datei namens `ena.inf` und dann Öffnen aus.
   f. Um die Installation zu starten, wählen Sie OK und dann Weiter.
5. Wenn das Installationsprogramm Ihre Instance nicht automatisch neu startet, führen Sie den Restart-Computer PowerShell Cmdlet aus.

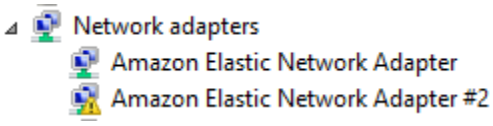
```
PS C:\> Restart-Computer
```

Gerätewarnung für ENA-Treiber

Beschreibung

Das ENA-Adaptersymbol im Abschnitt Network adapters (Netzwerkadapter) des Geräte-Managers zeigt ein Warnzeichen an (ein gelbes Dreieck mit einem Ausrufezeichen darin).

Das folgende Beispiel zeigt einen ENA-Adapter mit dem Warnsymbol im Windows-Geräte-Manager:



Ursache

Diese Gerätewarnung wird in der Regel durch Umgebungsprobleme verursacht, die möglicherweise weitere Nachforschungen und oft einen Eliminierungsprozess erfordern, um die zugrunde liegende Ursache zu ermitteln. Eine vollständige Liste der Gerätefehler finden Sie unter Geräte-Manager: Fehlermeldungen in der Microsoft-Dokumentation.

Lösung

Die Lösung für diese Gerätewarnung hängt von der Ursache ab. Der hier beschriebene Eliminierungsprozess umfasst einige grundlegende Schritte, um die häufigsten Probleme zu identifizieren und zu beheben, für die es möglicherweise eine einfache Lösung gibt. Eine zusätzliche Ursachenanalyse ist erforderlich, wenn diese Schritte das Problem nicht beheben.

Gehen Sie folgendermaßen vor, um häufige Probleme zu identifizieren und zu beheben:

1. Anhalten und Starten des Geräts

   Öffnen Sie das Eigenschaftenfenster des Geräte-Managers, wie im Abschnitt Überprüfen des ENA-Gerätestatus beschrieben. Damit wird die Registerkarte General (Allgemein) des Fensters Amazon Elastic Network Adapter Properties (Eigenschaften von Amazon Elastic Network Adapter) geöffnet, in dem der Device status (Gerätestatus) den Fehlercode und eine kurze Meldung anzeigt.

   a. Öffnen Sie die Registerkarte Driver (Treiber).
   b. Wählen Sie Disable Device (Gerät deaktivieren) aus und antworten Sie bei der angezeigten Warnmeldung mit Yes (Ja).
   c. Wählen Sie Enable Device (Gerät aktivieren) aus.

2. Stoppen und Starten der EC2-Instance

   Wenn der Adapter weiterhin das Warnsymbol im Geräte-Manager anzeigt, besteht der nächste Schritt darin, die EC2-Instance zu stoppen und zu starten. Dadurch wird die Instance in den meisten Fällen auf unterschiedlicher Hardware neu gestartet.

3. Untersuchen eines möglichen Instance-Ressourcenproblems

   Wenn Sie Ihre EC2-Instance gestoppt und gestartet haben und das Problem weiterhin besteht, kann dies auf ein Ressourcenproblem in Ihrer Instance hinweisen, z. B. auf unzureichenden Speicher.

Verbindungs-Timeout und Adapterzurücksetzung (Fehlercodes 5007, 5205)

Beschreibung

Die Windows-Ereignisanzeige zeigt Adapter-Timeout und Zurücksetzungsereignisse an, die in Kombination für ENA-Adapter auftreten. Die Meldungen können wie die folgenden Beispiele aussehen:

- Ereignis-ID 5007: Amazon Elastic Network Adapter: Timeout während eines Vorgangs.
- Ereignis-ID 5205: Amazon Elastic Network Adapter: Zurücksetzen des Adapters wurde gestartet.

Adapterzurücksetzungen verursachen minimale Datenverkehrsunterbrechungen. Selbst wenn es mehrere Zurücksetzungen gibt, wäre es ungewöhnlich, dass sie zu schwerwiegenden Netzwerkstörungen führen.

Ursache

Diese Ereignissequenz zeigt an, dass der ENA-Windows-Treiber eine Zurücksetzung für einen ENA-Adapter initiiert hat, der nicht reagierte. Der Mechanismus, den der Gerätetreiber verwendet, um dieses Problem zu erkennen, ist jedoch anfällig für Fehlalarme, die durch ein Verhungern von CPU 0 entstehen.

Lösung

Wenn diese Kombination von Fehlern häufig auftritt, überprüfen Sie Ihre Ressourcenzuweisungen, um zu sehen, wo Anpassungen hilfreich sein könnten.

1. Öffnen Sie das Dialogfeld Run (Ausführen) mit einer der im vorherigen Abschnitt beschriebenen Methoden.
2. Um den Windows-Ressourcenmonitor zu öffnen, geben Sie `resmon` im Feld Ausführen ein.
3. Wählen Sie OK aus. Daraufhin wird das Fenster „Ressourcenmonitor“ geöffnet.
4. Öffnen Sie die Registerkarte CPU. Diagramme der Auslastung pro CPU werden auf der rechten Seite des Ressourcenmonitor-Fensters angezeigt.

5. Überprüfen Sie die Auslastungswerte für CPU 0, um festzustellen, ob sie zu hoch sind.

Es wird empfohlen, RSS so zu konfigurieren, dass CPU 0 für den ENA-Adapter bei größeren Instance-Typen (mehr als 16 vCPU) ausgeschlossen wird. Bei kleineren Instance-Typen kann die Konfiguration von RSS die Erfahrung verbessern, aber aufgrund der geringeren Anzahl verfügbarer Kerne sind Tests erforderlich, um sicherzustellen, dass sich die Einschränkung von CPU-Kernen nicht negativ auf die Leistung auswirkt.

Verwenden Sie den Set-NetAdapterRss-Befehl, um RSS für Ihren ENA-Adapter zu konfigurieren, wie im folgenden Beispiel gezeigt.

```
Set-NetAdapterRss -name (Get-NetAdapter | Where-Object {$_.InterfaceDescription -like
 "*Elastic*"}).Name -Baseprocessorgroup 0 -BaseProcessorNumber 1
```

Die Migration auf eine Instance-Infrastruktur der sechsten Generation wirkt sich auf Leistung oder die Anfügung aus.

Beschreibung

Wenn Sie auf eine EC2-Instance der sechsten Generation migrieren, können eine Leistungsminderung oder Ausfälle von ENA-Anfügungen auftreten, wenn Sie Ihre ENA Windows-Treiberversion nicht aktualisiert haben.

Ursache

Für die EC2-Instance-Typen der sechsten Generation muss die folgende Mindestversion des ENA-Windows-Treibers vorhanden sein – basierend auf dem Instance-Betriebssystem (OS).

Mindestversion

Windows Server Version	ENA-Treiberversion
Windows Server 2008 R2	2.2.3 oder 2.4.0
Windows Server 2012 und höher	2.2.3 und höher
Windows Workstation	2.2.3 und höher

Windows Server Version	ENA-Treiberversion

Lösung

Vergewissern Sie sich vor dem Upgrade auf eine EC2-Instance der sechsten Generation, dass das AMI, von dem aus Sie starten, über kompatible Treiber verfügt (basierend auf dem Instance-OS gemäß der obigen Tabelle). Weitere Informationen finden Sie im AWS re:Post-Wissenszentrum unter Was muss ich tun, bevor ich meine EC2-Instance auf eine Instance der sechsten Generation migriere, um sicherzustellen, dass ich die maximale Netzwerkleistung erhalte?.

Suboptimale Leistung für die Elastic-Network-Schnittstelle

Beschreibung

Die ENA-Schnittstelle funktioniert nicht wie erwartet.

Ursache

Die Ursachenanalyse für Leistungsprobleme ist ein Eliminierungsprozess. Es sind zu viele Variablen beteiligt, um eine gängige Ursache zu nennen.

Lösung

Der erste Schritt bei der Ursachenanalyse besteht darin, die Diagnoseinformationen für die Instance, die nicht wie erwartet funktioniert, zu überprüfen, um festzustellen, ob es Fehler gibt, die das Problem verursachen könnten. Weitere Informationen finden Sie im Abschnitt Sammeln von Diagnoseinformationen über die Instance.

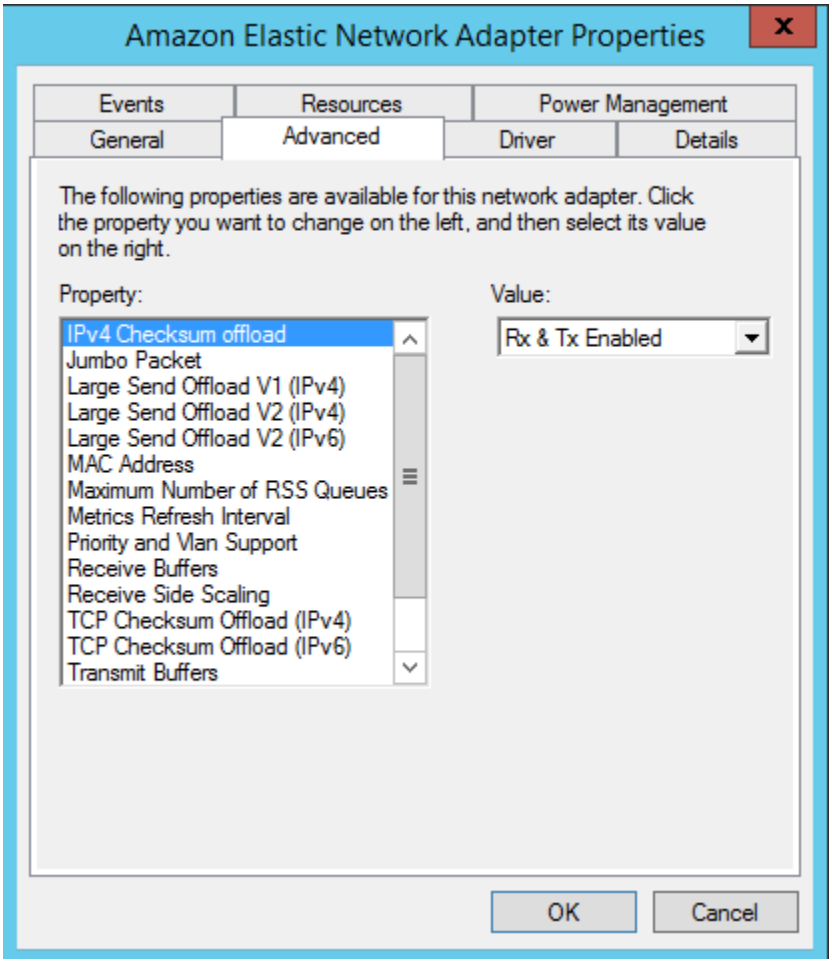
Möglicherweise müssen Sie die Standardkonfiguration des Betriebssystems ändern, um eine maximale Netzwerkleistung auf Instances mit Enhanced Networking zu erreichen. Einige Optimierungen, wie z. B. die Aktivierung des Prüfsummen-Offloads und die Aktivierung von RSS, sind in offiziellen Windows-AMIs standardmäßig konfiguriert. Weitere Optimierungen, die Sie auf den ENA-Adapter anwenden können, finden Sie in den Leistungsanpassungen unter Leistungsanpassungen des ENA-Adapters.

Wir empfehlen Ihnen, mit Vorsicht vorzugehen und nur die in diesem Abschnitt aufgeführten Geräteeigenschaften zu ändern bzw. die vom AWS-Support-Team empfohlenen Änderungen vorzunehmen.

Gehen Sie folgendermaßen vor, um die Eigenschaften des ENA-Adapters zu ändern:

1. Öffnen Sie das Dialogfeld Run (Ausführen) mit einer der im vorherigen Abschnitt beschriebenen Methoden.
2. Zum Aufrufen des Windows-Geräte-Managers geben Sie `devmgmt.msc` im Feld Run (Ausführen) ein.
3. Wählen Sie OK aus. Dadurch wird das Fenster „Device Manager“ (Geräte-Manager) geöffnet.
4. Wählen Sie den Pfeil links neben Network adapters (Netzwerkadapter) aus, um die Liste zu erweitern.
5. Wählen Sie den Namen aus oder öffnen Sie das Kontextmenü für den Amazon Elastic Network Adapter und wählen Sie dann Properties (Eigenschaften) aus. Dadurch wird das Dialogfeld mit den Eigenschaften des Amazon Elastic Network Adapters geöffnet.
6. Um Ihre Änderungen vorzunehmen, öffnen Sie die Registerkarte Erweitert.
7. Wenn Sie fertig sind, wählen Sie OK aus, um Ihre Änderungen zu speichern.

Das folgende Beispiel zeigt eine ENA-Adaptereigenschaft im Windows-Geräte-Manager:



Leistungsanpassungen des ENA-Adapters

Die folgende Tabelle enthält Eigenschaften, die angepasst werden können, um die Leistung für die ENA-Schnittstelle zu verbessern.

Eingabe

Property (Eigenschaft)	Description (Beschreibung)	Standardwert	Anpassung
Empfangspuffer	Steuert die Anzahl der Einträge in den Empfangswarteschlangen der Software.	1024	Kann auf maximal 8 192 erhöht werden.
Receive Side Scaling (RSS)	Ermöglicht die effiziente Verteilung der Netzwerkempfangsverarbeitung auf mehrere CPUs in Multiprozessorsystemen.	Aktiviert	Sie können die Last auf mehrere Prozessoren verteilen. Weitere Informationen hierzu finden Sie unter Die Netzwerkleistung in EC2-Windows-Instances optimieren.
Maximale Anzahl von RSS-Warteschlangen	Legt die maximal zulässige Anzahl von RSS-Warteschlangen fest, wenn RSS aktiviert ist.	32	Die Anzahl der RSS-Warteschlangen wird während der Treiberinitialisierung bestimmt und umfasst (unter anderem) die folgenden Beschränkungen: • Von dieser Eigenschaft

Property (Eigenschaft)	Description (Beschreibung)	Standardwert	Anpassung
			festgelegtes RSS-Warteschlangenlimit • Instance-Limits (vCPU-Anzahl) • Beschränkungen der Hardwaregenerierung (bis zu 8 RSS-Warteschlangen in ENAv1 und bis zu 32 RSS-Warteschlangen in ENAv2) Sie können einen Wert von 1–32 festlegen, je nach Ihren Beschränkungen für die Instance und Hardwaregenerierung. Weitere Informationen hierzu finden Sie unter Die Netzwerkleistung in EC2-Windows-Instances optimieren.

Property (Eigenschaft)	Description (Beschreibung)	Standardwert	Anpassung
Jumbo-Paket	Ermöglicht die Verwendung von Jumbo-Ethernet-Frames (mehr als 1 500 Byte Nutzlast).	Deaktiviert (dies begrenzt die Nutzlast auf höchstens 1 500 Byte).	Ein Wert bis zu 9015 kann festgelegt werden, was auf 9 001 Byte Nutzlast entspricht. Dies ist die maximale Nutzlast für Jumbo-Ethernet-Frames. Siehe Überlegungen zur Verwendung von Jumbo-Ethernet-Frames.

Überlegungen zur Verwendung von Jumbo-Ethernet-Frames

Für Jumbo-Frames sind mehr als 1 500 Byte an Daten zulässig, indem die Nutzlastgröße pro Paket und somit der Prozentsatz des Pakets erhöht wird, bei dem es sich nicht um Paket-Overhead handelt. Es werden weniger Pakete benötigt, um die gleiche Menge an verwendbaren Daten zu übertragen. Der Verkehr ist jedoch in folgenden Fällen auf eine maximale MTU von 1 500 beschränkt:

- Datenverkehr außerhalb einer bestimmten AWS-Region für EC2 Classic
- Datenverkehr außerhalb einer einzelnen VPC
- Datenverkehr über eine regionsübergreifende VPC-Peering-Verbindung
- Datenverkehr über VPN-Verbindungen
- Datenverkehr über ein Internet-Gateway

> **Note**
>
> Pakete über 1 500 Byte sind fragmentiert. Wenn Sie das `Don't Fragment`-Flag im IP-Header gesetzt haben, werden diese Pakete gelöscht.
> Jumbo-Frames sollten für Internet-Datenverkehr bzw. für Datenverkehr, der eine VPC verlässt, nur mit Vorsicht verwendet werden. Pakete werden durch zwischengeschaltete Systeme fragmentiert, sodass dieser Datenverkehr verlangsamt wird. Um Jumbo-

Frames innerhalb einer VPC zu verwenden, ohne den ausgehenden Datenverkehr zu beeinträchtigen, der die VPC verlässt, versuchen Sie es mit einer der folgenden Optionen:

- Konfigurieren Sie die MTU-Größe nach Route.
- Verwenden Sie mehrere Netzwerkschnittstellen mit unterschiedlichen MTU-Größen und Routen.

Empfohlene Anwendungsfälle für Jumbo-Frames

Jumbo-Frames können für den Datenverkehr innerhalb und zwischen VPCs nützlich sein. Wir empfehlen die Verwendung von Jumbo-Frames für folgende Anwendungsfälle:

- Bei Instances, die sich gemeinsam innerhalb einer Cluster-Placement-Gruppe befinden, helfen Jumbo-Frames dabei, den maximal möglichen Netzwerkdurchsatz zu erzielen. Weitere Informationen finden Sie unter Platzierungsgruppen für Ihre Amazon-EC2-Instances.
- Sie können für Datenverkehr zwischen Ihren VPCs und Ihren On-Premises-Netzwerken über Jumbo-Frames verwende Direct Connect. Weitere Informationen zur Verwendung von Direct Connect und zum Überprüfen der Jumbo-Frame-Funktionalität finden Sie unter MTU für private virtuelle Schnittstellen oder virtuelle Transitschnittstellen im Direct Connect-Benutzerhandbuch.
- Weitere Informationen zu unterstützten MTU-Größen für Transit Gateways finden Sie unter Kontingente für Ihre Transit Gateways in Amazon VPC Transit Gateways.

Verbessern Sie die Netzwerkleistung zwischen EC2 Instanzen mit ENA Express

ENA Express basiert auf der SRD-Technologie (AWS Scalable Reliable Datagram). SRD ist ein leistungsstarkes Netzwerktransportprotokoll, das dynamisches Routing verwendet, um den Durchsatz zu erhöhen und die Tail-Latenz zu minimieren. Mit ENA Express können Sie zwischen zwei EC2 Instances in derselben Availability Zone kommunizieren.

Vorteile von ENA Express

- Erhöht die maximale Bandbreite, die ein einzelner Datenablauf nutzen kann, von 5 Gbit/s auf 25 Gbit/s innerhalb der Availability Zone bis zum aggregierten Instance-Limit.
- Reduziert die Latenz des Netzwerkverkehrs zwischen EC2 Instances am Ende, insbesondere in Zeiten hoher Netzwerklast.

- Erkennt und vermeidet überlastete Netzwerkpfade.
- Führt einige Aufgaben direkt auf der Netzwerkebene aus, z. B. die Neuordnung von Paketen auf der Empfängerseite und die meisten erforderlichen Neuübertragungen. Dadurch wird die Anwendungsebene für andere Arbeiten freigegeben.

> **Note**
>
> - Wenn Ihre Anwendung ein hohes Volumen an Paketen pro Sekunde sendet oder empfängt und die meiste Zeit auf Latenz optimiert werden muss, insbesondere in Zeiten ohne Überlastung des Netzwerks, ist Enhanced Networking möglicherweise besser für Ihr Netzwerk geeignet.
> - ENA-Express-Datenverkehr kann nicht in einer Local Zone gesendet werden.

Nachdem Sie ENA Express für den Netzwerkschnittstellen-Anhang auf einer Instance aktiviert haben, initiiert die sendende Instance die Kommunikation mit der empfangenden Instance und SRD erkennt, ob ENA Express sowohl auf der sendenden als auch auf der empfangenden Instance ausgeführt wird. Wenn ENA Express in Betrieb ist, kann die Kommunikation eine SRD-Übertragung verwenden. Wenn ENA Express nicht funktioniert, fällt die Kommunikation auf die standardmäßige ENA-Übertragung zurück.

In Zeiträumen mit geringem Netzwerkverkehr bemerken Sie möglicherweise eine leichte Erhöhung der Paketlatenz (mehrere zehn Mikrosekunden), wenn das Paket ENA Express verwendet. Während dieser Zeiten können Anwendungen, die bestimmte Netzwerkleistungsmerkmale priorisieren, von ENA Express wie folgt profitieren:

- Prozesse können von einer erhöhten maximalen Bandbreite für einzelne Abläufe von 5 Gbit/s auf 25 Gbit/s innerhalb derselben Availability Zone bis zum aggregierten Instance-Limit profitieren. Wenn ein bestimmter Instance-Typ beispielsweise bis zu 12,5 Gbit/s unterstützt, ist die Single-Flow-Bandbreite ebenfalls auf 12,5 Gbit/s begrenzt.
- Länger ausgeführte Prozesse sollten in Zeiten der Netzwerküberlastung eine geringere Latenz aufweisen.
- Prozesse können von einer gleichmäßigeren und einheitlicheren Verteilung der Reaktionszeiten des Netzwerks profitieren.

Themen

- So funktioniert ENA Express
- Unterstützte Instance-Typen für ENA Express
- Voraussetzungen für Linux-Instances
- Die Leistung der ENA-Express-Einstellungen auf Linux-Instances erhöhen
- Überprüfen Sie die ENA Express-Einstellungen für Ihre Instanz EC2
- Konfigurieren Sie die ENA Express-Einstellungen für Ihre EC2 Instance

So funktioniert ENA Express

ENA Express basiert auf der SRD-Technologie (AWS Scalable Reliable Datagram). Sie verteilt Pakete für jeden Netzwerkfluss auf verschiedene AWS Netzwerkpfade und passt die Verteilung dynamisch an, wenn Anzeichen einer Überlastung erkannt werden. Sie verwaltet auch die Neuordnung von Paketen auf der Empfängerseite.

Um sicherzustellen, dass ENA Express den Netzwerkverkehr wie vorgesehen verwalten kann, müssen sendende und empfangende Instances, sowie die Kommunikation zwischen ihnen, alle nachstehenden Anforderungen erfüllen:

- Sowohl sendende als auch empfangende Instance-Typen werden unterstützt. Weitere Informationen finden Sie in der Unterstützte Instance-Typen für ENA Express-Tabelle.
- Sowohl die sendenden als auch die empfangenden Instances müssen ENA Express konfiguriert haben. Wenn es Unterschiede in der Konfiguration gibt, kann es zu Situationen kommen, in denen der Datenverkehr standardmäßig auf die ENA-Standardübertragung umgestellt wird. Das folgende Szenario zeigt, was in diesem Fall passieren kann.

  Szenario: Unterschiede in der Konfiguration

Instance	ENA Express aktiviert	UDP verwendet ENA Express
Instance 1	Ja	Ja
Instance 2	Ja	Nein

  In diesem Fall kann für den TCP-Verkehr zwischen den beiden Instances ENA Express verwendet werden, da beide Instances dies aktiviert haben. Da jedoch eine der Instances ENA Express nicht

für den UDP-Verkehr verwendet, verwendet die Kommunikation zwischen diesen beiden Instances via UDP die ENA-Standardübertragung.

- Die sendenden und empfangenden Instances müssen in derselben Availability Zone laufen.
- Der Netzwerkpfad zwischen den Instances darf keine Middleware-Boxen enthalten. ENA Express unterstützt derzeit keine Middleware-Boxen.
- (Nur Linux-Instances) Um das volle Bandbreitenpotenzial zu nutzen, verwenden Sie die Treiberversion 2.2.9 oder höher.
- (Nur Linux-Instances) Verwenden Sie zum Erstellen von Metriken die Treiberversion 2.8 oder höher.

Wenn eine Anforderung nicht erfüllt wird, verwenden die Instanzen das TCP/UDP Standardprotokoll, jedoch ohne SRD für die Kommunikation.

Um sicherzustellen, dass Ihr Instance-Netzwerktreiber für eine optimale Leistung konfiguriert ist, lesen Sie sich die empfohlenen bewährten Methoden für ENA-Treiber durch. Diese bewährten Methoden gelten auch für ENA Express. Weitere Informationen finden Sie im ENA Linux Driver Best Practices and Performance Optimization Guide auf der GitHub Website.

> **Note**
>
> Amazon EC2 bezeichnet die Beziehung zwischen einer Instance und einer Netzwerkschnittstelle, die an sie angehängt ist, als Anlage. Die ENA-Express-Einstellungen gelten für den Anhang. Wenn die Netzwerkschnittstelle von der Instance getrennt ist, existiert der Anhang nicht mehr und die ENA-Express-Einstellungen, die für ihn galten, sind nicht mehr gültig. Das Gleiche gilt, wenn eine Instance beendet wird, auch wenn die Netzwerkschnittstelle erhalten bleibt.

Nachdem Sie ENA Express für die Netzwerkschnittstellen-Anhänge sowohl auf der sendenden als auch auf der empfangenden Instance aktiviert haben, können Sie ENA-Express-Metriken verwenden, um dabei zu helfen, sicherzustellen, dass Ihre Instances die Leistungsverbesserungen der SRD-Technologie voll ausschöpfen. Weitere Informationen zu ENA-Express-Metriken finden Sie unter Metriken für ENA Express.

Unterstützte Instance-Typen für ENA Express

Folgende Instance-Typen unterstützen ENA Express.

General purpose

Instance-Typ	Architektur
m6a.12xlarge	x86_64
m6a.16xlarge	x86_64
m6a.24xlarge	x86_64
m6a.32xlarge	x86_64
m6a.48xlarge	x86_64
m6a.metal	x86_64
m6i.8xlarge	x86_64
m6i.12xlarge	x86_64
m6i.16xlarge	x86_64
m6i.24xlarge	x86_64
m6i.32xlarge	x86_64
m6i.metal	x86_64
m6id.8xlarge	x86_64
m6id.12xlarge	x86_64
m6id.16xlarge	x86_64
m6id.24xlarge	x86_64
m6id.32xlarge	x86_64
m6id.metal	x86_64
m6idn.8xlarge	x86_64

Instance-Typ	Architektur
m6idn.12xlarge	x86_64
m6idn.16xlarge	x86_64
m6idn.24xlarge	x86_64
m6idn.32xlarge	x86_64
m6idn.metal	x86_64
m6in.8xlarge	x86_64
m6in.12xlarge	x86_64
m6in.16xlarge	x86_64
m6in.24xlarge	x86_64
m6in.32xlarge	x86_64
m6in.metal	x86_64
m7a.12xlarge	x86_64
m7a.16xlarge	x86_64
m7a.24xlarge	x86_64
m7a.32xlarge	x86_64
m7a.48xlarge	x86_64
m7a.metal-48xl	x86_64
m7g.12xlarge	arm64
m7g.16xlarge	arm64
m7g.metal	arm64

Instance-Typ	Architektur
m7gd.12xlarge	arm64
m7gd.16xlarge	arm64
m7gd.metal	arm64
m7i.12xlarge	x86_64
m7i.16xlarge	x86_64
m7i.24xlarge	x86_64
m7i.48xlarge	x86_64
m7i.metal-24xl	x86_64
m7i.metal-48xl	x86_64
m8a.16xlarge	x86_64
m8a.24xlarge	x86_64
m8a.48xlarge	x86_64
m8a.metal-24xl	x86_64
m8a.metal-48xl	x86_64
m8g.12xlarge	arm64
m8g.16xlarge	arm64
m8g.24xlarge	arm64
m8g.48xlarge	arm64
m8g.metal-24xl	arm64
m8g.metal-48xl	arm64

Instance-Typ	Architektur
m8gd.12xlarge	arm64
m8gd.16xlarge	arm64
m8gd.24xlarge	arm64
m8gd.48xlarge	arm64
m8gd.metal-24xl	arm64
m8gd.metal-48xl	arm64
m8i.24xlarge	x86_64
m8i.32xlarge	x86_64
m8i.48xlarge	x86_64
m8i.96xlarge	x86_64
m8i.metal-48xl	x86_64
m8i.metal-96xl	x86_64

Compute optimized

Instance-Typ	Architektur
c6a.12xlarge	x86_64
c6a.16xlarge	x86_64
c6a.24xlarge	x86_64
c6a.32xlarge	x86_64
c6a.48xlarge	x86_64

Instance-Typ	Architektur
c6a.metal	x86_64
c6gn.4xlarge	arm64
c6gn.8xlarge	arm64
c6gn.12xlarge	arm64
c6gn.16xlarge	arm64
c6i.8xlarge	x86_64
c6i.12xlarge	x86_64
c6i.16xlarge	x86_64
c6i.24xlarge	x86_64
c6i.32xlarge	x86_64
c6i.metal	x86_64
c6id.8xlarge	x86_64
c6id.12xlarge	x86_64
c6id.16xlarge	x86_64
c6id.24xlarge	x86_64
c6id.32xlarge	x86_64
c6id.metal	x86_64
c6in.8xlarge	x86_64
c6in.12xlarge	x86_64
c6in.16xlarge	x86_64

Instance-Typ	Architektur
c6in.24xlarge	x86_64
c6in.32xlarge	x86_64
c6in.metal	x86_64
c7a.12xlarge	x86_64
c7a.16xlarge	x86_64
c7a.24xlarge	x86_64
c7a.32xlarge	x86_64
c7a.48xlarge	x86_64
c7a.metal-48xl	x86_64
c7g.12xlarge	arm64
c7g.16xlarge	arm64
c7g.metal	arm64
c7gd.12xlarge	arm64
c7gd.16xlarge	arm64
c7gd.metal	arm64
c7gn.4xlarge	arm64
c7gn.8xlarge	arm64
c7gn.12xlarge	arm64
c7gn.16xlarge	arm64
c7gn.metal	arm64

Instance-Typ	Architektur
c7i.12xlarge	x86_64
c7i.16xlarge	x86_64
c7i.24xlarge	x86_64
c7i.48xlarge	x86_64
c7i.metal-24xl	x86_64
c7i.metal-48xl	x86_64
c8a.16xlarge	x86_64
c8a.24xlarge	x86_64
c8a.48xlarge	x86_64
c8a.metal-24xl	x86_64
c8a.metal-48xl	x86_64
c8g.12xlarge	arm64
c8g.16xlarge	arm64
c8g.24xlarge	arm64
c8g.48xlarge	arm64
c8g.metal-24xl	arm64
c8g.metal-48xl	arm64
c8gb.8xlarge	arm64
c8gb.12xlarge	arm64
c8gb.16xlarge	arm64

Instance-Typ	Architektur
c8gb.24xlarge	arm64
c8gb.metal-24xl	arm64
c8gd.12xlarge	arm64
c8gd.16xlarge	arm64
c8gd.24xlarge	arm64
c8gd.48xlarge	arm64
c8gd.metal-24xl	arm64
c8gd.metal-48xl	arm64
c8gn.8xlarge	arm64
c8gn.12xlarge	arm64
c8gn.16xlarge	arm64
c8gn.24xlarge	arm64
c8gn.48xlarge	arm64
c8gn.metal-24xl	arm64
c8gn.metal-48xl	arm64
c8i.24xlarge	x86_64
c8i.32xlarge	x86_64
c8i.48xlarge	x86_64
c8i.96xlarge	x86_64
c8i.metal-48xl	x86_64

Instance-Typ	Architektur
c8i.metal-96xl	x86_64

Memory optimized

Instance-Typ	Architektur
r6a.12xlarge	x86_64
r6a.16xlarge	x86_64
r6a.24xlarge	x86_64
r6a.32xlarge	x86_64
r6a.48xlarge	x86_64
r6a.metal	x86_64
r6i.8xlarge	x86_64
r6i.12xlarge	x86_64
r6i.16xlarge	x86_64
r6i.24xlarge	x86_64
r6i.32xlarge	x86_64
r6i.metal	x86_64
r6id.8xlarge	x86_64
r6id.12xlarge	x86_64
r6id.16xlarge	x86_64
r6id.24xlarge	x86_64

Instance-Typ	Architektur
r6id.32xlarge	x86_64
r6id.metal	x86_64
r6idn.8xlarge	x86_64
r6idn.12xlarge	x86_64
r6idn.16xlarge	x86_64
r6idn.24xlarge	x86_64
r6idn.32xlarge	x86_64
r6idn.metal	x86_64
r6in.8xlarge	x86_64
r6in.12xlarge	x86_64
r6in.16xlarge	x86_64
r6in.24xlarge	x86_64
r6in.32xlarge	x86_64
r6in.metal	x86_64
r7a.12xlarge	x86_64
r7a.16xlarge	x86_64
r7a.24xlarge	x86_64
r7a.32xlarge	x86_64
r7a.48xlarge	x86_64
r7a.metal-48xl	x86_64

Instance-Typ	Architektur
r7g.12xlarge	arm64
r7g.16xlarge	arm64
r7g.metal	arm64
r7gd.12xlarge	arm64
r7gd.16xlarge	arm64
r7gd.metal	arm64
r7i.12xlarge	x86_64
r7i.16xlarge	x86_64
r7i.24xlarge	x86_64
r7i.48xlarge	x86_64
r7i.metal-24xl	x86_64
r7i.metal-48xl	x86_64
r7iz.8xlarge	x86_64
r7iz.12xlarge	x86_64
r7iz.16xlarge	x86_64
r7iz.32xlarge	x86_64
r7iz.metal-16xl	x86_64
r7iz.metal-32xl	x86_64
r8a.16xlarge	x86_64
r8a.24xlarge	x86_64

Instance-Typ	Architektur
r8a.48xlarge	x86_64
r8a.metal-24xl	x86_64
r8a.metal-48xl	x86_64
r8g.12xlarge	arm64
r8g.16xlarge	arm64
r8g.24xlarge	arm64
r8g.48xlarge	arm64
r8g.metal-24xl	arm64
r8g.metal-48xl	arm64
r8gb.8xlarge	arm64
r8gb.12xlarge	arm64
r8gb.16xlarge	arm64
r8gb.24xlarge	arm64
r8gb.metal-24xl	arm64
r8gd.12xlarge	arm64
r8gd.16xlarge	arm64
r8gd.24xlarge	arm64
r8gd.48xlarge	arm64
r8gd.metal-24xl	arm64
r8gd.metal-48xl	arm64

Instance-Typ	Architektur
r8gn.8xlarge	arm64
r8gn.12xlarge	arm64
r8gn.16xlarge	arm64
r8gn.24xlarge	arm64
r8gn.48xlarge	arm64
r8gn.metal-24xl	arm64
r8gn.metal-48xl	arm64
r8i.24xlarge	x86_64
r8i.32xlarge	x86_64
r8i.48xlarge	x86_64
r8i.96xlarge	x86_64
r8i.metal-48xl	x86_64
r8i.metal-96xl	x86_64
u7i-6tb.112xlarge	x86_64
u7i-8tb.112xlarge	x86_64
u7i-12tb.224xlarge	x86_64
u7in-16tb.224xlarge	x86_64
u7in-24tb.224xlarge	x86_64
u7in-32tb.224xlarge	x86_64
u7inh-32tb.480xlarge	x86_64

Instance-Typ	Architektur
x2idn.16xlarge	x86_64
x2idn.24xlarge	x86_64
x2idn.32xlarge	x86_64
x2idn.metal	x86_64
x2iedn.8xlarge	x86_64
x2iedn.16xlarge	x86_64
x2iedn.24xlarge	x86_64
x2iedn.32xlarge	x86_64
x2iedn.metal	x86_64
x8g.12xlarge	arm64
x8g.16xlarge	arm64
x8g.24xlarge	arm64
x8g.48xlarge	arm64
x8g.metal-24xl	arm64
x8g.metal-48xl	arm64
x8aedz.24xlarge	x86_64
x8aedz.metal-24xl	x86_64

Accelerated computing

Instance-Typ	Architektur
g6.48xlarge	x86_64
g6e.12xlarge	x86_64
g6e.24xlarge	x86_64
g6e.48xlarge	x86_64
p5.48xlarge	x86_64
p5e.48xlarge	x86_64
p5en.48xlarge	x86_64
p6-b200.48xlarge	x86_64
p6-b300.48xlarge	x86_64

Storage optimized

Instance-Typ	Architektur
i4g.4xlarge	arm64
i4g.8xlarge	arm64
i4g.16xlarge	arm64
i4i.8xlarge	x86_64
i4i.12xlarge	x86_64
i4i.16xlarge	x86_64
i4i.24xlarge	x86_64

Instance-Typ	Architektur
i4i.32xlarge	x86_64
i4i.metal	x86_64
i7i.12xlarge	x86_64
i7i.16xlarge	x86_64
i7i.24xlarge	x86_64
i7i.48xlarge	x86_64
i7i.metal-24xl	x86_64
i7i.metal-48xl	x86_64
i7ie.12xlarge	x86_64
i7ie.18xlarge	x86_64
i7ie.24xlarge	x86_64
i7ie.48xlarge	x86_64
i7ie.metal-24xl	x86_64
i7ie.metal-48xl	x86_64
i8g.12xlarge	arm64
i8g.16xlarge	arm64
i8g.24xlarge	arm64
i8g.48xlarge	arm64
i8g.metal-24xl	arm64
i8ge.12xlarge	arm64

Instance-Typ	Architektur
i8ge.18xlarge	arm64
i8ge.24xlarge	arm64
i8ge.48xlarge	arm64
i8ge.metal-24xl	arm64
i8ge.metal-48xl	arm64
im4gn.4xlarge	arm64
im4gn.8xlarge	arm64
im4gn.16xlarge	arm64

Voraussetzungen für Linux-Instances

Um sicherzustellen, dass ENA Express effektiv funktionieren kann, aktualisieren Sie die Einstellungen für Ihre Instance wie folgt.

- Wenn Ihre Instance Jumbo-Frames verwendet, führen Sie den folgenden Befehl aus, um Ihre maximale Übertragungseinheit (MTU) auf 8900 festzulegen.

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 8900
```

- Erhöhen Sie die Ringgröße des Empfängers (Rx) wie folgt:

```
[ec2-user ~]$ ethtool -G device rx 8192
```

- Um die ENA-Express-Bandbreite zu maximieren, konfigurieren Sie Ihre TCP-Warteschlangenlimits wie folgt:

  1. Legen Sie den Grenzwert für die kleine TCP-Warteschlange auf 1 MB oder höher fest. Dadurch erhöht sich die Datenmenge, die für die Übertragung auf einem Socket in der Warteschlange steht.

```
sudo sh -c 'echo 1048576 > /proc/sys/net/ipv4/tcp_limit_output_bytes'
```

2. Deaktivieren Sie Byte-Warteschlangenlimits auf dem ETH-Gerät, wenn diese für Ihre Linux-Distribution aktiviert sind. Dadurch erhöht sich die Anzahl der für die Übertragung in der Gerätewarteschlange anstehenden Daten.

```
sudo sh -c 'for txq in /sys/class/net/eth0/queues/tx-*; do echo max > ${txq}/
byte_queue_limits/limit_min; done'
```

> **Note**
>
> Der ENA-Treiber für die Amazon-Linux-Distribution deaktiviert standardmäßig die Byte-Warteschlangenlimits.

Die Leistung der ENA-Express-Einstellungen auf Linux-Instances erhöhen

Um Ihre Linux-Instance-Konfiguration auf optimale ENA Express-Leistung zu überprüfen, können Sie das folgende Skript ausführen, das im GitHub Amazon-Repository verfügbar ist:

https://github.com/amzn/amzn-ec2-ena-.sh utilities/blob/main/ena-express/check ena-express-settings

Das Skript führt eine Reihe von Tests durch und schlägt sowohl empfohlene als auch erforderliche Konfigurationsänderungen vor.

Überprüfen Sie die ENA Express-Einstellungen für Ihre Instanz EC2

Sie können die ENA Express-Einstellungen nach Instance oder Netzwerkschnittstelle überprüfen. Informationen zum Aktualisieren der ENA Express-Einstellungen finden Sie unter the section called “Konfigurieren der Instance”.

Console

So zeigen der ENA-Express-Einstellungen für eine Netzwerkschnittstelle an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich Network interfaces (Netzwerkschnittstellen) aus.

3. Wählen Sie eine Netzwerkschnittstelle aus, um Details für diese Instance zu sehen. Sie können den Link Network interface ID (Netzwerkschnittstellen-ID) wählen, um die Detailseite zu öffnen oder Sie können das Kontrollkästchen auf der linken Seite der Liste aktivieren, um Details im Detailbereich unten auf der Seite anzuzeigen.
4. Überprüfen Sie im Abschnitt Netzwerkschnittstellen-Anhang auf der Registerkarte Details oder auf der Detailseite die Einstellungen für ENA Express und ENA Express UDP.

So überprüfen Sie die ENA-Express-Einstellungen für eine Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. Wählen Sie eine Instance aus, um die Details der Instance anzuzeigen. Sie können den Link Instance ID (Instance-ID) wählen, um die Detailseite zu öffnen oder Sie können das Kontrollkästchen auf der linken Seite der Liste aktivieren, um Details im Detailbereich unten auf der Seite anzuzeigen.
4. Scrollen Sie im Abschnitt Network interfaces (Netzwerkschnittstellen) auf der Registerkarte Networking (Vernetzung) nach rechts, um die Einstellungen für ENA Express und ENA Express UDP zu überprüfen.

AWS CLI

So rufen Sie die ENA-Express-Einstellungen für eine Instance ab

Verwenden Sie den Befehl describe-instances. Dieses Befehlsbeispiel gibt eine Liste der ENA Express-Konfigurationen für die Netzwerkschnittstellen zurück, die an jede der laufenden Instances angeschlossen sind, die durch den `--instance-ids`-Parameter angegeben sind.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7 \
    --query 'Reservations[*].Instances[*].[InstanceId,
 NetworkInterfaces[*].Attachment.EnaSrdSpecification]'
```

Es folgt eine Beispielausgabe.

```
[
    [
        [
            "i-1234567890abcdef0",
```

```
            [
                {
                    "EnaSrdEnabled": true,
                    "EnaSrdUdpSpecification": {
                        "EnaSrdUdpEnabled": false
                    }
                }
            ]
        ]
    ],
    [
        [
            "i-0598c7d356eba48d7",
            [
            {
                    "EnaSrdEnabled": true,
                    "EnaSrdUdpSpecification": {
                        "EnaSrdUdpEnabled": false
                    }
                }
            ]
        ]
    ]
]
```

So rufen Sie die ENA-Express-Einstellungen für eine Netzwerkschnittstelle ab

Verwenden Sie den Befehl describe-network-interfaces.

```
aws ec2 describe-network-interfaces \
    --network-interface-ids eni-1234567890abcdef0 \
    --query NetworkInterfaces[].[NetworkInterfaceId,Attachment.EnaSrdSpecification]
```

Es folgt eine Beispielausgabe.

```
[
    [
        "eni-1234567890abcdef0",
        {
            "EnaSrdEnabled": true,
            "EnaSrdUdpSpecification": {
                "EnaSrdUdpEnabled": false
            }
```

```
        }
    ]
]
```

PowerShell

So rufen Sie die ENA-Express-Einstellungen für eine Netzwerkschnittstelle ab

Verwenden Sie das cmdlet Get-EC2NetworkInterface.

```
Get-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0 | `
Select-Object `
    Association,
    NetworkInterfaceId,
    OwnerId,
    @{Name = 'AttachTime'; Expression = { $_.Attachment.AttachTime } },
    @{Name = 'AttachmentId'; Expression = { $_.Attachment.AttachmentId } },
    @{Name = 'DeleteOnTermination'; Expression =
 { $_.Attachment.DeleteOnTermination } },
    @{Name = 'NetworkCardIndex'; Expression = { $_.Attachment.NetworkCardIndex } },
    @{Name = 'InstanceId'; Expression = { $_.Attachment.InstanceId } },
    @{Name = 'InstanceOwnerId'; Expression = { $_.Attachment.InstanceOwnerId } },
    @{Name = 'Status'; Expression = { $_.Attachment.Status } },
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled } },
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled } }
```

Es folgt eine Beispielausgabe.

```
Association         :
NetworkInterfaceId  : eni-0d1234e5f6a78901b
OwnerId             : 111122223333
AttachTime          : 6/11/2022 1:13:11 AM
AttachmentId        : eni-attach-0d1234e5f6a78901b
DeleteOnTermination : True
NetworkCardIndex    : 0
InstanceId          : i-1234567890abcdef0
InstanceOwnerId     : 111122223333
Status              : attached
EnaSrdEnabled       : True
EnaSrdUdpEnabled    : False
```

Konfigurieren Sie die ENA Express-Einstellungen für Ihre EC2 Instance

Sie können ENA Express für unterstützte EC2 Instance-Typen konfigurieren, ohne zusätzliche Software installieren zu müssen. Weitere Informationen finden Sie unter the section called “Unterstützte Instance-Typen für ENA Express”.

Console

So verwalten Sie die ENA-Express-Einstellungen für eine Netzwerkschnittstelle

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich Network interfaces (Netzwerkschnittstellen) aus.
3. Wählen Sie eine Netzwerkschnittstelle aus, die an eine Instance angehängt ist. Sie können den Link Network interface ID (Netzwerkschnittstellen-ID) wählen, um die Detailseite zu öffnen oder Sie können das Kontrollkästchen auf der linken Seite der Liste auswählen.
4. Wählen Sie im Menü Action (Aktion) oben rechts auf der Seite die Option Manage ENA Express (ENA Express verwalten) aus. Dadurch wird das Dialogfeld Manage ENA Express (ENA Express verwalten) geöffnet, in dem die ausgewählte Netzwerkschnittstellen-ID und die aktuellen Einstellungen angezeigt werden.

   Wenn die von Ihnen gewählte Netzwerkschnittstelle nicht mit einer Instance verbunden ist, wird diese Aktion nicht im Menü angezeigt.
5. Um ENA Express zu verwenden, wählen Sie das Kontrollkästchen Aktivieren aus.
6. Wenn ENA Express aktiviert ist, können Sie die UDP-Einstellungen konfigurieren. Um ENA Express UDP zu verwenden, wählen Sie das Kontrollkästchen Aktivieren aus.
7. Um Ihre Einstellungen zu speichern, wählen Sie Save (Speichern).

So verwalten Sie ENA Express für eine Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. Wählen Sie die Instance aus, die Sie verwalten möchten. Sie können den Link Instance ID (Instance-ID) wählen, um die Detailseite zu öffnen oder Sie können das Kontrollkästchen auf der linken Seite der Liste auswählen.
4. Wählen Sie die Network interface (Netzwerkschnittstelle) aus, die Sie für Ihre Instance konfigurieren möchten.

5. Wählen Sie im Menü Action (Aktion) oben rechts auf der Seite die Option Manage ENA Express (ENA Express verwalten) aus.
6. Um ENA Express für eine Netzwerkschnittstelle zu konfigurieren, die an Ihre Instance angeschlossen ist, wählen Sie sie aus der Liste der Network interface (Netzwerkschnittstelle) aus.
7. Um ENA Express für den ausgewählten Netzwerkschnittstellenanhang zu verwenden, aktivieren Sie das Kontrollkästchen Aktivieren.
8. Wenn ENA Express aktiviert ist, können Sie die UDP-Einstellungen konfigurieren. Um ENA Express UDP zu verwenden, wählen Sie das Kontrollkästchen Aktivieren aus.
9. Um Ihre Einstellungen zu speichern, wählen Sie Save (Speichern).

So konfigurieren Sie ENA Express, wenn Sie eine Netzwerkschnittstelle anhängen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich Network interfaces (Netzwerkschnittstellen) aus.
3. Wählen Sie eine Netzwerkschnittstelle aus, die nicht an eine Instance angeschlossen ist (Status ist Available (Verfügbar)). Sie können den Link Network interface ID (Netzwerkschnittstellen-ID) wählen, um die Detailseite zu öffnen oder Sie können das Kontrollkästchen auf der linken Seite der Liste auswählen.
4. Wählen Sie die Instance aus, an die Sie anhängen möchten.
5. Um ENA Express zu verwenden, nachdem Sie die Netzwerkschnittstelle an die Instance angefügt haben, aktivieren Sie das Kontrollkästchen Aktivieren.
6. Wenn ENA Express aktiviert ist, können Sie die UDP-Einstellungen konfigurieren. Um ENA Express UDP zu verwenden, wählen Sie das Kontrollkästchen Aktivieren aus.
7. Um die Netzwerkschnittstelle an die Instance anzuschließen und Ihre ENA Express-Einstellungen zu speichern, wählen Sie Attach (Anhängen).

AWS CLI

So konfigurieren Sie ENA Express, wenn Sie eine Netzwerkschnittstelle anhängen

Verwenden Sie den Befehl attach-network-interface, wie in den folgenden Beispielen gezeigt.

Beispiel 1: ENA Express für den TCP-Datenverkehr verwenden, aber nicht für den UDP-Datenverkehr

Dieses Beispiel konfiguriert `EnaSrdEnabled` als `true` und erlaubt `EnaSrdUdpEnabled` auf die Standardeinstellung `false` zu wechseln.

```
aws ec2 attach-network-interface \
    --network-interface-id eni-1234567890abcdef0 \
    --instance-id i-1234567890abcdef0 \
    --device-index 1 \
    --ena-srd-specification 'EnaSrdEnabled=true'
```

Beispiel 2: Verwenden von ENA Express sowohl für den TCP-Verkehr als auch für den UDP-Verkehr

In diesem Beispiel werden sowohl `EnaSrdEnabled` und `EnaSrdUdpEnabled` als `true` konfiguriert.

```
aws ec2 attach-network-interface \
    --network-interface-id eni-1234567890abcdef0 \
    --instance-id i-1234567890abcdef0 \
    --device-index 1 \
    --ena-srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
```

So aktualisieren Sie die ENA-Express-Einstellungen für einen Netzwerkschnittstellen-Anhang

Verwenden Sie den Befehl modify-network-interface-attribute, wie in den folgenden Beispielen gezeigt.

Beispiel 1: ENA Express für den TCP-Datenverkehr verwenden, aber nicht für den UDP-Datenverkehr

Dieses Beispiel konfiguriert `EnaSrdEnabled` als `true` und erlaubt es `EnaSrdUdpEnabled`, standardmäßig auf `false` zu wechseln, wenn es zuvor noch nie eingestellt wurde.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --ena-srd-specification 'EnaSrdEnabled=true'
```

Beispiel 2: Verwenden von ENA Express sowohl für den TCP-Verkehr als auch für den UDP-Verkehr

In diesem Beispiel werden sowohl `EnaSrdEnabled` und `EnaSrdUdpEnabled` als `true` konfiguriert.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --ena-srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
```

Beispiel 3: Beenden der Verwendung von ENA Express für den UDP-Verkehr

In diesem Beispiel wird `EnaSrdUdpEnabled` als `false` konfiguriert.

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-1234567890abcdef0 \
    --ena-srd-specification 'EnaSrdUdpSpecification={EnaSrdUdpEnabled=false}'
```

PowerShell

So konfigurieren Sie ENA Express, wenn Sie eine Netzwerkschnittstelle anhängen

Verwenden Sie das cmdlet Add-EC2NetworkInterface, wie in den folgenden Beispielen gezeigt.

Beispiel 1: ENA Express für den TCP-Datenverkehr verwenden, aber nicht für den UDP-Datenverkehr

Dieses Beispiel konfiguriert `EnaSrdEnabled` als `true` und erlaubt `EnaSrdUdpEnabled` auf die Standardeinstellung `false` zu wechseln.

```
Add-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -InstanceId i-1234567890abcdef0 `
    -DeviceIndex 1 `
    -EnaSrdSpecification_EnaSrdEnabled $true
```

Beispiel 2: Verwenden von ENA Express sowohl für den TCP-Verkehr als auch für den UDP-Verkehr

In diesem Beispiel werden sowohl `EnaSrdEnabled` und `EnaSrdUdpEnabled` als `true` konfiguriert.

```
Add-EC2NetworkInterface `
    -NetworkInterfaceId eni-1234567890abcdef0 `
```

```
    -InstanceId i-1234567890abcdef0 `
    -DeviceIndex 1 `
    -EnaSrdSpecification_EnaSrdEnabled $true `
    -EnaSrdUdpSpecification_EnaSrdUdpEnabled $true
```

So aktualisieren Sie die ENA-Express-Einstellungen für Ihren Netzwerkschnittstellen-Anhang

Verwenden Sie das cmdlet Edit-EC2NetworkInterfaceAttribute, wie in den folgenden Beispielen gezeigt.

Beispiel 1: ENA Express für den TCP-Datenverkehr verwenden, aber nicht für den UDP-Datenverkehr

Dieses Beispiel konfiguriert `EnaSrdEnabled` als `true` und erlaubt es `EnaSrdUdpEnabled`, standardmäßig auf `false` zu wechseln, wenn es zuvor noch nie eingestellt wurde.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -EnaSrdSpecification_EnaSrdEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List
```

Beispiel 2: Verwenden von ENA Express sowohl für den TCP-Verkehr als auch für den UDP-Verkehr

In diesem Beispiel werden sowohl `EnaSrdEnabled` und `EnaSrdUdpEnabled` als `true` konfiguriert.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-1234567890abcdef0 `
    -EnaSrdSpecification_EnaSrdEnabled $true `
    -EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-1234567890abcdef0 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
```

```
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List
```

Beispiel 3: Beenden der Verwendung von ENA Express für den UDP-Verkehr

In diesem Beispiel wird `EnaSrdUdpEnabled` als `false` konfiguriert.

```
Edit-EC2NetworkInterfaceAttribute `
    -NetworkInterfaceId eni-0123f4567890a1b23 `
    -EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $false ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List
```

Konfigurieren von ENA Express beim Start

Sie können eine der folgenden Methoden verwenden, um ENA Express für ein AMI zu konfigurieren, wenn Sie eine Instance starten. Die angegebenen Links verweisen Sie auf die AWS-Managementkonsole Anweisungen für diese Methoden.

- Launch Instance Wizard – Sie können ENA Express beim Start mit dem Launch Instance Wizard konfigurieren. Ausführliche Informationen zur Konfiguration finden Sie unter Erweiterte Netzwerkkonfiguration in den Netzwerkeinstellungen für den Launch Instance Wizard.
- Startvorlage – Sie können ENA Express beim Start konfigurieren, wenn Sie eine Startvorlage verwenden. Weitere Informationen finden Sie auf der Seite Erstellen Sie eine EC2 Amazon-Startvorlage. Erweitern Sie dann den Abschnitt Netzwerkeinstellungen und überprüfen Sie die Erweiterte Netzwerkkonfiguration.

Erweitertes Netzwerk mit der Intel 82599 VF-Schnittstelle

Für XEN-basierte Instances bietet die Intel 82599 Virtual Function (VF)-Schnittstelle erweiterte Netzwerkfunktionen. Die Schnittstelle verwendet den Intel-`ixgbevf`-Treiber.

Die folgenden Registerkarten zeigen, wie Sie den Netzwerkadaptertreiber überprüfen können, der für Ihr Instance-Betriebssystem installiert ist.

Linux

Linux-Netzwerkschnittstellentreiber

Prüfen Sie mit dem folgenden Befehl, ob das Modul aktuell an einer bestimmten Schnittstelle verwendet wird; setzen Sie dabei den Namen der Schnittstelle ein, die Sie überprüfen möchten. Wenn Sie eine einzige Schnittstelle verwenden (der Standard), lautet der Name `eth0`. Wenn das Betriebssystem vorhersagbare Netzwerknamen unterstützt, könnte der Name `ens5` lauten.

Im folgenden Beispiel wird das `ixgbevf`-Modul nicht geladen, da als Treiber `vif` angezeigt wird.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

In diesem Beispiel wird das Modul `ixgbevf` geladen. In dieser Instance wurde Enhanced Networking richtig konfiguriert.

```
[ec2-user ~]$ ethtool -i eth0
driver: ixgbevf
version: 4.0.3
firmware-version: N/A
bus-info: 0000:00:03.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: no
supports-register-dump: yes
supports-priv-flags: no
```

Windows

Windows-Netzwerkadapter

Sie überprüfen, ob der Treiber installiert wurde, indem Sie sich bei der Instance anmelden und den Geräte-Manager öffnen. Sie sollten `Intel(R) 82599 Virtual Function` unter Netzwerkadapter gelistet sehen.

Inhalt

- Ihre Instance für Erweitertes Netzwerk vorbereiten
- Testen, ob Enhanced Networking aktiviert ist
- Aktivieren von Enhanced Networking auf Ihrer Instance
- Fehlerbehebung bei Verbindungsproblemen

Ihre Instance für Erweitertes Netzwerk vorbereiten

Zur Vorbereitung für Enhanced Networking mit der Intel 82599 VF-Schnittstelle sollten Sie Ihre Instance wie folgt einrichten:

- Stellen Sie sicher, dass es sich um einen der folgenden Instance-Typen handelt: C3, C4, D2, I2, M4 (außer`m4.16xlarge`) und R3.
- Überprüfen Sie, ob der Instance eine Verbindung zum Internet fehlt.
- Wenn Sie wichtige Daten auf der Instance gespeichert haben, die Sie erhalten möchten, sollten Sie diese Daten jetzt sichern, indem Sie ein AMI von Ihrer Instance erstellen. Die Aktualisierung von Kernels und Kernel-Modulen sowie die Aktivierung des Attributs `sriovNetSupport` kann dazu führen, dass Instances inkompatibel oder Betriebssysteme unerreichbar werden. Wenn Sie über ein aktuelles Backup verfügen, gehen die Daten nicht verloren, falls das geschieht.
- Linux-Instances – Starten Sie die Instance aus einem HVM-AMI mit der Linux-Kernel-Version 2.6.32 oder höher. In den aktuellen Amazon Linux HVM-AMIs sind die für Enhanced Networking erforderlichen Module bereits installiert und die entsprechenden Attribute gesetzt. D. h., wenn Sie eine Amazon-EBS-gestützte Instance mit Enhanced-Networking-Unterstützung mithilfe eines aktuellen Amazon Linux HVM-AMI starten, ist Enhanced Networking für Ihre Instance bereits aktiviert.

> **Warning**
>
> Enhanced Networking wird ausschließlich für HVM-Instances unterstützt. Die Aktivierung von Enhanced Networking in einer PV-Instance kann dazu führen, dass diese nicht mehr erreichbar ist. Das Setzen dieses Attributs, ohne dass das richtige Modul bzw. die richtige

Modulversion vorhanden ist, kann ebenso dazu führen, dass die Instance nicht mehr erreichbar ist.

- Windows-Instances – Starten Sie die Instance über ein 64-Bit-HVM-AMI. Sie können Erweitertes Netzwerk in Windows Server 2008 nicht aktivieren. Enhanced Networking ist in AMIs für Windows Server 2012 R2 sowie Windows Server 2016 und höher bereits aktiviert. Windows Server 2012 R2 enthält den Intel-Treiber 1.0.15.3; wir empfehlen, ein Upgrade dieses Treibers auf die aktuelle Version mithilfe des Dienstprogramms Pnputil.exe durchzuführen.
- Verwenden Sie AWS CloudShell aus der AWS-Managementkonsole, oder installieren und konfigurieren Sie die AWS CLI oder die AWS Tools for Windows PowerShell auf einem beliebigen Computer, am besten aber auf Ihrem lokalen Desktop oder Laptop. Weitere Informationen finden Sie unter Zugriff auf Amazon EC2 oder im AWS CloudShell-Benutzerhandbuch. Enhanced Networking kann nicht über die Amazon EC2-Konsole verwaltet werden.

Testen, ob Enhanced Networking aktiviert ist

Stellen Sie sicher, dass das Attribut `sriovNetSupport` für die Instance oder das Image festgelegt ist.

AWS CLI

So überprüfen Sie das Instance-Attribut (sriovNetSupport)

Verwenden Sie den folgenden describe-instance-attribute-Befehl. Wenn das Attribut gesetzt ist, ist der Wert `simple`.

```
aws ec2 describe-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --attribute sriovNetSupport
```

So überprüfen Sie das Image-Attribut (sriovNetSupport)

Verwenden Sie den folgenden describe-images-Befehl. Wenn das Attribut gesetzt ist, ist der Wert `simple`.

```
aws ec2 describe-images \
    --image-id ami-0abcdef1234567890 \
    --query "Images[].SriovNetSupport"
```

PowerShell

So überprüfen Sie das Instance-Attribut (sriovNetSupport)

Verwenden Sie das cmdlet Get-EC2InstanceAttribute. Wenn das Attribut gesetzt ist, ist der Wert `simple`.

```
Get-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -Attribute sriovNetSupport
```

So überprüfen Sie das Image-Attribut (sriovNetSupport)

Verwenden Sie den folgenden describe-images-Befehl. Wenn das Attribut gesetzt ist, ist der Wert `simple`.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).SriovNetSupport
```

Aktivieren von Enhanced Networking auf Ihrer Instance

Welches Verfahren Sie verwenden, hängt vom Betriebssystem der Instance ab.

> **Warning**
>
> Es ist nicht möglich, das Enhanced Networking-Attribut zu deaktivieren, wenn Sie es einmal aktiviert haben.

Amazon Linux

In den aktuellen Amazon Linux HVM-AMIs ist das für Enhanced Networking erforderliche `ixgbevf`-Modul bereits installiert und das `sriovNetSupport`-Attribute gesetzt. Wenn Sie also einen Instance-Typ mit einem aktuellen Amazon Linux-HVM-AMI starten, ist die optimierte Netzwerkfunktionalität bereits für die Instance aktiviert. Weitere Informationen finden Sie unter Testen, ob Enhanced Networking aktiviert ist.

Wenn Sie Ihre Instance aus einem älteren Amazon Linux AMI gestartet haben und Enhanced Networking noch nicht aktiviert wurde, gehen Sie wie folgt vor, um die optimierte Netzwerkleistung zu aktivieren.

Aktivieren von Enhanced Networking

1. Verbinden Sie sich mit der Instance.
2. Führen Sie den folgenden Befehl in der Instance aus, um die Instance mit dem aktuellen Kernel und den aktuellen Kernel-Modulen einschließlich zu aktualisiere `ixgbevf`:

   ```
   [ec2-user ~]$ sudo yum update
   ```

3. Starten Sie die Instance von Ihrem lokalen Computer aus neu, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: reboot-instances (AWS CLI) oder Restart-EC2Instance (AWS Tools for Windows PowerShell).
4. Stellen Sie erneut eine Verbindung mit der Instance her und prüfen Sie, ob das `ixgbevf`-Modul installiert wurde und in der empfohlenen Mindestversion vorliegt, indem Sie den Befehl modinfo ixgbevf aus dem Abschnitt Testen, ob Enhanced Networking aktiviert ist verwenden.
5. [EBS-gestützte Instance] Halten Sie die Instance von Ihrem lokalen Computer aus an, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: stop-instances (AWS CLI) oder Stop-EC2Instance (AWS Tools for Windows PowerShell).

   [In einem Instance-Speicher gesicherte Instance] Sie können die Instance nicht anhalten, um das Attribut zu ändern. Springen Sie stattdessen dann zum nächsten Schritt weiter.
6. Aktivieren Sie auf Ihrem lokalen Computer das Enhanced Networking-Attribut mit einem der folgenden Befehle:

   AWS CLI

   Verwenden Sie den modify-instance-attribute-Befehl wie folgt:

   ```
   aws ec2 modify-instance-attribute \
       --instance-id i-1234567890abcdef0 \
       --sriov-net-support simple
   ```

   PowerShell

   Verwenden Sie das cmdlet Edit-EC2InstanceAttribute wie folgt.

   ```
   Edit-EC2InstanceAttribute `
       -InstanceId i-1234567890abcdef0 `
       -SriovNetSupport "simple"
   ```

7. (Optional) Erstellen Sie ein AMI von der Instance, wie unter beschrieb Ein Amazon-EBS-gestütztes AMI erstellen. Das AMI erbt das Enhanced Networking-Attribut von der Instance. D. h. Sie können mit diesem AMI eine andere Instance starten, in der Enhanced Networking standardmäßig aktiviert ist.
8. Starten Sie die Instance von Ihrem lokalen Computer aus, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: start-instances (AWS CLI) oder Start-EC2Instance (AWS Tools for Windows PowerShell).
9. Stellen Sie eine Verbindung mit der Instance her und prüfen Sie, ob das `ixgbevf`-Modul installiert und in der Netzwerkschnittstelle geladen wurde, indem Sie den Befehl ethtool -i eth***n*** aus dem Abschnitt Testen, ob Enhanced Networking aktiviert ist verwenden.

So aktivieren Sie Enhanced Networking (Instance Store-Backed Instances)

Führen Sie die Schritte aus dem vorherigen Verfahren durch bis zu dem Schritt, in dem die Instance angehalten wird. Erstellen Sie ein neues AMI, wie in Ein Amazon-S3-gestütztes AMI erstellen beschreiben, um sicherzustellen, dass Sie das Enhanced Networking-Attribut aktivieren, wenn Sie das AMI registrieren.

AWS CLI

Verwenden Sie den register-image-Befehl wie folgt:

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Verwenden Sie Register-EC2Image wie folgt.

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Ubuntu

Bevor Sie anfangen, überprüfen Sie, ob das Enhanced Networking bereits auf Ihrer Instance aktiviert ist.

Die Quick Start Ubuntu HVM AMIs enthalten die erforderlichen Treiber für Enhanced Networking. Bei einer Version von `ixgbevf` vor 2.16.4 können Sie das Kernel-Paket `linux-aws` installieren, um die neuesten Enhanced Networking-Treiber zu erhalten.

In der folgenden Anleitung sind die allgemeinen Schritte für die Kompilierung des `ixgbevf`-Moduls auf einer Ubuntu-Instance.

`linux-aws`-Kernel-Paket installieren

1. Verbinden Sie sich mit der Instance.
2. Aktualisieren Sie den Cache der Paketverwaltung und die einzelnen Pakete.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

> **Important**
>
> Wenn Sie während des Aktualisierungsvorgangs aufgefordert werden, `grub` zu installieren, verwenden Sie `/dev/xvda` für die Installation von `grub` und wählen Sie anschließend aus, dass die aktuelle Version von `/boot/grub/menu.lst` beibehalten werden soll.

Andere Linux-Distributionen

Bevor Sie anfangen, überprüfen Sie, ob das Enhanced Networking bereits auf Ihrer Instance aktiviert ist. Die neuesten Quick Start HVM AMIs enthalten die erforderlichen Treiber für Enhanced Networking, Sie müssen deshalb keine weiteren Schritte ausführen.

In der folgenden Anleitung werden die Schritte beschrieben, die Sie für die Aktivierung von Enhanced Networking für die Intel 82599 VF-Schnittstelle unter einer anderen Linux-Distributionen als Amazon Linux oder Ubuntu ausführen müssen. Weitere Informationen z. B. hinsichtlich der genauen Syntax für Befehle, der Speicherorte von Dateien oder der Unterstützung von einzelnen Paketen bzw. Tools finden Sie in der Dokumentation zu der jeweiligen Linux-Distribution.

Aktivieren von Enhanced Networking in Linux

1. Verbinden Sie sich mit der Instance.
2. Laden Sie die Quelldatei für das `ixgbevf`-Modul in Ihrer Instance herunter. Sie finden diese auf der Sourceforge-Website unter https://sourceforge.net/projects/e1000/files/ixgbevf%20stable/.

   Mit früheren Versionen von `ixgbevf` als 2.16.4 – einschließlich Version 2.14.2 – werden die Builds unter manchen Linux-Distributionen nicht richtig erstellt, einschließlich bestimmter Versionen von Ubuntu.

3. Kompilieren und installieren Sie das `ixgbevf`-Module in Ihrer Instance.

   > **Warning**
   >
   > Wenn Sie das `ixgbevf`-Modul für den aktuellen Kernel kompilieren und anschließend ein Upgrade des Kernels durchführen, ohne einen neuen Build des Treibers für den neuen Kernel zu erstellen, wechselt das System beim nächsten Neustart möglicherweise zum ursprünglichen `ixgbevf`-Modul der Verteilung zurück. Dies kann den Zugriff auf das System verhindern, wenn die verteilungsspezifische Version mit Enhanced Networking nicht kompatibel ist.

4. Führen Sie den Befehl sudo depmod aus, um die Abhängigkeiten für das Modul zu aktualisieren.
5. Aktualisieren Sie `initramfs` in Ihrer Instance, um sicherzustellen, dass das neue Modul während des Bootvorgangs geladen wird.
6. Ermitteln Sie, ob Ihr System standardmäßig transparente Netzwerkschnittstellennamen verwendet. Systeme, die systemd- oder udev-Versionen ab 197 verwenden, können Ethernet-Geräte umbenennen, d. h. die einzige Netzwerkschnittstelle in einem solchen System wird nicht zwingend als `eth0` bezeichnet. Dieses Verhalten kann Probleme bei der Verbindung mit Ihrer Instance verursachen. Weitere Informationen und andere Konfigurationsoptionen finden Sie unter Predictable Network Interface Names auf der freedesktop.org-Website.

   a. Sie können die systemd- und udev-Versionen auf RPM-basierten Systemen mit den folgenden Befehl überprüfen:

      ```
      [ec2-user ~]$ rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
          systemd-208-11.el7_0.2.x86_64
      ```

      In dem Red Hat Enterprise Linux 7-Beispiel oben lautet die systemd-Version 208, d. h. transparente Netzwerkschnittstellennamen müssen deaktiviert werden.

   b. Sie können transparente Netzwerkschnittstellennamen deaktivieren, indem Sie in der Zeile `net.ifnames=0` in der Datei `GRUB_CMDLINE_LINUX` die Option `/etc/default/grub` hinzufügen.

      ```
      [ec2-user ~]$ sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /
      etc/default/grub
      ```

   c. Erstellen Sie die neue Grub-Konfigurationsdatei.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [EBS-gestützte Instance] Halten Sie die Instance von Ihrem lokalen Computer aus an, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: stop-instances (AWS CLI) oder Stop-EC2Instance (AWS Tools for Windows PowerShell).

   [In einem Instance-Speicher gesicherte Instance] Sie können die Instance nicht anhalten, um das Attribut zu ändern. Springen Sie stattdessen dann zum nächsten Schritt weiter.

8. Aktivieren Sie auf Ihrem lokalen Computer das Enhanced Networking-Attribut mit einem der folgenden Befehle:

   AWS CLI

   Verwenden Sie den modify-instance-attribute-Befehl wie folgt:

   ```
   aws ec2 modify-instance-attribute \
       --instance-id i-1234567890abcdef0 -\
       -sriov-net-support simple
   ```

   PowerShell

   Verwenden Sie das cmdlet Edit-EC2InstanceAttribute wie folgt.

   ```
   Edit-EC2InstanceAttribute `
       -InstanceId i-1234567890abcdef0 `
       -SriovNetSupport "simple"
   ```

9. (Optional) Erstellen Sie ein AMI von der Instance, wie unter beschrieb Ein Amazon-EBS-gestütztes AMI erstellen. Das AMI erbt das Enhanced Networking-Attribut von der Instance. D. h. Sie können mit diesem AMI eine andere Instance starten, in der Enhanced Networking standardmäßig aktiviert ist.

   Wenn Ihr Instance-Betriebssystem eine `/etc/udev/rules.d/70-persistent-net.rules`-Datei enthält, müssen Sie diese vor der Erstellung des AMI löschen. Diese Datei enthält die MAC-Adresse des Ethernet-Adapters in der ursprünglichen Instance. Wenn eine andere Instance mit dieser Datei gestartet wird, kann das Betriebssystem das Gerät nicht finden und von `eth0` schlägt möglicherweise fehl, was zu Problemen beim Start führt. Diese Datei wird während des nächsten Bootvorgangs neu generiert, und jede aus dem AMI gestartete Instance erstellt eine eigene Version der Datei.

10. Starten Sie die Instance von Ihrem lokalen Computer aus, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: start-instances (AWS CLI) oder Start-EC2Instance (AWS Tools for Windows PowerShell).
11. (Optional) Stellen Sie eine Verbindung mit Ihrer Instance her und überprüfen Sie, ob das Modul installiert wurde.

So aktivieren Sie Enhanced Networking (Instance-Speicher-gestützte Instances):

Führen Sie die Schritte aus dem vorherigen Verfahren durch bis zu dem Schritt, in dem die Instance angehalten wird. Erstellen Sie ein neues AMI, wie in Ein Amazon-S3-gestütztes AMI erstellen beschreiben, um sicherzustellen, dass Sie das Enhanced Networking-Attribut aktivieren, wenn Sie das AMI registrieren.

AWS CLI

Verwenden Sie den register-image-Befehl wie folgt:

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Verwenden Sie Register-EC2Image wie folgt.

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Windows

Wenn Sie Ihre Instance gestartet haben und Enhanced Networking noch nicht aktiviert wurde, müssen Sie den erforderlichen Netzwerkadaptertreiber herunterladen und in der Instance installieren sowie anschließend das `sriovNetSupport`-Instance-Attribut setzen, um die optimierte Netzwerkleistung zu erzielen. Sie können dieses Attribut nur in unterstützten Instance-Typen aktivieren. Weitere Informationen finden Sie unter Erweitertes Netzwerk in Amazon-EC2-Instances.

> **Important**
>
> Die neuesten Treiberupdates in den Windows-AMIs finden Sie im Windows AMI-Versionsverlauf in der AWS-Windows AMI-Referenz.

Aktivieren von Enhanced Networking

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
2. [Windows Server 2016 und höher] Führen Sie das folgende EC2-Launch-PowerShell-Skript aus, um die Instance nach der Installation des Treibers zu konfigurieren.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

> **Important**
>
> Das Administratorpasswort wird zurückgesetzt, wenn Sie das EC2-Launch-Skript zum Initialisieren der Instance aktivieren. Sie können die Konfigurationsdatei bearbeiten, um das Zurücksetzen des Administratorpassworts zu deaktivieren, indem Sie es in den Einstellungen für die Initialisierungsaufgaben festlegen.

3. Laden Sie von der Instance den Intel-Netzwerkadaptertreiber für Ihr Betriebssystem herunter:

   - Windows Server 2022

     Besuchen Sie die Download-Seite und laden Sie `Wired_driver_`*`version`*`_x64.zip` herunter.
   - Windows Server 2019, einschließlich Server-Version 1809 und neuer*

     Besuchen Sie die Download-Seite und laden Sie `Wired_driver_`*`version`*`_x64.zip` herunter.
   - Windows Server 2016, einschließlich Server-Version 1803 und früher*

     Besuchen Sie die Download-Seite und laden Sie `Wired_driver_`*`version`*`_x64.zip` herunter.
   - Windows Server 2012 R2

     Besuchen Sie die Download-Seite und laden Sie `Wired_driver_`*`version`*`_x64.zip` herunter.
   - Windows Server 2012

Besuchen Sie die Download-Seite und laden Sie `Wired_driver_version_x64.zip` herunter.

- Windows Server 2008 R2

  Besuchen Sie die Download-Seite und laden Sie `PROWinx64Legacy.exe` herunter.

*Die Serverversionen 1803 und früher sowie 1809 und später werden auf den Intel-Seiten für Treiber und Software nicht ausdrücklich genannt.

4. Installieren Sie den Intel-Netzwerkadaptertreiber für Ihr Betriebssystem.

   - Windows Server 2008 R2

     1. Suchen Sie im Downloads-Ordner die Datei `PROWinx64Legacy.exe` und benennen Sie sie in `PROWinx64Legacy.zip` um.
     2. Extrahieren Sie den Inhalt der Datei `PROWinx64Legacy.zip`.
     3. Öffnen Sie die Befehlszeile, navigieren Sie zum extrahierten Ordner und führen Sie den folgenden Befehl aus, um das Dienstprogramm `pnputil` zum Hinzufügen und Installieren der INF-Datei im Treiberspeicher zu verwenden.

        ```
        C:\> pnputil -a PROXGB\Winx64\NDIS62\vxn62x64.inf
        ```

   - Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012

     1. Extrahieren Sie im Downloads-Ordner den Inhalt der Datei `Wired_driver_version_x64.zip`.
     2. Öffnen Sie die Befehlszeile, navigieren Sie zum extrahierten Ordner und führen Sie einen der folgenden Befehle aus, um das Dienstprogramm `pnputil` zum Hinzufügen und Installieren der INF-Datei im Treiberspeicher zu verwenden.

        - Windows Server 2022

          ```
          pnputil -i -a PROXGB\Winx64\NDIS68\vxn68x64.inf
          ```

        - Windows Server 2019

          ```
          pnputil -i -a PROXGB\Winx64\NDIS68\vxn68x64.inf
          ```

        - Windows Server 2016

```
pnputil -i -a PROXGB\Winx64\NDIS65\vxn65x64.inf
```

- Windows Server 2012 R2

```
pnputil -i -a PROXGB\Winx64\NDIS64\vxn64x64.inf
```

- Windows Server 2012

```
pnputil -i -a PROXGB\Winx64\NDIS63\vxn63x64.inf
```

5. Aktivieren Sie auf Ihrem lokalen Computer das Enhanced Networking-Attribut mit einem der folgenden Befehle:

   AWS CLI

   Verwenden Sie den modify-instance-attribute-Befehl wie folgt:

   ```
   aws ec2 modify-instance-attribute \
       --instance-id i-1234567890abcdef0 \
       --sriov-net-support simple
   ```

   PowerShell

   Verwenden Sie das cmdlet Edit-EC2InstanceAttribute wie folgt.

   ```
   Edit-EC2InstanceAttribute `
       -InstanceId i-1234567890abcdef0 `
       -SriovNetSupport "simple"
   ```

6. (Optional) Erstellen Sie ein AMI von der Instance, wie unter beschrieb Ein Amazon-EBS-gestütztes AMI erstellen. Das AMI erbt das Enhanced Networking-Attribut von der Instance. D. h. Sie können mit diesem AMI eine andere Instance starten, in der Enhanced Networking standardmäßig aktiviert ist.
7. Starten Sie die Instance von Ihrem lokalen Computer aus, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: start-instances (AWS CLI) oder Start-EC2Instance (AWS Tools for Windows PowerShell).

Fehlerbehebung bei Verbindungsproblemen

Wenn die Verbindung bei der Aktivierung von Enhanced Networkings verloren geht, ist das `ixgbevf`-Modul u. U. nicht mit dem Kernel kompatibel. Versuchen Sie, die Version des `ixgbevf`-Moduls zu installieren, die in der Linux-Distribution Ihrer Instance enthalten war.

Wenn Sie Enhanced Networking für eine PV-Instance oder -AMI aktivieren, ist Ihre Instance möglicherweise nicht mehr erreichbar.

Weitere Informationen finden Sie unter Wie kann ich Erweitertes Netzwerk auf meinen EC2-Instances aktivieren und konfigurieren?

Netzwerkleistung für ENA-Einstellungen auf Ihrer EC2-Instance überwachen

Der Elastic Network Adapter (ENA)-Treiber veröffentlicht Netzwerkleistungsmetriken aus den Instances, in denen sie aktiviert sind. Sie können diese Metriken verwenden, um Probleme mit der Instance-Performance zu beheben, die richtige Instance-Größe für eine Workload auszuwählen, Skalierungsaktivitäten proaktiv zu planen und Anwendungen zu vergleichen, um zu bestimmen, ob sie die auf einer Instance verfügbare Leistung maximieren.

Amazon EC2 definiert Netzwerkmaxima auf Instance-Ebene, um eine gute Netzwerkerfahrung sicherzustellen, einschließlich einer konsistenten Netzwerkleistung für alle Instance-Größen. AWS stellt für jede Instance Maxima für Folgendes bereit:

- Bandwidth capability (Bandbreitenfähigkeit) – Jede EC2-Instance verfügt über eine maximale Bandbreite für aggregierten ein- und ausgehenden Datenverkehr, basierend auf Instance-Typ und -Größe. Manche Instances nutzen einen Netzwerk-I/O-Guthabenmechanismus, bei dem die Netzwerkbandbreite anhand der durchschnittlichen Bandbreitenauslastung zugewiesen wird. Amazon EC2 verfügt außerdem über eine maximale Bandbreite für Datenverkehr zu Direct Connect und ins Internet. Weitere Informationen finden Sie unter Netzwerkbandbreite der EC2 Amazon-Instance.
- Packet-per-second (PPS) performance (Pakete-pro-Sekunden-Leistung) – Jede EC2-Instance verfügt über eine maximale PPS-Leistung, basierend auf Instance-Typ und -Größe.
- Connections tracked (Nachverfolgte Verbindungen) – Die Sicherheitsgruppe verfolgt jede aufgebaute Verbindung, um sicherzustellen, dass die Rückpakete wie erwartet übertragen werden. Es gibt eine maximale Anzahl von Verbindungen, die pro Instance verfolgt werden können. Weitere Informationen finden Sie unter . Verbindungsverfolgung EC2 für Amazon-Sicherheitsgruppen

- Verbindungslokaler Servicezugriff – Amazon EC2 bietet eine Schnittstelle für maximale PPS pro Netzwerk für Datenverkehr zu lokalen Proxy-Services wie dem Amazon-DNS-Service, dem Instance Metadata Service und dem Amazon Time Sync Service.

Wenn der Netzwerkverkehr für eine Instance ein Maximum überschreitet, formtAWS den Datenverkehr, der das Maximum übersteigt, indem es Netzwerkpakete in die Warteschlange stellt und dann löscht. Mithilfe der Metriken zur Netzwerkleistung können Sie überwachen, wann der Datenverkehr ein Maximum überschreitet. Diese Metriken informieren Sie in Echtzeit über Auswirkungen auf den Netzwerkverkehr und mögliche Probleme mit der Netzwerkleistung.

Inhalt

- Voraussetzungen
- Metriken für den ENA-Treiber
- Anzeigen der Netzwerkleistungsmetriken für Ihre -Instance
- Metriken für ENA Express
- Metriken zur Netzwerkleistung mit dem DPDK-Treiber für ENA
- Metriken für Instances, die FreeBSD ausführen

Voraussetzungen

Linux-Instances

- Installieren Sie ENA-Treiberversion 2.2.10 oder höher. Verwenden Sie den ethtool-Befehl, um die installierte Version zu überprüfen. Im folgenden Beispiel erfüllt die Version die Mindestanforderung.

```
[ec2-user ~]$ ethtool -i eth0 | grep version
version: 2.2.10
```

  Informationen zum Upgrade Ihres ENA-Treibers finden Sie unter Enhanced networking (Verbessertes Networking).
- Um diese Metriken in Amazon CloudWatch zu importieren, installieren Sie den CloudWatch-Agenten. Weitere Informationen finden Sie unter Collect network performance metrics (Sammeln von Metriken zur Netzwerkleistung) im Amazon CloudWatch-Benutzerhandbuch.
- Installieren Sie zur Unterstützung der `conntrack_allowance_available`-Metrik den ENA-Treiber Version 2.8.1 oder höher.

- Um das PPS-Limit für ausgehende Fragmente von 1 024 zu überschreiben, installieren Sie den ENA-Treiber Version 2.13.3 oder höher.

Windows-Instances

- Installieren Sie ENA-Treiberversion 2.2.2 oder höher. Verwenden Sie den Geräte-Manager, um die installierte Version zu überprüfen.
  1. Öffnen Sie den Geräte-Manager, indem Sie ausführe `devmgmt.msc`.
  2. Erweitern Sie Network Adapters (Netzwerkadapter).
  3. Wählen Sie Amazon Elastic Network Adapter (Amazon-Elastic-Netzwerkadapter), Properties (Eigenschaften).
  4. Suchen Sie auf der Registerkarte Driver (Treiber) nach Driver Version (Treiberversion).

  Informationen zum Upgrade Ihres ENA-Treibers finden Sie unter Enhanced networking (Verbessertes Networking).
- Um diese Metriken in Amazon CloudWatch zu importieren, installieren Sie den CloudWatch-Agenten. Weitere Informationen finden Sie unter Collect advanced network metrics (Sammeln von fortgeschrittenen Netzwerkmetriken) im Amazon CloudWatch-Benutzerhandbuch.

Metriken für den ENA-Treiber

Der ENA-Treiber liefert die folgenden Metriken in Echtzeit an die Instance. Sie liefern die kumulative Anzahl von Paketen, die seit dem letzten Zurücksetzen des Treibers in jeder Netzwerkschnittstelle in die Warteschlange gestellt oder verworfen wurden.

Metrik	Beschreibung	Unterstützt auf
`bw_in_allowance_exceeded`	Die Anzahl der Pakete, die in die Warteschlange gestellt oder verworfen wurden, da die eingehende aggregierte Bandbreite das Maximum für die Instance überschritten hat.	Allen Instance-Typen
`bw_out_allowance_exceeded`	Die Anzahl der Pakete, die in die Warteschlange gestellt	Allen Instance-Typen

Metrik	Beschreibung	Unterstützt auf
	oder verworfen wurden, weil die ausgehende aggregierte Bandbreite das Maximum für die Instance überschritten hat.	
`conntrack_allowance_exceeded`	Die Anzahl der verworfenen Pakete, weil die Verbindungsverfolgung das Maximum für die Instance überschritten hat und keine neuen Verbindungen hergestellt werden konnten. Dies kann zu einem Paketverlust für den Datenverkehr zur oder von der Instance führen.	Allen Instance-Typen
`conntrack_allowance_available`	Die Anzahl der nachverfolgten Verbindungen, die von der Instance hergestellt werden können, bevor die zulässige Anzahl nachverfolgter Verbindungen dieses Instance-Typs erreicht wird.	Nur Nitro-basierte Instances

Metrik	Beschreibung	Unterstützt auf
`linklocal_allowance_exceeded`	Die Anzahl der verworfenen Pakete, weil das PPS des Datenverkehrs zu lokalen Proxy-Diensten das Maximum für die Netzwerkschnittstelle überschritten hat. Dies wirkt sich auf den Datenverkehr zum Amazon-DNS-Service, zum Instance Metadata Service und zum Amazon Time Sync Service aus, hat jedoch keine Auswirkung auf den Datenverkehr an benutzerdefinierte DNS-Resolver.	Allen Instance-Typen
`pps_allowance_exceeded`	Die Anzahl der Pakete, die in die Warteschlange gestellt oder verworfen wurden, weil die bidirektionale PPS das Maximum für die Instance überschritten hat. *	Allen Instance-Typen

* Abhängig von der Einstellung für den Fragment-Proxymodus für den ENA-Linux-Treiber v2.13.3 oder höher kann dieses Limit auch ausgehende Fragmentverluste umfassen, die 1 024 PPS für die Netzwerkschnittstelle überschreiten. Wenn der Fragment-Proxymodus für den Linux-Treiber aktiviert ist, umgehen ausgehende Fragment-Drops das normalerweise geltende Limit von 1 024 PPS und werden innerhalb der Standard-PPS-Zulagen gezählt. Der Fragment-Proxymodus ist standardmäßig deaktiviert.

Anzeigen der Netzwerkleistungsmetriken für Ihre -Instance

Welches Verfahren Sie verwenden, hängt vom Betriebssystem der Instance ab.

Linux-Instances

Sie können Metriken in Ihren bevorzugten Tools veröffentlichen, um die Metrikdaten zu visualisieren. Sie können die Metriken beispielsweise mit dem CloudWatch-Agent in Amazon CloudWatch

veröffentlichen. Der Agent ermöglicht es Ihnen, einzelne Metriken auszuwählen und die Veröffentlichung zu steuern.

Sie können auch den ethtool verwenden, um die Metriken für jede Netzwerkschnittstelle wie eth0 wie folgt abzurufen.

```
[ec2-user ~]$ ethtool -S eth0
     bw_in_allowance_exceeded: 0
     bw_out_allowance_exceeded: 0
     pps_allowance_exceeded: 0
     conntrack_allowance_exceeded: 0
     linklocal_allowance_exceeded: 0
     conntrack_allowance_available: 136812
```

Windows-Instances

Sie können die Metriken mit jedem Verbraucher von Windows-Leistungsindikatoren anzeigen. Die Daten können gemäß dem EnaPerfCounter-Manifest analysiert werden. Dies ist eine XML-Datei, die den Leistungsindikatoranbieter und seine Leistungsindikatoren definiert.

So installieren Sie das Manifest

Wenn Sie die Instance mit einem AMI gestartet haben, das ENA-Treiber 2.2.2 oder höher enthält oder das Installationsskript im Treiberpaket für ENA-Treiber 2.2.2 verwendet hat, ist das Manifest bereits installiert. Gehen Sie folgendermaßen vor, um das Manifest manuell zu installieren:

1. Entfernen Sie das vorhandene Manifest mit dem folgenden Befehl:

   ```
   unlodctr /m:EnaPerfCounters.man
   ```

2. Kopieren Sie die Manifestdatei `EnaPerfCounters.man` aus dem Treiberinstallationspaket nach `%SystemRoot%\System32\drivers`.
3. Installieren Sie das neue Manifest mit dem folgenden Befehl:

   ```
   lodctr /m:EnaPerfCounters.man
   ```

So zeigen Sie Metriken mit dem Leistungsmonitor an

1. Öffnen Sie Performance Monitor.
2. Drücken Sie Strg+N, um neue Leistungsindikatoren hinzuzufügen.

3. Wählen Sie ENA Packets Shaping (ENA-Paketformung) aus der Liste aus.
4. Wählen Sie die zu überwachenden Instances aus und wählen Sie Add (Hinzufügen).
5. Klicken Sie auf OK.

Metriken für ENA Express

ENA Express wird von der AWS Scalable Reliable Datagram (SRD)-Technologie unterstützt. SRD ist ein leistungsstarkes Netzwerktransportprotokoll, das dynamisches Routing verwendet, um den Durchsatz zu erhöhen und die Tail-Latenz zu minimieren. Nachdem Sie ENA Express für die Netzwerkschnittstellen-Anhänge sowohl auf der sendenden als auch auf der empfangenden Instance aktiviert haben, können Sie ENA-Express-Metriken verwenden, um zu helfen sicherzustellen, dass Ihre Instances die Leistungsverbesserungen der SRD-Technologie voll ausschöpfen. Zum Beispiel:

- Bewerten Sie Ihre Ressourcen, um sicherzustellen, dass sie über ausreichende Kapazitäten verfügen, um mehr SRD-Verbindungen herzustellen.
- Identifizieren Sie, wo potenzielle Probleme bestehen, die verhindern, dass berechtigte ausgehende Pakete SRD verwenden.
- Berechnen Sie den Prozentsatz des ausgehenden Datenverkehrs, welcher SRD für die Instance verwendet.
- Berechnen Sie den Prozentsatz des eingehenden Datenverkehrs, welcher SRD für die Instance verwendet.

> **Note**
>
> Verwenden Sie zum Erstellen von Metriken die Treiberversion 2.8 oder höher.

Um eine Liste der Metriken für Ihre Linux Instance anzuzeigen, die für ENA Express gefiltert wurde, führen Sie den folgenden ethtool-Befehl für Ihre Netzwerkschnittstelle aus (hier als `eth0` gezeigt). Notieren Sie sich den Wert der `ena_srd_mode`-Metrik.

```
[ec2-user ~]$ ethtool -S eth0 | grep ena_srd
NIC statistics:
 ena_srd_mode: 1
 ena_srd_tx_pkts: 0
 ena_srd_eligible_tx_pkts: 0
 ena_srd_rx_pkts: 0
```

```
ena_srd_resource_utilization: 0
```

Die folgenden Metriken sind für alle Instances verfügbar, für die ENA Express aktiviert ist.

ena_srd_mode

Beschreibt, welche ENA-Express-Features aktiviert sind. Werte sind wie folgt:

- `0` = ENA Express aus, UDP aus
- `1` = ENA Express ein, UDP aus
- `2` = ENA Express aus, UDP ein

> **Note**
>
> Dies passiert nur, wenn ENA Express ursprünglich aktiviert war und UDP für dessen Verwendung konfiguriert wurde. Der vorherige Wert wird für UDP-Verkehr beibehalten.

- `3` = ENA Express ein, UDP ein

ena_srd_eligible_tx_pkts

Die Anzahl der Netzwerke wie folgt:

- Sowohl sendende als auch empfangende Instance-Typen werden unterstützt. Weitere Informationen finden Sie in der Unterstützte Instance-Typen für ENA Express-Tabelle.
- Sowohl die sendenden als auch die empfangenden Instances müssen ENA Express konfiguriert haben.
- Die sendenden und empfangenden Instances müssen in derselben Availability Zone laufen.
- Der Netzwerkpfad zwischen den Instances darf keine Middleware-Boxen enthalten. ENA Express unterstützt derzeit keine Middleware-Boxen.

> **Note**
>
> Die ENA-Express-Zulassungsmetrik deckt die Quell- und Zielanforderungen sowie das Netzwerk zwischen den beiden Endpunkten ab. Zugelassene Pakete können immer noch disqualifiziert werden, nachdem sie bereits gezählt wurden. Wenn beispielsweise ein berechtigtes Paket das Maximum Transmission Unit (MTU)-Limit überschreitet, wird auf die standardmäßige ENA-Übertragung zurückgegriffen, obwohl das Paket im Zähler immer noch als geeignet angezeigt wird.

ena_srd_tx_pkts

Die Anzahl der SRD-Pakete, die innerhalb eines bestimmten Zeitraums übertragen wurden.

ena_srd_rx_pkts

Die Anzahl der SRD-Pakete, die innerhalb eines bestimmten Zeitraums empfangen wurden.

ena_srd_resource_utilization

Der Prozentsatz der maximal zulässigen Arbeitsspeichernutzung für gleichzeitige SRD-Verbindungen, den die Instance verbraucht hat.

Um zu überprüfen, ob die Paketübertragung SRD verwendet, können Sie die Anzahl der zulässigen Pakete (`ena_srd_eligible_tx_pkts`-Metrik) mit der Anzahl der übertragenen SRD-Pakete (`ena_srd_tx_pkts`-Metrik) während eines bestimmten Zeitraums vergleichen.

Ausgehender Verkehr (ausgehende Pakete)

Um sicherzustellen, dass Ihr ausgehender Verkehr SRD wie erwartet verwendet, vergleichen Sie die Anzahl der SRD-fähigen Pakete (`ena_srd_eligible_tx_pkts`) mit der Anzahl der gesendeten SRD-Pakete (`ena_srd_tx_pkts`) über einen bestimmten Zeitraum.

Signifikante Unterschiede zwischen der Anzahl der berechtigten Pakete und der Anzahl der gesendeten SRD-Pakete werden häufig durch Probleme mit der Ressourcenauslastung verursacht. Wenn die an die Instance angeschlossene Netzwerkkarte ihre maximalen Ressourcen aufgebraucht hat oder wenn die Pakete das MTU-Limit überschreiten, können berechtigte Pakete nicht über SRD übertragen werden und müssen auf die standardmäßige ENA-Übertragung zurückgreifen. Pakete können auch während Live-Migrationen oder Aktualisierungen des Live-Servers in diese Lücke fallen. Eine zusätzliche Fehlerbehebung ist erforderlich, um die Grundursache zu ermitteln.

> **Note**
>
> Sie können gelegentliche geringfügige Unterschiede zwischen der Anzahl der berechtigten Pakete und der Anzahl der SRD-Pakete ignorieren. Dies kann beispielsweise passieren, wenn Ihre Instance eine Verbindung zu einer anderen Instance für SRD-Traffic herstellt.

Um herauszufinden, welcher Prozentsatz Ihres gesamten ausgehenden Datenverkehrs in einem bestimmten Zeitraum SRD verwendet, vergleichen Sie die Anzahl der gesendeten SRD-Pakete

(`ena_srd_tx_pkts`) mit der Gesamtzahl der Pakete, die während dieser Zeit für die Instance (`NetworkPacketOut`) gesendet wurden.

Eingehender Verkehr (eingehende Pakete)

Um herauszufinden, welcher Prozentsatz Ihres gesamten eingehenden Datenverkehrs in einem bestimmten Zeitraum SRD verwendet, vergleichen Sie die Anzahl der empfangenen SRD-Pakete (`ena_srd_rx_pkts`) mit der Gesamtzahl der Pakete, die während dieser Zeit von der Instance (`NetworkPacketIn`) erhalten wurden.

Ressourcenauslastung

Die Ressourcenauslastung basiert auf der Anzahl der gleichzeitigen SRD-Verbindungen, die eine einzelne Instance zu einem bestimmten Zeitpunkt unterhalten kann. Die Metrik zur Ressourcenauslastung (`ena_srd_resource_utilization`) verfolgt Ihre aktuelle Auslastung für die Instance. Wenn sich die Auslastung 100 % nähert, können Sie Leistungsproblemen erwarten. ENA Express greift von der SRD auf die standardmäßige ENA-Übertragung zurück und die Wahrscheinlichkeit, dass Pakete verworfen werden, steigt. Eine hohe Ressourcenauslastung ist ein Zeichen dafür, dass es an der Zeit ist, die Instance aufzuskalieren, um die Netzwerkleistung zu verbessern.

> **Note**
>
> Wenn der Netzwerkverkehr für eine Instance ein Maximum überschreitet, formtAWS den Datenverkehr, der das Maximum übersteigt, indem es Netzwerkpakete in die Warteschlange stellt und dann löscht.

Persistenz

Ausgangs- und Eingangsmetriken fallen an, solange ENA Express für die Instance aktiviert ist. Metriken fallen nicht mehr an, wenn ENA Express deaktiviert ist, aber sie bleiben bestehen, solange die Instance noch läuft. Die Metriken werden zurückgesetzt, wenn die Instance neu gestartet oder beendet wird oder wenn die Netzwerkschnittstelle von der Instance getrennt ist.

Metriken zur Netzwerkleistung mit dem DPDK-Treiber für ENA

Die ENA-Treiberversion 2.2.0 und höher unterstützt die Berichterstellung von Netzwerkmetriken. DPDK 20.11 enthält den ENA-Treiber 2.2.0 und ist die erste DPDK-Version, die dieses Feature unterstützt.

Der DPDK-Treiber v25.03 oder höher unterstützt den Fragment-Proxymodus. Wenn der Fragment-Proxymodus für den DPDK-Treiber aktiviert ist, umgehen ausgehende Fragment-Drops das normalerweise geltende Limit von 1 024 PPS und werden innerhalb der Standard-PPS-Zulagen gezählt. Der Fragment-Proxymodus ist standardmäßig deaktiviert.

Sie können eine Beispielanwendung verwenden, um DPDK-Statistiken anzuzeigen. Um eine interaktive Version der Beispielanwendung zu starten, führen Sie den folgenden Befehl aus.

```
./app/dpdk-testpmd -- -i
```

In dieser interaktiven Sitzung können Sie einen Befehl eingeben, um erweiterte Statistiken für einen Port abzurufen. Der folgende Beispielbefehl ruft die Statistiken für Port 0 ab.

```
show port xstats 0
```

Das Folgende ist ein Beispiel für eine interaktive Sitzung mit der DPDK-Beispielanwendung.

```
[root@ip-192.0.2.0 build]# ./app/dpdk-testpmd -- -i
        EAL: Detected 4 lcore(s)
        EAL: Detected 1 NUMA nodes
        EAL: Multi-process socket /var/run/dpdk/rte/mp_socket
        EAL: Selected IOVA mode 'PA'
        EAL: Probing VFIO support...
        EAL:   Invalid NUMA socket, default to 0
        EAL:   Invalid NUMA socket, default to 0
        EAL: Probe PCI driver: net_ena (1d0f:ec20) device: 0000:00:06.0
(socket 0)
        EAL: No legacy callbacks, legacy socket not created
        Interactive-mode selected

        Port 0: link state change event
        testpmd: create a new mbuf pool <mb_pool_0>: n=171456,
size=2176, socket=0
        testpmd: preferred mempool ops selected: ring_mp_mc

        Warning! port-topology=paired and odd forward ports number, the
last port will pair with itself.

        Configuring Port 0 (socket 0)
        Port 0: 02:C7:17:A2:60:B1
        Checking link statuses...
        Done
```

```
        Error during enabling promiscuous mode for port 0: Operation
not supported - ignore
        testpmd> show port xstats 0
        ###### NIC extended statistics for port 0
        rx_good_packets: 0
        tx_good_packets: 0
        rx_good_bytes: 0
        tx_good_bytes: 0
        rx_missed_errors: 0
        rx_errors: 0
        tx_errors: 0
        rx_mbuf_allocation_errors: 0
        rx_q0_packets: 0
        rx_q0_bytes: 0
        rx_q0_errors: 0
        tx_q0_packets: 0
        tx_q0_bytes: 0
        wd_expired: 0
        dev_start: 1
        dev_stop: 0
        tx_drops: 0
        bw_in_allowance_exceeded: 0
        bw_out_allowance_exceeded: 0
        pps_allowance_exceeded: 0
        conntrack_allowance_exceeded: 0
        linklocal_allowance_exceeded: 0
        rx_q0_cnt: 0
        rx_q0_bytes: 0
        rx_q0_refill_partial: 0
        rx_q0_bad_csum: 0
        rx_q0_mbuf_alloc_fail: 0
        rx_q0_bad_desc_num: 0
        rx_q0_bad_req_id: 0
        tx_q0_cnt: 0
        tx_q0_bytes: 0
        tx_q0_prepare_ctx_err: 0
        tx_q0_linearize: 0
        tx_q0_linearize_failed: 0
        tx_q0_tx_poll: 0
        tx_q0_doorbells: 0
        tx_q0_bad_req_id: 0
        tx_q0_available_desc: 1023
        testpmd>
```

Weitere Informationen über die Beispielanwendung und deren Verwendung zum Abrufen erweiterter Statistiken. Siehe Testpmd Application User Guide (Testpmd-Anwendungs-Benutzerhandbuch) in der DPDK-Dokumentation.

Metriken für Instances, die FreeBSD ausführen

Ab Version 2.3.0 unterstützt der ENA-FreeBSD-Treiber das Sammeln von Netzwerkleistungsmetriken auf Instances, auf denen FreeBSD ausgeführt wird. Um die Erfassung von FreeBSD-Metriken zu aktivieren, geben Sie den folgenden Befehl ein und legen Sie das *Intervall* auf einen Wert zwischen 1 und 3 600 fest. Dies gibt an, wie oft in Sekunden FreeBSD-Metriken gesammelt werden.

```
sysctl dev.ena.network_interface.eni_metrics.sample_interval=interval
```

Mit dem folgenden Befehl wird beispielsweise festgelegt, dass der Treiber alle 10 Sekunden FreeBSD-Metriken auf der Netzwerkschnittstelle 1 sammelt:

```
sysctl dev.ena.1.eni_metrics.sample_interval=10
```

Um die Sammlung von FreeBSD-Metriken zu deaktivieren, können Sie den vorhergehenden Befehl ausführen und `0` als das *Intervall* angeben.

Sobald Sie FreeBSD-Metriken sammeln aktiviert haben, können Sie den neuesten Satz gesammelter Metriken abrufen, indem Sie den folgenden Befehl ausführen.

```
sysctl dev.ena.network_interface.eni_metrics
```

Verbessern Sie die Netzwerklatenz für Linux-basierte EC2-Instances

Die Netzwerklatenz ist die Zeitspanne, die ein Datenpaket benötigt, um von seiner Quelle zu seinem Ziel zu gelangen. Anwendungen, die Daten über das Netzwerk senden, sind auf zeitnahe Antworten angewiesen, um eine positive Benutzererfahrung zu bieten. Eine hohe Netzwerklatenz kann zu verschiedenen Problemen führen, z. B. zu den folgenden:

- Langsame Ladezeiten für Webseiten
- Verzögerung des Videostreams
- Schwierigkeiten beim Zugriff auf Online-Ressourcen

In diesem Abschnitt werden Schritte beschrieben, die Sie ergreifen können, um die Netzwerklatenz auf Amazon-EC2-Instances zu verbessern, die auf Linux ausgeführt werden. Um eine optimale Latenz zu erreichen, führen Sie die folgenden Schritte aus, um Ihre Instance, den Kernel und die ENA-Treibereinstellungen zu konfigurieren. Weitere Hinweise zur Konfiguration finden Sie unter Leitfaden für bewährte Methoden für ENA-Linux-Treiber und Leistungsoptimierung auf GitHub.

> **Note**
>
> Die Schritte und Einstellungen können je nach Ihrer spezifischen Netzwerkhardware, dem AMI, von dem aus Sie Ihre Instance gestartet haben, und Ihrem Anwendungsfall leicht variieren. Bevor Sie Änderungen vornehmen, testen und überwachen Sie Ihre Netzwerkleistung gründlich, um sicherzustellen, dass Sie die gewünschten Ergebnisse erzielen.

Die Anzahl der Netzwerk-Hops für Datenpakete reduzieren

Jeder Sprung, den ein Datenpaket bei der Übertragung von Router zu Router zurücklegt, erhöht die Netzwerklatenz. Üblicherweise muss der Datenverkehr mehrere Sprünge machen, um Ihr Ziel zu erreichen. Es gibt zwei Möglichkeiten, Netzwerksprünge für Ihre Amazon-EC2-Instances zu reduzieren:

- Cluster-Placement-Gruppe – Wenn Sie eine Cluster-Placement-Gruppe angeben, startet Amazon EC2-Instances, die sich in unmittelbarer Nähe zueinander befinden, d. h. physisch in derselben Availability Zone (AZ), mit engerer Packung. Durch die räumliche Nähe der Instances in der Gruppe können sie die Vorteile einer Hochgeschwindigkeitsverbindung nutzen, was zu niedrigen Latenzzeiten und einem hohen Durchsatz für einzelne Datenströme führt.
- Dedicated Host – Ein Dedicated Host ist ein physischer Server ausschließlich für Ihre Verwendung. Mit einem Dedicated Host können Sie Ihre Instances so starten, dass sie auf demselben physischen Server ausgeführt werden. Kommunikation zwischen Instances, die auf demselben Dedicated Host ausgeführt werden, kann ohne zusätzliche Sprünge erfolgen.

Wie Linux-Kernelkonfiguration die Latenz beeinflusst

Die Konfiguration des Linux-Kernels kann die Netzwerklatenz erhöhen oder verringern. Um Ihre Ziele zur Latenzoptimierung zu erreichen, ist es wichtig, die Konfiguration des Linux-Kernels an die spezifischen Anforderungen Ihres Workloads anzupassen.

Es gibt viele Konfigurationsoptionen für den Linux-Kernel, die helfen können, die Netzwerklatenz zu verringern. Die wirkungsvollsten Optionen sind folgende.

- Aktivieren des Besetztabfrage-Modus – Der Besetztabfrage-Modus reduziert die Latenzzeit auf dem Netzwerkempfangspfad. Wenn Sie den Besetztabfrage-Modus aktivieren, kann der Socket-Schicht-Code die Empfangswarteschlange eines Netzwerkgeräts direkt abfragen. Der Nachteil des Busy-Polls ist die höhere CPU-Auslastung des Hosts, die durch das Abrufen neuer Daten in einer engen Schleife entsteht. Es gibt zwei globale Einstellungen, welche die Anzahl der Mikrosekunden steuern, die auf Pakete für alle Schnittstellen gewartet wird.

  `busy_read`

  Ein Busy-Poll-Timeout mit geringer Latenz für Socket-Lesevorgänge. Dies steuert die Anzahl der Mikrosekunden, die gewartet wird, bis die Socket-Schicht Pakete in der Geräte-Warteschlange liest. Um das Feature global mit dem Befehl sysctl zu aktivieren, empfiehlt die Linux Kernel-Organisation einen Wert von 50 Mikrosekunden. Weitere Informationen finden Sie unter busy_read im Benutzer- und Administratorenhandbuch für Linux-Kernel.

  ```
  [ec2-user ~]$ sudo sysctl -w net.core.busy_read=50
  ```

  `busy_poll`

  Ein Busy-Poll-Timeout mit geringer Latenzzeit für die Abfrage und Auswahl. Das steuert die Anzahl der Mikrosekunden, die auf Ereignisse gewartet wird. Der empfohlene Wert liegt zwischen 50 und 100 Mikrosekunden, abhängig von der Anzahl der abzufragenden Sockets. Je mehr Sockets Sie hinzufügen, desto höher sollte die Zahl sein.

  ```
  [ec2-user ~]$ sudo sysctl -w net.core.busy_poll=50
  ```

- Konfigurieren des CPU-Energiestatus (C-Status) – C-Status steuert die Ruhezustände, in denen sich ein Kern in inaktiven Zustand befinden kann. Es kann ratsam sein, die C-Status zu steuern, um Ihr System im Hinblick auf Latenz und Leistung zu optimieren. In tieferen C-Zuständen ist die CPU im Wesentlichen „eingeschlafen“ und kann nicht auf Anfragen reagieren, bis sie aufwacht und wieder in einen aktiven Zustand übergeht. Das Versetzen von Cores in den Ruhezustand benötigt Zeit. Und auch wenn ein Core im Ruhezustand mehr Spielraum zur Nutzung einer höheren Frequenz durch einen anderen Core zulässt, dauert es auch wieder eine gewisse Zeit, bis der Core aus dem Ruhezustand erwacht und Arbeitsschritte ausführen kann.

Wenn beispielsweise ein Core, der für die Bearbeitung von Interrupts für Netzwerkpakete zuständig ist, schläft, kann es zu einer Verzögerung bei der Bearbeitung des Interrupts kommen. Sie können das System so konfigurieren, dass es keine tieferen C-Zustände verwendet. Diese Konfiguration reduziert zwar die Latenz der Prozessorreaktion, aber gleichzeitig wird auch der Turbo-Boost-Spielraum für andere Cores verringert.

Um die Reaktionslatenz des Prozessors zu verringern, können Sie tiefere C-Status begrenzen. Weitere Informationen finden Sie unter Hohe Performance und geringe Latenz durch die Beschränkung von tieferen C-Zuständen im Benutzerhandbuch für Amazon Linux 2.

Moderation unterbrechen

Der ENA-Netzwerktreiber ermöglicht die Kommunikation zwischen einer Instance und einem Netzwerk. Der Treiber verarbeitet Netzwerkpakete und leitet sie an den entsprechenden Netzwerkstapel oder die Nitro-Karte weiter. Wenn ein Netzwerkpaket eingeht, generiert die Nitro-Karte eine Unterbrechung für die CPU, um die Software über ein Ereignis zu informieren.

Unterbrechen

Eine Unterbrechung ist ein Signal, das ein Gerät oder eine Anwendung an den Prozessor sendet. Die Unterbrechung teilt dem Prozessor mit, dass ein Ereignis eingetreten ist oder eine Bedingung erfüllt wurde, die sofortige Aufmerksamkeit erfordert. Interrupts können zeitkritische Aufgaben wie den Empfang von Daten von einer Netzwerkschnittstelle, die Bearbeitung von Hardwareereignissen oder die Bearbeitung von Anforderungen von anderen Geräten erledigen.

Moderation unterbrechen

Die Interrupt-Moderation ist eine Technik, die die Anzahl der von einem Gerät generierten Interrupts reduziert, indem sie aggregiert oder verzögert werden. Der Zweck der Interrupt-Moderation besteht darin, die Systemleistung zu verbessern, indem der mit der Bearbeitung einer großen Anzahl von Interrupts verbundene Aufwand reduziert wird. Zu viele Interrupts erhöhen die CPU-Auslastung, was sich negativ auf den Durchsatz auswirkt, während zu wenige Interrupts die Latenz erhöhen.

Dynamische Interrupt-Moderation

Die dynamische Interrupt-Moderation ist eine erweiterte Form der Interrupt-Moderation, bei der die Interrupt-Rate dynamisch an die aktuelle Systemlast und die Verkehrsmuster angepasst wird.

Sie zielt darauf ab, ein Gleichgewicht zwischen der Reduzierung des Interrupt-Overheads und der Reduzierung der Pakete pro Sekunde oder Bandbreite zu finden.

> **Note**
>
> Die dynamische Unterbrechungsmoderation ist in einigen AMIs standardmäßig aktiviert (kann aber in allen AMIs aktiviert oder deaktiviert werden).

Um die Netzwerklatenz zu minimieren, ist es eventuell erforderlich, die Unterbrechungsmoderation zu deaktivieren. Dies kann jedoch auch den Aufwand für die Verarbeitung von Unterbrechungen erhöhen. Es ist wichtig, das richtige Gleichgewicht zwischen der Reduzierung der Latenzzeit und der Minimierung des Aufwands zu finden. `ethtool`-Befehle können Sie bei der Konfiguration der Unterbrechungsmoderation unterstützen. `rx-usecs` Ist standardmäßig auf `20` gesetzt und `tx-usecs` ist auf `64` gesetzt.

Verwenden Sie den folgenden Befehl, um die aktuelle Änderungskonfiguration der Unterbrechung abzurufen.

```
[ec2-user ~]$ ethtool -c interface | egrep "rx-usecs:|tx-usecs:|Adaptive RX"
Adaptive RX: on  TX: off
rx-usecs: 20
tx-usecs: 64
```

Verwenden Sie den folgenden Befehl, um die Unterbrechungsmodifikation und die dynamische Unterbrechungsmoderation zu deaktivieren.

```
[ec2-user ~]$ sudo ethtool -C interface adaptive-rx off rx-usecs 0 tx-usecs 0
```

Überlegungen zum Nitro-System für die Leistungsoptimierung

Das Nitro-System ist eine von AWS entwickelte Sammlung von Hardware- und Softwarekomponenten, die eine hohe Leistung, Verfügbarkeit und Sicherheit ermöglichen. Das Nitro-System bietet Bare-Metal-ähnliche Funktionen, die den Virtualisierungsaufwand reduzieren und Workloads unterstützen, die einen vollständigen Zugriff auf die Host-Hardware erfordern. Weitere Informationen finden Sie unter AWS Nitro System.

Alle EC2-Instance-Typen der aktuellen Generation verarbeiten Netzwerkpakete auf EC2-Nitro-Karten. Dieses Thema behandelt die Paketverarbeitung auf hoher Ebene auf der Nitro-Karte, allgemeine

Aspekte der Netzwerkarchitektur und -konfiguration, die sich auf die Leistung der Paketverarbeitung auswirken, und welche Maßnahmen Sie ergreifen können, um Spitzenleistung für Ihre Nitro-basierten Instances zu erzielen.

Nitro-Karten verarbeiten alle Eingangs- und Ausgangsschnittstellen (E/A), wie sie beispielsweise für Virtual Private Clouds (VPC) benötigt werden. Für alle Komponenten, die Informationen über das Netzwerk senden oder empfangen, fungieren die Nitro-Karten als eigenständiges Computergerät für den E/A-Datenverkehr, das physisch von der Hauptplatine des Systems getrennt ist, auf der die Workloads der Kunden ausgeführt werden.

Netzwerk-Paket-Ablauf auf Nitro-Karten

EC2-Instances, die auf dem Nitro-System basieren, verfügen über Hardwarebeschleunigungsfunktionen, die eine schnellere Paketverarbeitung ermöglichen, gemessen an den Durchsatzraten von Paketen pro Sekunde (PPS). Wenn eine Nitro-Karte die erste Evaluierung für einen neuen Ablauf durchführt, speichert sie Informationen, die für alle Pakete im Ablauf identisch sind, wie Sicherheitsgruppen, Zugriffskontrolllisten und Routing-Tabellen-Einträge. Wenn sie zusätzliche Pakete für denselben Datenfluss verarbeitet, kann sie die gespeicherten Informationen verwenden, um den Overhead für diese Pakete zu reduzieren.

Ihre Verbindungsrate wird mit der Metrik „Verbindungen pro Sekunde (CPS)“ gemessen. Jede neue Verbindung erfordert zusätzlichen Verarbeitungsaufwand, der bei den Einschätzungen der Workload-Fähigkeit berücksichtigt werden muss. Es ist wichtig, bei der Gestaltung Ihrer Workloads sowohl die CPS- als auch die PPS-Metriken zu berücksichtigen.

Wie eine Verbindung hergestellt wird

Wenn eine Verbindung zwischen einer Nitro-basierten Instance und einem anderen Endpunkt hergestellt wird, bewertet die Nitro-Karte den gesamten Datenblauf für das erste Paket, das zwischen den beiden Endpunkten gesendet oder empfangen wird. Bei nachfolgenden Paketen desselben Datenflusses ist eine vollständige Neubewertung normalerweise nicht erforderlich. Es gibt jedoch Ausnahmen. Weitere Informationen zu Ausnahmen finden Sie unter Pakete, die keine Hardwarebeschleunigung verwenden.

Die folgenden Eigenschaften definieren die beiden Endpunkte und den Paketablauf zwischen ihnen. Diese fünf Eigenschaften zusammen werden als 5-Tupelfluss bezeichnet.

- Quell-IP
- Quell-Port

- Ziel-IP
- Ziel-Port
- Kommunikationsprotokoll

Die Richtung des Paketablaufs wird als Eingang (eingehend) und Ausgang (ausgehend) bezeichnet. Die folgenden allgemeinen Beschreibungen fassen den gesamten Paketfluss im Netzwerk zusammen.

- Eingang – Wenn eine Nitro-Karte ein eingehendes Netzwerkpaket verarbeitet, bewertet sie das Paket anhand von statusbehafteten Firewallregeln und Zugriffskontrolllisten. Sie verfolgt die Verbindung, misst sie und führt gegebenenfalls weitere Aktionen durch. Anschließend leitet sie das Paket an sein Ziel auf der Host-CPU weiter.
- Ausgang – Wenn eine Nitro-Karte ein ausgehendes Netzwerkpaket verarbeitet, sucht sie nach dem Remote-Schnittstellenziel, bewertet verschiedene VPC-Funktionen, wendet Ratenbegrenzungen an und führt andere zutreffende Aktionen aus. Anschließend leitet sie das Paket an das nächste Hop-Ziel im Netzwerk weiter.

Gestalten Sie Ihr Netzwerk für optimale Leistung

Um die Leistungsfähigkeit Ihres Nitro-Systems optimal nutzen zu können, müssen Sie wissen, was Ihre Anforderungen an die Netzwerkverarbeitung sind und wie sich diese Anforderungen auf den Workload Ihrer Nitro-Ressourcen auswirken. Anschließend können Sie die optimale Leistung für Ihre Netzwerklandschaft entwerfen. Ihre Infrastruktureinstellungen sowie der Entwurf und die Konfiguration der Anwendungs-Workloads können sich sowohl auf die Paketverarbeitung als auch auf die Verbindungsraten auswirken. Wenn Ihre Anwendung beispielsweise eine hohe Verbindungsaufbaurate aufweist, z. B. ein DNS-Service, eine Firewall oder ein virtueller Router, hat sie weniger Möglichkeiten, die Hardwarebeschleunigung zu nutzen, die erst nach dem Verbindungsaufbau erfolgt.

Sie können Anwendungs- und Infrastruktureinstellungen konfigurieren, um Workloads zu rationalisieren und die Netzwerkleistung zu verbessern. Allerdings sind nicht alle Pakete für eine Beschleunigung geeignet. Das Nitro-System verwendet den gesamten Netzwerkablauf für neue Verbindungen und für Pakete, die nicht für eine Beschleunigung in Frage kommen.

Der Rest dieses Abschnitts konzentriert sich auf Überlegungen zur Anwendung und zum Infrastrukturdesign, um sicherzustellen, dass der Ablauf der Pakete so weit wie möglich innerhalb des beschleunigten Pfads erfolgt.

Überlegungen zum Netzwerkdesign für das Nitro-System

Bei der Konfiguration des Netzwerkverkehrs für Ihre Instance müssen viele Aspekte berücksichtigt werden, die sich auf die PPS-Leistung auswirken können. Sobald ein Datenablauf eingerichtet ist, können die meisten Pakete, die regelmäßig ein- oder ausgehen, beschleunigt werden. Es gibt jedoch Ausnahmen, um sicherzustellen, dass Infrastrukturdesigns und Paketflüsse weiterhin den Protokollstandards entsprechen.

Um die beste Leistung aus Ihrer Nitro-Karte herauszuholen, sollten Sie die Vor- und Nachteile der folgenden Konfigurationsdetails für Ihre Infrastruktur und Anwendungen sorgfältig abwägen.

Überlegungen zur Infrastruktur

Ihre Infrastrukturkonfiguration kann sich auf Ihren Paketablauf und Ihre Verarbeitungseffizienz auswirken. Die folgende Liste enthält einige wichtige Überlegungen.

Konfiguration der Netzwerkschnittstelle mit Asymmetrie

Sicherheitsgruppen verwenden die Verbindungsverfolgung zur Nachverfolgung des Datenverkehrs zu und von der Instance. Asymmetrisches Routing, bei dem der Datenverkehr über eine Netzwerkschnittstelle in eine Instance eingeht und über eine andere Netzwerkschnittstelle wieder austritt, kann die Spitzenleistung verringern, die eine Instance erzielen kann, wenn Datenflüsse nachverfolgt werden. Weitere Informationen zur Verbindungsverfolgung von Sicherheitsgruppen, nicht verfolgten Verbindungen und automatisch verfolgten Verbindungen finden Sie unter Verbindungsverfolgung EC2 für Amazon-Sicherheitsgruppen.

Netzwerktreiber

Netzwerktreiber werden regelmäßig aktualisiert und veröffentlicht. Wenn Ihre Treiber veraltet sind, kann dies die Leistung erheblich beeinträchtigen. Halten Sie Ihre Treiber auf dem neuesten Stand, um sicherzustellen, dass Sie über die neuesten Patches verfügen und Leistungsverbesserungen nutzen können, z. B. das Feature für beschleunigte Pfade, die nur für die neueste Treibergeneration verfügbar ist. Frühere Treiber unterstützen das Feature für beschleunigte Pfade nicht.

Um die Vorteile des Features für beschleunigte Pfade nutzen zu können, empfehlen wir Ihnen, den neuesten ENA-Treiber auf Ihren Instances zu installieren.

Linux-Instances – ENA-Linux-Treiber 2.2.9 oder höher. Informationen zur Installation oder Aktualisierung des ENA-Linux-Treibers aus dem Amazon-Treiber-GitHub-Repository finden Sie im Abschnitt Treiberkompilierung der Readme-Datei.

Windows-Instances – ENA-Windows-Treiber 2.0.0 oder höher. Informationen zur Installation oder Aktualisierung des ENA-Windows-Treibers finden Sie unter ENA-Treiber auf EC2-Windows-Instances installieren.

Entfernung zwischen Endpunkten

Eine Verbindung zwischen zwei Instances in derselben Availability Zone kann mehr Pakete pro Sekunde verarbeiten als eine Verbindung zwischen Regionen. Dies ist auf das TCP-Fenster auf Anwendungsebene zurückzuführen, das bestimmt, wie viele Daten zu einem bestimmten Zeitpunkt übertragen werden können. Große Entfernungen zwischen Instances erhöhen die Latenz und verringern die Anzahl der Pakete, die die Endpunkte verarbeiten können.

Byte-Warteschlangenlimit (BQL)

BQL ist ein Feature, das die Anzahl der an die Nitro-Karte übergebenen Byte begrenzt, um Warteschlangen zu reduzieren. BQL ist in ENA-Treibern, in Amazon-Linux-Betriebssystemen und in den meisten Linux-Distributionen standardmäßig deaktiviert. Wenn BQL und Fragment-Proxy-Override beide aktiviert sind, kann dies zu Leistungseinschränkungen führen, da die Anzahl der an Nitro übergebenen Byte begrenzt wird, bevor alle Fragmente verarbeitet werden.

Überlegungen zum Anwendungsdesign

Es gibt Aspekte des Anwendungsdesigns und der Konfiguration, die sich auf Ihre Verarbeitungseffizienz auswirken können. Die folgende Liste enthält einige wichtige Überlegungen.

Paket-Größe

Größere Paketgrößen können den Durchsatz für die Daten erhöhen, die eine Instance im Netzwerk senden und empfangen kann. Amazon EC2 unterstützt Jumbo-Frames von 9 001 Byte, dies kann jedoch bei anderen Services zu unterschiedlichen Grenzwerten führen. Kleinere Paketgrößen können die Paketverarbeitungsrate erhöhen, aber dadurch kann die maximal erreichte Bandbreite reduziert werden, wenn die Anzahl der Pakete die PPS-Erlaubnis überschreitet.

Wenn die Größe eines Pakets die maximale Übertragungseinheit (MTU) eines Netzwerk-Hops überschreitet, wird es möglicherweise von einem Router entlang des Pfads fragmentiert. Die resultierenden Paketfragmente gelten als Ausnahmen und werden normalerweise mit der Standardrate (nicht beschleunigt) verarbeitet. Dies kann zu Leistungsschwankungen führen. Sie können jedoch das Standardverhalten für ausgehende fragmentierte Pakete mit der Einstellung für den Fragment-Proxymodus außer Kraft setzen. Weitere Informationen finden Sie unter

Maximieren Sie die Netzwerkleistung auf Ihrem Nitro-System. Wir empfehlen Ihnen, Ihre Topologie bei der Konfiguration der MTU zu evaluieren.

Nachteile von Protokollen

Zuverlässige Protokolle wie TCP haben mehr Overhead als unzuverlässige Protokolle wie UDP. Der geringere Overhead und die vereinfachte Netzwerkverarbeitung für das UDP-Transportprotokoll können zu einer höheren PPS-Rate führen, allerdings auf Kosten einer zuverlässigen Paketzustellung. Wenn eine zuverlässige Paketzustellung für Ihre Anwendung nicht entscheidend ist, ist UDP möglicherweise eine gute Option.

Micro-Bursting

Micro-Bursting tritt auf, wenn der Verkehr in kurzen Zeiträumen die zulässigen Grenzwerte überschreitet und nicht gleichmäßig verteilt wird. Dies geschieht in der Regel im Mikrosekundenbereich.

Nehmen wir zum Beispiel an, Sie haben eine Instance, die bis zu 10 Gbit/s senden kann, und Ihre Anwendung sendet die vollen 10 Gbit/s in einer halben Sekunde. Dieser Micro-Burst überschreitet in der ersten halben Sekunde den zulässigen Wert und für den Rest der Sekunde bleibt nichts übrig. Auch wenn Sie in der ersten Sekunde 10 Gbit gesendet haben, können Freigaben in der ersten halben Sekunde dazu führen, dass Pakete in die Warteschlange gestellt oder verworfen werden.

Sie können einen Netzwerkplaner wie Linux Traffic Control verwenden, um Ihren Durchsatz zu beschleunigen und zu verhindern, dass Pakete aufgrund von Micro-Bursting in die Warteschlange gestellt oder verworfen werden.

Anzahl der Flows

Ein einzelner Datenablauf ist auf 5 Gbit/s begrenzt, es sei denn, er gehört zu einer Cluster-Placement-Gruppe, die bis zu 10 Gbit/s unterstützt, oder er verwendet ENA Express, das bis zu 25 Gbit/s unterstützt.

In ähnlicher Weise kann eine Nitro-Karte mehr Pakete über mehrere Datenflüsse verarbeiten, anstatt einen einzigen Datenfluss zu verwenden. Um die maximale Paketverarbeitungsrate pro Instance zu erreichen, empfehlen wir mindestens 100 Flows auf Instances mit einer Gesamtbandbreite von 100 Gbit/s oder mehr. Mit zunehmender Gesamtbandbreitenkapazität steigt auch die Anzahl der Datenflüsse, die zur Erreichung der Spitzenverarbeitungsraten erforderlich sind. Mithilfe von Benchmarking können Sie ermitteln, welche Konfiguration Sie benötigen, um Spitzenraten in Ihrem Netzwerk zu erreichen.

Elastic Network Adapter (ENA)-Warteschlangen

ENA (Elastic Network Adapter) verwendet mehrere Empfangs- (Rx) und Übertragungswarteschlangen (Tx) (ENA-Warteschlangen), um die Netzwerkleistung und Skalierbarkeit auf EC2-Instances zu verbessern. Diese Warteschlangen verwalten den Netzwerkverkehr effizient, indem sie gesendete und empfangene Daten auf die verfügbaren Warteschlangen verteilen.

Weitere Informationen finden Sie unter the section called “ENA-Warteschlangen”.

Feature Overhead-Prozess

Feature wie Traffic Mirroring und ENA Express können den Verarbeitungsaufwand erhöhen, wodurch die absolute Paketverarbeitungsleistung reduziert werden kann. Sie können die Nutzung von Features einschränken oder Feature deaktivieren, um die Paketverarbeitungsraten zu erhöhen.

Verbindungsverfolgung zur Beibehaltung des Zustands

Ihre Sicherheitsgruppen verwenden die Verbindungsverfolgung, um Informationen über den Verkehr zur und von der Instance zu speichern. Die Verbindungsverfolgung wendet Regeln für jeden einzelnen Ablauf des Netzwerkdatenverkehrs an, um zu ermitteln, ob der Datenverkehr zulässig ist oder nicht. Die Nitro-Karte verwendet Ablaufnachverfolgung, um den Status des Datenablaufs aufrechtzuerhalten. Je mehr Sicherheitsgruppenregeln angewendet werden, desto mehr Arbeit ist erforderlich, um den Ablauf auszuwerten.

> **Note**
>
> Nicht alle Datenverkehrsflüsse werden verfolgt. Wenn eine Sicherheitsgruppenregel mit Unverfolgte Verbindungen konfiguriert ist, ist keine zusätzliche Arbeit erforderlich, mit Ausnahme von Verbindungen, die automatisch nachverfolgt werden, um symmetrisches Routing zu gewährleisten, wenn mehrere gültige Antwortpfade vorhanden sind.

Pakete, die keine Hardwarebeschleunigung verwenden

Nicht alle Pakete können die Hardwarebeschleunigung nutzen. Die Behandlung dieser Ausnahmen ist mit einem gewissen Verarbeitungsaufwand verbunden, der erforderlich ist, um die Integrität Ihrer Netzwerkflüsse sicherzustellen. Netzwerkflüsse müssen zuverlässig den Protokollstandards entsprechen, Änderungen im VPC-Design entsprechen und Pakete nur an zulässige Ziele weiterleiten. Der Overhead reduziert jedoch Ihre Leistung.

Fragmente von Paketen

Wie unter Überlegungen zu Anwendungen erwähnt, werden Paketfragmente, die aus Paketen resultieren, die die Netzwerk-MTU überschreiten, normalerweise als Ausnahmen behandelt und können die Vorteile der Hardwarebeschleunigung nicht nutzen. Je nach Treiberversion können Sie jedoch die Beschränkungen für ausgehende Fragmente mit dem Fragment-Proxymodus umgehen. Weitere Informationen finden Sie unter „Aktionen, die Sie ausführen können“ im Abschnitt Maximieren Sie die Netzwerkleistung auf Ihrem Nitro-System.

Verbindungen im Leerlauf

Wenn eine Verbindung eine Zeit lang nicht aktiv ist, kann das System ihre Priorität herabsetzen, auch wenn die Verbindung ihr Timeout-Limit noch nicht erreicht hat. Wenn dann Daten eingehen, nachdem die Verbindung nicht mehr priorisiert wurde, muss das System sie ausnahmsweise behandeln, um die Verbindung wieder herzustellen.

Um Ihre Verbindungen zu verwalten, können Sie Timeouts für die Verbindungsverfolgung verwenden, um inaktive Verbindungen zu schließen. Sie können auch TCP-Keepalives verwenden, um inaktive Verbindungen aufrechtzuerhalten. Weitere Informationen finden Sie unter Timeout für die Nachverfolgung von Leerlaufverbindungen.

VPC-Mutation

Aktualisierungen von Sicherheitsgruppen, Routing-Tabellen und Zugriffskontrolllisten müssen alle im Verarbeitungspfad neu bewertet werden, um sicherzustellen, dass Routeneinträge und Sicherheitsgruppenregeln weiterhin wie erwartet gelten.

ICMP-Flows

Das Internet Control Message Protocol (ICMP) ist ein Netzwerkschichtprotokoll, das Netzwerkgeräte zur Diagnose von Netzwerkkommunikationsproblemen verwenden. Diese Pakete verwenden immer den vollen Datenfluss.

Asymmetrische L2-Abläufe

NitroV3 und frühere Plattformen verwenden keine Hardwarebeschleunigung für den Datenverkehr zwischen zwei ENIs im selben Subnetz, wobei eine ENI den Standard-Gateway-Router verwendet und die andere nicht. NitroV4 und neuere Plattformen verwenden in diesem Szenario die Hardwarebeschleunigung. Um eine bessere Leistung auf NitroV3 oder früheren Plattformen zu erzielen, stellen Sie sicher, dass entweder der verwendete Standard-Gateway-Router den beiden ENIs entspricht oder dass sich diese ENIs in unterschiedlichen Subnetzen befinden.

Maximieren Sie die Netzwerkleistung auf Ihrem Nitro-System

Sie können Ihre Netzwerkleistung auf dem Nitro-System maximieren, indem Sie die Netzwerkeinstellungen anpassen.

Themen

- Überlegungen
- Optimieren der PPS-Leistung
- ENA-Warteschlangenzuweisung konfigurieren
- Überwachen Sie die Leistung auf Linux-Instances

Überlegungen

Bevor Sie Designentscheidungen treffen oder Netzwerkeinstellungen auf Ihrer Instance anpassen, empfehlen wir Ihnen, die folgenden Schritte durchzuführen, um sicherzustellen, dass Sie das beste Ergebnis erzielen:

1. Machen Sie sich mit den Vor- und Nachteilen der Maßnahmen vertraut, die Sie ergreifen können, um die Leistung zu verbessern, indem Sie sie Überlegungen zum Netzwerkdesign für das Nitro-System überprüfen.

   Weitere Überlegungen und bewährte Methoden für Ihre Instance-Konfiguration unter Leitfaden für bewährte Methoden für ENA-Linux-Treiber und Leistungsoptimierung in GitHub.
2. Vergleichen Sie Ihre Workloads anhand der maximalen Anzahl an aktiven Datenabläufen, um eine Ausgangsbasis für Ihre Anwendungsleistung zu ermitteln. Anhand einer Leistungsbasislinie können Sie Variationen in Ihren Einstellungen oder Ihrem Anwendungsdesign testen, um herauszufinden, welche Überlegungen die größte Wirkung haben werden, insbesondere, wenn Sie eine Hochskalierung oder Aufskalierung planen.

Optimieren der PPS-Leistung

Die folgende Liste enthält Maßnahmen, die Sie je nach Ihren Systemanforderungen ergreifen können, um die Leistung Ihres PPS zu optimieren.

- Reduzieren Sie die physische Entfernung zwischen zwei Instances. Wenn sich sendende und empfangende Instances in derselben Availability Zone befinden oder Cluster-Placement-Gruppe

verwenden, können Sie die Anzahl der Hops reduzieren, die ein Paket zurücklegen muss, um von einem Endpunkt zum anderen zu gelangen.

- Verwenden Sie Unverfolgte Verbindungen.
- Verwenden Sie das UDP-Protokoll für den Netzwerkverkehr.
- Verteilen Sie bei EC2-Instances mit einer Gesamtbandbreite von 100 Gbit/s oder mehr den Workload auf 100 oder mehr einzelne Datenflüsse, um die Arbeit gleichmäßig auf die Nitro-Karte zu verteilen.
- Um das PPS-Limit für ausgehende Fragmente auf EC2-Instances zu umgehen, können Sie den Fragment-Proxymodus aktivieren (abhängig von Ihrer Treiberversion). Mit dieser Einstellung können fragmentierte Pakete im Verarbeitungspfad ausgewertet werden, wodurch das PPS-Limit für ausgehende Zugriffe von 1 024 überschritten wird. Führen Sie beim Laden des Treibers einen der folgenden Befehle aus, um den Fragment-Proxymodus zu aktivieren oder zu deaktivieren:

  Fragment-Proxymodus aktivieren

  ```
  sudo insmod ena.ko enable_frag_bypass=1
  ```

  Fragment-Proxymodus deaktivieren

  ```
  sudo insmod ena.ko enable_frag_bypass=0
  ```

ENA-Warteschlangenzuweisung konfigurieren

Bei unterstützten Instance-Typen können Sie diese Warteschlangen dynamisch über Elastic-Network-Schnittstellen (ENIs) verteilen. Die flexible ENA-Warteschlangenzuweisung optimiert die Ressourcenverteilung und ermöglicht so eine maximale vCPU-Auslastung. Workloads mit hoher Netzwerkleistung erfordern in der Regel mehrere ENA-Warteschlangen. Weitere Informationen finden Sie unter ENA-Warteschlangen.

Überwachen Sie die Leistung auf Linux-Instances

Sie können Ethtool-Metriken auf Linux-Instances verwenden, um Leistungsindikatoren für das Instance-Netzwerk wie Bandbreite, Paketrate und Verbindungsverfolgung zu überwachen. Weitere Informationen finden Sie unter Netzwerkleistung für ENA-Einstellungen auf Ihrer EC2-Instance überwachen.

Die Netzwerkleistung in EC2-Windows-Instances optimieren

Um die maximale Netzwerkleistung auf Ihren Windows-Instances mit erweitertem Netzwerk zu erreichen, müssen Sie möglicherweise die Standardkonfiguration des Betriebssystems ändern. Wir empfehlen die folgenden Konfigurationsänderungen für Anwendungen, die eine hohe Netzwerkleistung erfordern. Andere Optimierungen (wie zum Beispiel das Einschalten der Prüfsummenentladung und das Aktivieren von RSS) sind bereits in offiziellen Windows-AMIs konfiguriert.

> **Note**
>
> TCP-Chimney-Verschiebung sollte in den meisten Anwendungsfällen deaktiviert werden und ist ab Windows Server 2016 veraltet.

Zusätzlich zu diesen Betriebssystemoptimierungen sollten Sie auch die Maximum Transmission Unit (MTU, maximale Übertragungseinheit) Ihres Netzwerkverkehrs berücksichtigen und an Ihren Workload und Ihre Netzwerkarchitektur anpassen. Weitere Informationen finden Sie unter Netzwerk-MTU (Maximum Transmission Unit) für Ihre EC2-Instance.

AWS misst regelmäßig die durchschnittlichen Umlauflatenzen zwischen den Instances, die in einer Cluster Placement-Gruppe von 50us gestartet werden, und Tail-Latenzen von 200us beim Perzentil 99,9. Wenn Ihre Anwendungen konsistent niedrige Latenzen erfordern, empfehlen wir, die neueste Version der ENA-Treiber auf Instances mit fester Leistung, die auf dem Nitro-System basieren.

Konfiguration der CPU-Affinität für empfangsseitige Skalierung

Empfangsseitige Skalierung (RSS, Receive Side Scaling) wird verwendet, um die CPU-Auslastung von Netzwerkverkehr auf mehrere Prozessoren zu verteilen. Standardmäßig ist für die offiziellen Amazon Windows-AMIs RSS aktiviert. ENA-Elastic-Network-Interfaces stellen bis zu acht RSS-Warteschlangen bereit. Durch das Definieren der CPU-Affinität für RSS-Warteschlangen und andere Systemprozesse lässt sich die CPU-Auslastung auf Multi-Core-Systeme verteilen, wodurch mehr Netzwerkverkehr verarbeitet werden kann. Bei Instances mit mehr als 16 vCPUs wird empfohlen, das `Set-NetAdapterRSS`-PowerShell-Cmdlet zu verwenden, das den Boot-Prozessor (logischer Prozessor 0 und 1, wenn Hyper-Threading aktiviert ist) manuell von der RSS-Konfiguration für alle elastischen Netzwerkschnittstellen ausschließt, um eine Konkurrenzsituation mit verschiedenen Systemkomponenten zu vermeiden.

Windows ist hyper-thread-fähig und sorgt dafür, dass die RSS-Warteschlangen einer einzelnen Netzwerkkarte (NIC) immer auf verschiedenen physischen Kernen platziert werden. Sofern Hyper-Threading nicht deaktiviert ist, sollten Sie die RSS-Konfiguration jeder NIC auf einen Bereich von 16 logischen Prozessoren verteilen, um Konflikte unter anderen NICs vollständig zu vermeiden. Mit dem `Set-NetAdapterRss`-Cmdlet können Sie für jede NIC einen Bereich von gültigen logischen Prozessoren definieren, indem Sie die Werte von „BaseProcessorGroup“, „BaseProcessorNumber“, „MaxProcessingGroup“, „MaxProcessorNumber“ und „NumaNode“ (optional) festlegen. Wenn es nicht genügend physische Kerne gibt, um Konflikte zwischen NICs vollkommen zu beseitigen, sollten Sie die überlappenden Bereiche minimieren oder die Anzahl der logischen Prozessoren in den ENI-Bereichen abhängig von den voraussichtlichen Workload der ENI reduzieren (das heißt, ggf. müssen einer Administrator-Netzwerk-ENI mit geringem Volumen nicht so viele RSS-Warteschlangen zugewiesen werden). Zudem müssen, wie zuvor erwähnt, verschiedene Komponenten in der CPU 0 ausgeführt werden. Daher wird empfohlen, sie aus allen RSS-Konfigurationen auszuschließen, wenn genügend vCPUs verfügbar sind.

Wenn beispielsweise drei elastische Netzwerkschnittstellen auf einer Instance mit 72 vCPUs und 2 NUMA-Knoten mit aktiviertem Hyperthreading bestehen, verteilen die folgenden Befehle die Netzwerklast auf die beiden CPUs ohne Überlappung und verhindern die Nutzung von Kern 0 vollständig.

```
Set-NetAdapterRss -Name NIC1 -BaseProcessorGroup 0 -BaseProcessorNumber 2 -
MaxProcessorNumber 16
Set-NetAdapterRss -Name NIC2 -BaseProcessorGroup 1 -BaseProcessorNumber 0 -
MaxProcessorNumber 14
Set-NetAdapterRss -Name NIC3 -BaseProcessorGroup 1 -BaseProcessorNumber 16 -
MaxProcessorNumber 30
```

Beachten Sie, dass diese Einstellungen für jeden Netzwerkadapter bestehen bleiben. Wenn die Größe einer Instance geändert wird und die Instance danach eine andere Anzahl von vCPUs hat, sollten Sie die RSS-Konfiguration für jede aktivierte elastische Netzwerkschnittstelle erneut auswerten. Die vollständige Microsoft-Dokumentation für das cmdlet finden Sie hier: Set-NetAdapterRss.

Besonderer Hinweis für SQL-Workloads: Wir empfehlen auch, die E/A-Thread-Affinitätseinstellungen zusammen mit Ihrer RSS-Konfiguration der elastischen Netzwerkschnittstelle zu prüfen, um E/A- und Netzwerkkonflikte für dieselben CPUs zu minimieren. Weitere Informationen finden Sie unter Serverkonfiguration: Affinitätsmaske.

Elastic Fabric Adapter für AI/ML und HPC-Workloads bei Amazon EC2

Ein Elastic Fabric Adapter (EFA) ist ein Netzwerkgerät, das Sie an Ihre EC2 Amazon-Instance anschließen können, um Anwendungen für künstliche Intelligenz (KI), Machine Learning (ML) und High Performance Computing (HPC) zu beschleunigen. Mit EFA können Sie die Anwendungsleistung eines On-Premises- KI/ML- oder HPC-Clusters erreichen – mit der Skalierbarkeit, Flexibilität und Elastizität der AWS Cloud.

EFA bietet eine geringere und konsistentere Latenz und höheren Durchsatz als der TCP-Transport, der normalerweise in Cloud-basierten HPC-Systemen verwendet wird. Es verbessert die Leistung der Kommunikation zwischen Instanzen, was für Skalierungs- AI/ML und HPC-Anwendungen entscheidend ist. Es ist für die Verwendung in der vorhandenen AWS Netzwerkinfrastruktur optimiert und kann je nach Anwendungsanforderungen skaliert werden.

EFA lässt sich in Libfabric 1.7.0 und höher integrieren und unterstützt die Nvidia Collective Communications Library (NCCL) für KI- und ML-Anwendungen sowie Open MPI 4.1 und höher sowie Intel MPI 2019 Update 5 und höher für HPC-Anwendungen.

EFA unterstützt RDMA (Remote Direct Memory Access)-Schreibvorgänge auf den meisten unterstützten Instance-Typen mit Nitro Version 4 und höher. RDMA-Lesevorgänge werden auf allen Instances mit Nitro Version 4 und höher unterstützt. Weitere Informationen finden Sie unter Unterstützte Instance-Typen.

Inhalt

- EFA-Grundlagen
- Unterstützte Schnittstellen und Bibliotheken
- Unterstützte Instance-Typen
- Unterstützte Betriebssysteme
- EFA-Einschränkungen
- EFA-Preisgestaltung
- Erste Schritte mit EFA und MPI für HPC-Workloads auf Amazon EC2
- Erste Schritte mit EFA und NCCL für ML-Workloads auf Amazon EC2
- Maximieren Sie die Netzwerkbandbreite auf EC2 Amazon-Instances mit mehreren Netzwerkkarten
- Einen Elastic Fabric-Adapter erstellen und an eine EC2 Amazon-Instance anhängen

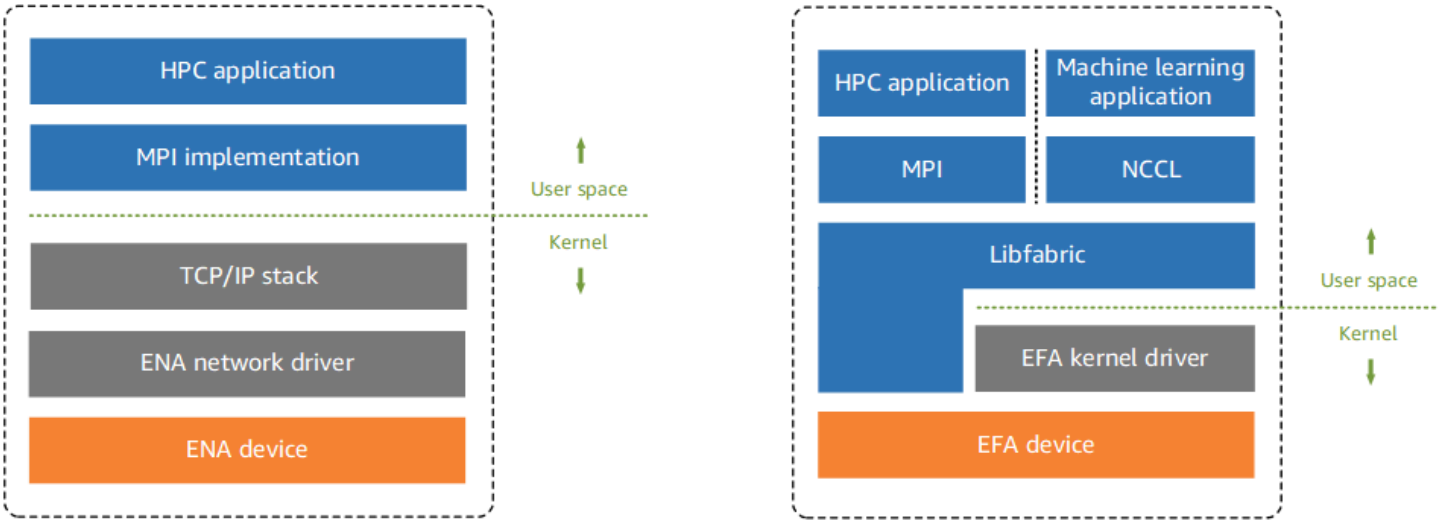
- Trennen und löschen Sie eine EFA von einer Amazon-Instance EC2
- Überwachen Sie einen Elastic Fabric-Adapter bei Amazon EC2
- Überprüfen des EFA-Installationsprogramms mithilfe einer Prüfsumme
- Versionshinweise zu Elastic Fabric Adapter

EFA-Grundlagen

Ein EFA-Gerät kann auf zwei Arten an eine Instance angehängt werden: EC2

1. Verwendung einer herkömmlichen EFA-Schnittstelle, auch EFA genannt, mit ENA, die sowohl ein EFA-Gerät als auch ein ENA-Gerät erstellt.
2. Verwendung einer reinen EFA-Schnittstelle, bei der nur das EFA-Gerät erstellt wird.

Das EFA-Gerät bietet Funktionen wie eine integrierte Betriebssystemumgehung und die Überlastungskontrolle über das SRD-Protokoll (Scalable Reliable Datagram). Die EFA-Gerätefunktionen ermöglichen zuverlässige Transportfunktionen mit niedriger Latenz, sodass die EFA-Schnittstelle eine bessere Anwendungsleistung für HPC- und ML-Anwendungen auf Amazon bietet. EC2 Das ENA-Gerät bietet dagegen herkömmliche IP-Netzwerke.



Traditionell verwenden AI/ML Anwendungen NCCL und HPC-Anwendungen das Message Passing Interface (MPI) als Schnittstelle zum Netzwerktransport des Systems. In der AWS Cloud bedeutete dies, dass Anwendungen über eine Schnittstelle zu NCCL oder MPI verfügen, die dann den TCP/IP

Stack des Betriebssystems und den ENA-Gerätetreiber verwenden, um die Netzwerkkommunikation zwischen den Instanzen zu ermöglichen.

Bei einer herkömmlichen EFA- (EFA mit ENA) oder einer reinen EFA-Schnittstelle verwenden AI/ML Anwendungen NCCL und HPC-Anwendungen MPI, um direkt mit der Libfabric-API zu kommunizieren. Die Libfabric-API umgeht den Betriebssystem-Kernel und kommuniziert direkt mit dem EFA-Gerät, um Pakete auf dem Netzwerk zu platzieren. Dies reduziert den Overhead und ermöglicht eine effizientere Ausführung von HPC-Anwendungen. AI/ML

> **Note**
>
> Libfabric ist eine Kernkomponente des OpenFabrics Interfaces (OFI) -Frameworks, das die Userspace-API von OFI definiert und exportiert. Weitere Informationen finden Sie auf der Libfabric-Website. OpenFabrics

Unterschiede zwischen ENA-, EFA- und reinen EFA-Netzwerkschnittstellen

Amazon EC2 bietet zwei Arten von Netzwerkschnittstellen:

- ENA-Schnittstellen bieten alle herkömmlichen IP-Netzwerk- und Routing-Funktionen, die zur Unterstützung von IP-Netzwerken für eine VPC erforderlich sind. Weitere Informationen finden Sie unter Ermöglichen Sie Enhanced Networking mit ENA auf Ihren EC2 Instances.
- EFA-Schnittstellen (EFA mit ENA) bieten sowohl das ENA-Gerät für IP-Netzwerke als auch das EFA-Gerät für die Kommunikation mit niedriger Latenz und hohem Durchsatz.
- Nur-EFA-Schnittstellen unterstützen nur die Funktionen des EFA-Geräts, ohne das ENA-Gerät für herkömmliche IP-Netzwerke.

Die folgende Tabelle enthält einen Vergleich von ENA-, EFA- und Nur-EFA-Netzwerkschnittstellen.

	ENA	EFA (EFA mit ENA)	Nur-EFA
Unterstützt IP-Netzwerkfunktionalität	Ja	Ja	Nein

	ENA	EFA (EFA mit ENA)	Nur-EFA
Können IPv6 Adressen zugewiesen IPv4 werden	Ja	Ja	Nein
Kann als primäre Netzwerks chnittstelle für die Instance verwendet werden	Ja	Ja	Nein
Wird auf das ENI-Anhan gslimit der Instance angerechnet	Ja	Ja	Ja
Unterstüt zung für Instance-Typen	Unterstützt auf allen Nitro-bas ierten Instance-Typen	Unterstützte Instance-Typen	Unterstützte Instance-Typen
Benennung von Parametern in EC2 APIs	`interface`	`efa`	`efa-only`
Benennung von Feldern in der EC2 Konsole	Keine Auswahl	EFA mit ENA	Nur-EFA

Unterstützte Schnittstellen und Bibliotheken

EFAs unterstützt die folgenden Schnittstellen und Bibliotheken:

- Öffnen Sie MPI 4.1 und höher
- Intel MPI 2019 Update 5 und höher
- NVIDIA Collective Communications Library (NCCL) 2.4.2 und neuer
- AWS Neuron SDK Version 2.3 und höher

Unterstützte Instance-Typen

Alle der folgenden Instance-Typen unterstützen EFA. Darüber hinaus geben die Tabellen die RDMA-Lese- und RDMA-Schreibunterstützung für die Instance-Typen an.

Nitro v6

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
Allgemeine Zwecke		
m8a.48xlarge	Ja	Ja
M8 A, Metall, 48 XL	Ja	Ja
m8i.48x groß	Ja	Ja
m8i.96xlarge	Ja	Ja
m8i.metal-48xl	Ja	Ja
m8i.metal-96xl	Ja	Ja
Für Datenverarbeitung optimiert		

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
c8a.48x groß	Ja	Ja
C8A.Metall-48 XL	Ja	Ja
c8gb. 16x groß	Ja	Ja
c 8 gb. 24 x groß	Ja	Ja
C 8 GB, Metall, 24 XL	Ja	Ja
c8gn.16x groß	Ja	Ja
c8gn.24xlarge	Ja	Ja
c8gn.48xlarge	Ja	Ja
c8gn.metal-24xl	Ja	Ja
c8gn.metal-48xl	Ja	Ja
c8i.48x groß	Ja	Ja
c8i.96xlarge	Ja	Ja
c8i.metall-48xl	Ja	Ja

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
c8i.metal-96xl	Ja	Ja
RAM-optimiert		
r8a.48x groß	Ja	Ja
r8a.metal-48xl	Ja	Ja
r8gb.16xlarge	Ja	Ja
r8gb.24xlarge	Ja	Ja
r8gb.metal-24xl	Ja	Ja
r8gn.16xlarge	Ja	Ja
r8gn.24xlarge	Ja	Ja
r8gn.48xlarge	Ja	Ja
r8gn.metal-24xl	Ja	Ja
r8gn.metal-48xl	Ja	Ja
r8i.48x groß	Ja	Ja

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
r8i.96xlarge	Ja	Ja
r8i.metall-48xl	Ja	Ja
r8i.metal-96xl	Ja	Ja
x8aedz.24x groß	Ja	Ja
x8aedz.metall-24xl	Ja	Ja
Speicheroptimiert		
i8ge.48xlarge	Ja	Nein
i8ge.metal-48xl	Ja	Nein
Beschleunigte Datenverarbeitung		
p6-b200.48xlarge	Ja	Ja
p6-b300.48x groß	Ja	Ja

Nitro v5

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
Allgemeine Zwecke		

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
m8g.24xlarge	Ja	Nein
m8g.48xlarge	Ja	Nein
m8g.metal-24xl	Ja	Nein
m8g.metal-48xl	Ja	Nein
m8gd.24xlarge	Nein	Nein
m8gd.48xlarge	Nein	Nein
m8gd.metal-24xl	Nein	Nein
m8gd.metal-48xl	Nein	Nein
Für Datenverarbeitung optimiert		
c7gn.16xlarge	Ja	Nein
c7gn.metal	Ja	Nein
c8g.24xlarge	Ja	Nein
c8g.48xlarge	Ja	Nein

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
c8g.metal-24xl	Ja	Nein
c8g.metal-48xl	Ja	Nein
c8gd.24xlarge	Nein	Nein
c8gd.48xlarge	Nein	Nein
c8gd.metal-24xl	Nein	Nein
c8gd.metal-48xl	Nein	Nein
RAM-optimiert		
r8g.24xlarge	Nein	Nein
r8g.48xlarge	Nein	Nein
r8g.metal-24xl	Nein	Nein
r8g.metal-48xl	Nein	Nein
r8gd.24xlarge	Nein	Nein
r8gd.48xlarge	Nein	Nein

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
r8gd.metal-24xl	Nein	Nein
r8gd.metal-48xl	Nein	Nein
x8g.24xlarge	Nein	Nein
x8g.48xlarge	Nein	Nein
x8g.metal-24xl	Nein	Nein
x8g.metal-48xl	Nein	Nein
Speicheroptimiert		
i7ie.48xlarge	Ja	Nein
i7ie.metal-48xl	Ja	Nein
i8g.48xlarge	Nein	Nein
Beschleunigte Datenverarbeitung		
p5en.48xlarge	Ja	Ja
p6e-gb200.36xlarge	Ja	Ja

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
trn2.48xlarge	Ja	Ja
trn2u.48xlarge	Ja	Ja
High Performance Computing (HPC)		
hpc7g.4xlarge	Ja	Nein
hpc7g.8xlarge	Ja	Nein
hpc7g.16xlarge	Ja	Nein

Nitro v4

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
Allgemeine Zwecke		
m6a.48xlarge	Ja	Ja
m6a.metal	Ja	Ja
m6i.32xlarge	Ja	Ja
m6i.metal	Ja	Ja
m6id.32xlarge	Ja	Ja

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
m6id.metal	Ja	Ja
m6idn.32xlarge	Ja	Ja
m6idn.metal	Ja	Ja
m6in.32xlarge	Ja	Ja
m6in.metal	Ja	Ja
m7a.48xlarge	Ja	Nein
m7a.metal-48xl	Ja	Nein
m7g.16xlarge	Ja	Nein
m7g.metal	Ja	Nein
m7gd.16xlarge	Ja	Nein
m7gd.metal	Ja	Nein
m7i.48xlarge	Ja	Nein
m7i.metal-48xl	Ja	Nein

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
Für Datenverarbeitung optimiert		
c6a.48xlarge	Ja	Ja
c6a.metal	Ja	Ja
c6gn.16xlarge	Ja	Ja
c6i.32xlarge	Ja	Ja
c6i.metal	Ja	Ja
c6id.32xlarge	Ja	Ja
c6id.metal	Ja	Ja
c6in.32xlarge	Ja	Ja
c6in.metal	Ja	Ja
c7a.48xlarge	Ja	Nein
c7a.metal-48xl	Ja	Nein
c7g.16xlarge	Ja	Ja

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
c7g.metal	Ja	Ja
c7gd.16xlarge	Ja	Nein
c7gd.metal	Ja	Nein
c7i.48xlarge	Ja	Nein
c7i.metal-48xl	Ja	Nein
RAM-optimiert		
r6a.48xlarge	Ja	Ja
r6a.metal	Ja	Ja
r6i.32xlarge	Ja	Ja
r6i.metal	Ja	Ja
r6id.32xlarge	Ja	Ja
r6id.metal	Ja	Ja
r6idn.32xlarge	Ja	Ja

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
r6idn.metal	Ja	Ja
r6in.32xlarge	Ja	Ja
r6in.metal	Ja	Ja
r7a.48xlarge	Nein	Nein
r7a.metal-48xl	Nein	Nein
r7g.16xlarge	Nein	Nein
r7g.metal	Nein	Nein
r7gd.16xlarge	Nein	Nein
r7gd.metal	Nein	Nein
r7i.48xlarge	Nein	Nein
r7i.metal-48xl	Nein	Nein
r7iz.32xlarge	Nein	Nein
r7iz.metal-32xl	Nein	Nein

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
u7i-6tb.112xlarge	Ja	Ja
u7i-8tb.112xlarge	Ja	Ja
u7i-12tb.224xlarge	Ja	Ja
u7in-16tb.224xlarge	Ja	Ja
u7in-24tb.224xlarge	Ja	Ja
u7in-32tb.224xlarge	Ja	Ja
u7inh-32tb.480xlarge	Ja	Ja
x2idn.32xlarge	Ja	Ja
x2idn.metal	Ja	Ja
x2iedn.32xlarge	Ja	Ja
x2iedn.metal	Ja	Ja
Speicheroptimiert		
i4g.16xlarge	Ja	Ja

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
i4i.32xlarge	Ja	Ja
i4i.metal	Ja	Ja
i7i.24x groß	Ja	Nein
i7i.48xlarge	Ja	Nein
i7i.metal-48xl	Ja	Nein
im4gn.16xlarge	Ja	Ja
Beschleunigte Datenverarbeitung		
f2.48xlarge	Ja	Ja
g6.8xlarge	Ja	Ja
g6.12xlarge	Ja	Ja
g6.16xlarge	Ja	Ja
g6.24xlarge	Ja	Ja
g6.48xlarge	Ja	Ja

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
g6e.8xlarge	Ja	Ja
g6e.12xlarge	Ja	Ja
g6e.16xlarge	Ja	Ja
g6e.24xlarge	Ja	Ja
g6e.48xlarge	Ja	Ja
gr6.8xlarge	Ja	Ja
p5.4xlarge	Ja	Ja
p5.48xlarge	Ja	Ja
p5e.48xlarge	Ja	Ja
trn1.32xlarge	Ja	Ja
trn1n.32xlarge	Ja	Ja
High Performance Computing (HPC)		
hpc6a.48xlarge	Ja	Ja

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
hpc6id.32xlarge	Ja	Ja
hpc7a.12xlarge	Ja	Nein
hpc7a.24xlarge	Ja	Nein
hpc7a.48xlarge	Ja	Nein
hpc7a.96xlarge	Ja	Nein

Nitro v3

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
Allgemeine Zwecke		
m5dn.24xlarge	Nein	Nein
m5dn.metal	Nein	Nein
m5n.24xlarge	Nein	Nein
m5n.metal	Nein	Nein
m5zn.12xlarge	Nein	Nein

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
m5zn.metal	Nein	Nein
Für Datenverarbeitung optimiert		
c5n.9xlarge	Nein	Nein
c5n.18xlarge	Nein	Nein
c5n.metal	Nein	Nein
RAM-optimiert		
r5dn.24xlarge	Nein	Nein
r5dn.metal	Nein	Nein
r5n.24xlarge	Nein	Nein
r5n.metal	Nein	Nein
x2iezn.12xlarge	Nein	Nein
x2iezn.metal	Nein	Nein
Speicheroptimiert		
i3en.12xlarge	Nein	Nein

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
i3en.24xlarge	Nein	Nein
i3en.metal	Nein	Nein
Beschleunigte Datenverarbeitung		
dl1.24xlarge	Ja	Nein
dl2q.24xlarge	Nein	Nein
g4dn.8xgroß	Nein	Nein
g4dn.12xgroß	Nein	Nein
g4dn.16xgroß	Nein	Nein
g4dn.metal	Nein	Nein
g5.8xlarge	Nein	Nein
g5.12xlarge	Nein	Nein
g5.16xlarge	Nein	Nein
g5.24xlarge	Nein	Nein

Instance-Typ	RDMA-Leseunterstützung	RDMA-Schreibunterstützung.
g5.48xlarge	Nein	Nein
inf1.24xlarge	Nein	Nein
p3dn.24xgroß	Nein	Nein
p4d.24xgroß	Ja	Nein
p4de.24xlarge	Ja	Nein
vt1.24xlarge	Nein	Nein
Vorherige Generation		
p3dn.24xgroß	Nein	Nein

Um die verfügbaren Instance-Typen zu sehen, die EFAs in einer bestimmten Region unterstützt werden

Die verfügbaren Instance-Typen variieren je nach Region. Um die verfügbaren Instance-Typen zu sehen, die EFAs in einer Region unterstützt werden, verwenden Sie den describe-instance-typesBefehl mit dem `--region` Parameter. Schließen Sie den Parameter `--filters` ein, um die Ergebnisse auf die Instance-Typen zu beschränken, die EFA unterstützen, und den Parameter `--query`, um die Ausgabe auf den Wert von `InstanceType` zu beschränken.

```
aws ec2 describe-instance-types \
    --region us-east-1  \
    --filters Name=network-info.efa-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]"  \
    --output text | sort
```

Unterstützte Betriebssysteme

Die Betriebssystemunterstützung ist je nach Prozessortyp unterschiedlich. Die folgende Tabelle zeigt die unterstützten Betriebssysteme.

Betriebssystem	Intel/AMD (**x86_64**)-Instance-Typen	AWS Graviton (**arm64**) -Instanztypen
Amazon Linux 2023	✓	✓
Amazon Linux 2	✓	✓
RHEL 8 und 9	✓	✓
Debian 11 und 12	✓	✓
Rocky Linux 8 und 9	✓	✓
Ubuntu 22.04 und 24.04	✓	✓
SUSE Linux Enterprise 15 und höher SP2	✓	✓
OpenSUSE Leap 15.5 und höher	✓	

> **Note**
>
> Einige der aufgelisteten Betriebssysteme werden möglicherweise nicht mit Intel MPI unterstützt. Wenn Sie Intel MPI verwenden, lesen Sie in der Intel-MPI-Dokumentation nach, ob Ihr Betriebssystem unterstützt wird.

EFA-Einschränkungen

EFAs haben die folgenden Einschränkungen:

- RDMA-Schreibvorgänge werden nicht bei allen Instance-Typen unterstützt. Weitere Informationen finden Sie unter Unterstützte Instance-Typen.
- EFA-Verkehr [1] zwischen d/P4de/DL P4-1-Instances und anderen Instance-Typen wird derzeit nicht unterstützt.
- Instance-Typen, die mehrere Netzwerkkarten unterstützen, können mit einer EFA pro Netzwerkkarte konfiguriert werden. Alle anderen unterstützten Instance-Typen unterstützen nur einen EFA pro Instance.
- Dedicated Instances und Dedicated Hosts werden für `c7g.16xlarge`-, `m7g.16xlarge`- und `r7g.16xlarge`-Instances nicht unterstützt, wenn ein EFA angehängt ist.
- EFA-Verkehr [1] kann Availability Zones nicht überschreiten oder. VPCs Dies gilt nicht für normalen IP-Verkehr vom ENA-Gerät einer EFA-Schnittstelle.
- EFA-Datenverkehr[1] kann nicht umgeleitet werden. Normaler IP-Datenverkehr vom ENA-Gerät einer EFA-Schnittstelle bleibt umleitbar.
- EFA wird auf nicht unterstützt. AWS Outposts
- Das EFA-Gerät einer EFA-Schnittstelle (EFA mit ENA) wird auf Windows-Instances nur für Anwendungen unterstützt, die auf dem AWS Cloud Digital Interface Software Development Kit (AWS CDI SDK) basieren. Wenn Sie eine EFA-Schnittstelle (EFA mit ENA) an eine Windows-Instance für Anwendungen anhängen, die nicht auf dem CDI-SDK basieren, funktioniert diese als ENA-Schnittstelle, jedoch ohne die zusätzlichen EFA-Gerätefunktionen. Die reine EFA-Schnittstelle wird von AWS CDI basierten Anwendungen unter Windows oder Linux nicht unterstützt. Weitere Informationen finden Sie im AWS Cloud Digital Interface Software Development Kit (AWS CDI SDK) -Benutzerhandbuch.

[1]EFA-Datenverkehr bezieht sich auf den Datenverkehr, der über das EFA-Gerät entweder über eine EFA (EFA mit ENA)- oder eine Nur-EFA-Schnittstelle übertragen wird.

EFA-Preisgestaltung

EFA ist als optionale EC2 Amazon-Netzwerkfunktion verfügbar, die Sie auf jeder unterstützten Instance ohne zusätzliche Kosten aktivieren können.

Erste Schritte mit EFA und MPI für HPC-Workloads auf Amazon EC2

Dieses Tutorial unterstützt Sie beim Starten eines EFA- und MPI-konformen Instance-Clusters für HPC-Workloads.

> **Note**
>
> Die Instances `u7i-12tb.224xlarge`, `u7in-16tb.224xlarge`, `u7in-24tb.224xlarge` und `u7in-32tb.224xlarge` können bis zu 128 parallele MPI-Prozesse mit Open MPI oder bis zu 256 parallele MPI-Prozesse mit Intel MPI ausführen.

Aufgaben

- Schritt 1: Vorbereiten einer EFA-aktivierten Sicherheitsgruppe
- Schritt 2: Starten einer temporären Instance
- Schritt 3: Installieren der EFA-Software
- Schritt 4: (Optional) Open MPI 5 aktivieren
- Schritt 5: (Optional) Installieren von Intel MPI
- Schritt 6: Ptrace-Schutz aktivieren
- Schritt 7. Bestätigen der Installation
- Schritt 8: Ihre HPC-Anwendung installieren
- Schritt 9: Ein EFA-fähiges AMI erstellen
- Schritt 10: EFA-fähige Instances in einer Cluster-Placement-Gruppe starten
- Schritt 11: Beenden der temporären Instance
- Schritt 12: Passwortloses SSH aktivieren

Schritt 1: Vorbereiten einer EFA-aktivierten Sicherheitsgruppe

Ein EFA erfordert eine Sicherheitsgruppe, die allen ein- und ausgehenden Datenverkehr von und zur Sicherheitsgruppe zulässt. Mit dem folgenden Verfahren wird eine Sicherheitsgruppe erstellt, die allen eingehenden und ausgehenden Datenverkehr zu und von der Gruppe selbst sowie eingehenden SSH-Verkehr von jeder beliebigen IPv4 Adresse für die SSH-Konnektivität zulässt.

> **Important**
>
> Diese Sicherheitsgruppe dient nur zu Testzwecken. Für Produktionsumgebungen sollten Sie eine Regel für eingehenden SSH-Datenverkehr erstellen, die Datenverkehr nur von der IP-Adresse zulässt, von der aus Sie eine Verbindung herstellen, z. B. die IP-Adresse Ihres Computers oder einen Bereich von IP-Adressen im lokalen Netzwerk.

Weitere Szenarien finden Sie unter Sicherheitsgruppenregeln für verschiedene Anwendungsfälle.

So erstellen Sie eine EFA-fähige Sicherheitsgruppe:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) und anschließend Create Security Group (Sicherheitsgruppe erstellen) aus.
3. Führen Sie im Fenster Create Security Group Folgendes aus:
   a. Geben Sie für Security group name (Name der Sicherheitsgruppe) einen beschreibenden Namen für die Sicherheitsgruppe ein, wie etwa `EFA-enabled security group`.
   b. (Optional:) Geben Sie unter Description (Beschreibung) eine kurze Beschreibung der Sicherheitsgruppe ein.
   c. Wählen Sie bei VPC die VPC aus, in der Sie Ihre EFA-fähigen Instances starten möchten.
   d. Wählen Sie Sicherheitsgruppe erstellen aus.
4. Wählen Sie die von Ihnen erstellte Sicherheitsgruppe aus und kopieren Sie dann auf der Registerkarte Details die Security group ID (Sicherheitsgruppen-ID).
5. Bei noch ausgewählter Sicherheitsgruppe wählen Sie Actions (Aktionen), Edit inbound rules (Eingangsregeln bearbeiten) aus und gehen dann folgendermaßen vor:
   a. Wählen Sie Regel hinzufügen aus.
   b. Wählen Sie für Type (Typ) die Option All traffic (Gesamter Datenverkehr) aus.
   c. Wählen Sie bei Source type (Quellentyp) Custom (Benutzerdefiniert) aus und fügen Sie die Sicherheitsgruppen-ID, die Sie kopiert hatten, ins Feld ein.
   d. Wählen Sie Regel hinzufügen aus.
   e. Wählen Sie unter Typ die Option SSH aus.
   f. Wählen Sie als Quelltyp die Option Anywhere- IPv4.

g. Wählen Sie Save rules (Regeln speichern) aus.

6. Bei noch ausgewählter Sicherheitsgruppe wählen Sie Actions (Aktionen), Edit outbound rules (Ausgangsregeln bearbeiten) aus und gehen dann folgendermaßen vor:

   a. Wählen Sie Regel hinzufügen aus.

   b. Wählen Sie für Type (Typ) die Option All traffic (Gesamter Datenverkehr) aus.

   c. Wählen Sie bei Destination type (Zieltyp) Custom (Benutzerdefiniert) aus und fügen Sie die Sicherheitsgruppen-ID, die Sie kopiert hatten, ins Feld ein.

   d. Wählen Sie Save rules (Regeln speichern) aus.

Schritt 2: Starten einer temporären Instance

Starten Sie eine temporäre Instance, die Sie verwenden können, um die EFA-Softwarekomponenten zu installieren und zu konfigurieren. Sie können mit dieser Instance ein EFA-aktiviertes AMI erstellen, von dem Sie Ihre EFA-aktivierten Instances starten können.

So starten Sie eine temporäre Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Instances starten aus, um den Launch Instance Wizard zu öffnen.
3. (Optional) Geben Sie im Bereich Name and tags (Name und Tags) einen Namen für die Instance an, z. B. `EFA-instance`. Der Name wird der Instance als Ressourcen-Tag (`Name=`*`EFA-instance`*) zugewiesen.
4. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) ein AMI für eines der unterstützten Betriebssysteme aus.
5. Wählen Sie im Bereich Instance type (Instance-Typ) einen supported instance type (unterstützten Instance-Typ) aus.
6. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das für die Instance verwendet werden soll.
7. Wählen Sie im Bereich Network settings (Netzwerkeinstellungen) Edit (Bearbeiten) aus und führen Sie dann Folgendes aus:

   a. Wählen Sie unter Subnetz das Subnetz aus, in dem die Instance gestartet werden soll. Wenn Sie kein Subnetz auswählen, können Sie die Instance nicht für EFA aktivieren.

b. Wählen Sie bei Firewall (security groups) Firewall (Sicherheitsgruppen) Select existing security group (Vorhandene Sicherheitsgruppe auswählen) und dann die Sicherheitsgruppe aus, die Sie im vorherigen Schritt erstellt haben.

c. Erweitern Sie den Abschnitt Erweiterte Netzwerkkonfiguration.

   Wählen Sie für Netzwerkschnittstelle 1 Netzwerkkartenindex = 0, Geräteindex = 0 und Schnittstellentyp = EFA mit ENA aus.

   (Optional) Wenn Sie einen Instance-Typ mit mehreren Karten verwenden, z. B. **`p4d.24xlarge`** oder **`p5.48xlarge`**, wählen Sie für jede weitere erforderliche Netzwerkschnittstelle die Option Netzwerkschnittstelle hinzufügen, wählen Sie für Netzwerkkartenindex den nächsten ungenutzten Index aus und wählen Sie dann Geräteindex = 1 und Schnittstellentyp = EFA mit ENA oder Nur-EFA aus.

8. Konfigurieren Sie im Bereich Storage (Speicher) die Volumes nach Bedarf.
9. Wählen Sie im Bereich Summary (Zusammenfassung) rechts Launch instance (Instance starten) aus.

> **Note**
>
> Erwägen Sie, die Verwendung von sowohl IMDSv2 für die temporäre Instance als auch für das AMI, das Sie in Schritt 9 erstellen, vorzuschreiben, sofern Sie dies nicht bereits IMDSv2 als Standard für das Konto festgelegt haben. Weitere Informationen zu den IMDSv2 Konfigurationsschritten finden Sie unterKonfigurieren von Instance-Metadatenoptionen für neue Instances.

Schritt 3: Installieren der EFA-Software

Installieren Sie den EFA-fähigen Kernel, die EFA-Treiber, Libfabric und den Open MPI-Stack, der zur Unterstützung von EFA auf Ihrer temporären Instance erforderlich ist.

Die Schritte unterscheiden sich abhängig davon, ob Sie EFA mit Open MPI, Intel MPI oder mit Open MPI und Intel MPI verwenden möchten.

> **Note**
>
> Einige der Betriebssysteme werden möglicherweise nicht mit Intel MPI unterstützt. Wenn Sie Intel MPI verwenden, lesen Sie in der Intel-MPI-Dokumentation nach, ob Ihr Betriebssystem unterstützt wird.

So installieren Sie die EFA-Software

1. Stellen Sie eine Verbindung zu der Instance her, die Sie gestartet haben. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance mit SSH.
2. Um sicherzustellen, dass alle Ihre Softwarepakete aktuell sind, führen Sie ein schnelles Softwareupdate auf Ihrer Instance aus. Dieser Vorgang kann einige Minuten dauern.

   - Amazon Linux 2023, Amazon Linux 2, RHEL 8/9, Rocky Linux 8/9

     ```
     $ sudo yum update -y
     ```

   - Ubuntu und Debian

     ```
     $ sudo apt-get update && sudo apt-get upgrade -y
     ```

   - SUSE Linux Enterprise

     ```
     $ sudo zypper update -y
     ```

3. Starten Sie die Instance neu und stellen Sie die Verbindung zur Instance wieder her.
4. Laden Sie die EFA-Software-Installationsdateien herunter. Die Software-Installationsdateien sind in einer komprimierten Tarball-Datei (`.tar.gz`) verpackt. Laden Sie die neueste stabile Version mit dem folgenden Befehl herunter.

   Sie erhalten die neueste Version auch, indem Sie anstelle der Versionsnummer im vorangegangenen Befehl `latest` eingeben.

   ```
   $ curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.45.1.tar.gz
   ```

5. (Optional) Überprüfen Sie die Authentizität und Integrität der EFA-Tarball-Datei (`.tar.gz`).

Diese Vorgehensweise wird empfohlen, um die Identität des Software-Publishers zu überprüfen und sicherzustellen, dass die Datei seit ihrer Veröffentlichung nicht verändert oder beschädigt wurde. Wenn Sie die Tarball-Datei nicht überprüfen möchten, überspringen Sie diesen Schritt.

> **Note**
>
> Falls Sie es vorziehen, die Tarball-Datei stattdessen mit einer SHA256 Prüfsumme MD5 oder zu verifizieren, finden Sie weitere Informationen unter. Überprüfen des EFA-Installationsprogramms mithilfe einer Prüfsumme

a. Laden Sie den öffentlichen GPG-Schlüssel herunter und importieren Sie ihn in Ihren Schlüsselbund.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
import aws-efa-installer.key
```

Der Befehl sollte einen Schlüsselwert zurückgeben. Notieren Sie sich den Schlüsselwert. Sie benötigen ihn im nächsten Schritt.

b. Überprüfen Sie den Fingerabdruck des GPG-Schlüssels. Führen Sie den folgenden Befehl aus und geben den Schlüsselwert aus dem vorherigen Schritt an.

```
$ gpg --fingerprint key_value
```

Der Befehl sollte einen Fingerabdruck zurückgeben, der mit `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC` identisch ist. Wenn der Fingerabdruck nicht übereinstimmt, führen Sie das EFA-Installationsskript nicht aus und wenden Sie sich an den Support.

c. Laden Sie die Signaturdatei herunter und überprüfen Sie die Signatur der EFA-Tarball-Datei.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.45.1.tar.gz.sig
 && gpg --verify ./aws-efa-installer-1.45.1.tar.gz.sig
```

Das folgende Beispiel zeigt eine Ausgabe.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
```

```
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Wenn das Ergebnis `Good signature` enthält und der Fingerabdruck mit dem Fingerabdruck übereinstimmt, der im vorherigen Schritt zurückgegeben wurde, fahren Sie mit dem nächsten Schritt fort. Wenn nicht, führen Sie das EFA-Installationsskript nicht aus und wenden Sie sich an den Support.

6. Extrahieren Sie die Daten aus der komprimierten `.tar.gz`-Datei und wechseln Sie in das extrahierte Verzeichnis.

```
$ tar -xf aws-efa-installer-1.45.1.tar.gz && cd aws-efa-installer
```

7. Installieren Sie die EFA-Software. Führen Sie je nach Anwendungsfall einen der folgenden Schritte durch.

> **Note**
>
> EFA unterstützt NVIDIA GPUDirect mit SUSE Linux nicht. Wenn Sie SUSE Linux verwenden, müssen Sie zusätzlich `--skip-kmod` festlegen, um die Installation von kmod zu verhindern. Standardmäßig erlaubt out-of-tree SUSE Linux keine Kernelmodule.

Open MPI and Intel MPI

Falls Sie EFA mit Open MPI und Intel MPI verwenden möchten, müssen Sie die EFA-Software mit Libfabric und Open MPI installieren und Schritt 5: Intel MPI installieren abschließen.

Führen Sie den folgenden Befehl aus, um die EFA-Software mit Libfabric und Open MPI zu installieren.

> **Note**
>
> Ab EFA 1.30.0 sind sowohl Open MPI 4.1 als auch Open MPI 5 standardmäßig installiert. Sie können optional die Version von Open MPI angeben, die Sie installieren möchten. Um nur Open MPI 4.1 zu installieren, schließen Sie Folgendes

ein: `--mpi=openmpi4` Um nur Open MPI 5 zu installieren, schließen Sie `--mpi=openmpi5` ein. Um beide zu installieren, lassen Sie die `--mpi`-Option weg.

```
$ sudo ./efa_installer.sh -y
```

Libfabric ist auf `/opt/amazon/efa` installiert. Open MPI 4.1 ist installiert auf. `/opt/amazon/openmpi` Open MPI 5 ist auf `/opt/amazon/openmpi5` installiert.

Open MPI only

Falls Sie EFA nur mit Open MPI verwenden möchten, müssen Sie die EFA-Software mit Libfabric und Open MPI installieren und können Schritt 5: Intel MPI installieren überspringen. Führen Sie den folgenden Befehl aus, um die EFA-Software mit Libfabric und Open MPI zu installieren.

> **Note**
>
> Ab EFA 1.30.0 sind sowohl Open MPI 4.1 als auch Open MPI 5 standardmäßig installiert. Sie können optional die Version von Open MPI angeben, die Sie installieren möchten. Um nur Open MPI 4.1 zu installieren, schließen Sie Folgendes ein: `--mpi=openmpi4` Um nur Open MPI 5 zu installieren, schließen Sie `--mpi=openmpi5` ein. Um beide zu installieren, lassen Sie die `--mpi`-Option weg.

```
$ sudo ./efa_installer.sh -y
```

Libfabric ist auf `/opt/amazon/efa` installiert. Open MPI 4.1 ist installiert auf. `/opt/amazon/openmpi` Open MPI 5 ist auf `/opt/amazon/openmpi5` installiert.

Intel MPI only

Wenn Sie EFA nur mit Intel MPI verwenden möchten, können Sie die EFA-Software ohne Libfabric und Open MPI installieren. In diesem Fall verwendet Intel MPI seine eingebettete Libfabric. Wenn Sie dies tun, müssen Sie Schritt :5 Intel MPI installieren abschließen.

Führen Sie den folgenden Befehl aus, um die EFA-Software ohne Libfabric und Open MPI zu installieren.

```
$ sudo ./efa_installer.sh -y --minimal
```

8. Wenn das EFA-Installationsprogramm Sie auffordert, die Instance neu zu starten, tun Sie dies und stellen Sie dann erneut eine Verbindung mit der Instance her. Melden Sie sich andernfalls von der Instance ab und wieder an, um die Installation abzuschließen.
9. Löschen Sie den unkomprimierten Tarball und den Tarball selbst. Andernfalls werden diese in das von Ihnen erstellte EFA-fähige AMI aufgenommen, wodurch dessen Größe erhöht wird.

Schritt 4: (Optional) Open MPI 5 aktivieren

> **Note**
>
> Führen Sie diesen Schritt nur aus, wenn Sie Open MPI 5 verwenden wollen.

Ab EFA 1.30.0 sind sowohl Open MPI 4.1 als auch Open MPI 5 standardmäßig installiert. Alternativ können Sie wählen, nur Open MPI 4.1 oder Open MPI 5 zu installieren.

Wenn Sie sich in Schritt 3: EFA-Software installieren für die Installation von Open MPI 5 entschieden haben und diese Software verwenden möchten, müssen Sie die folgenden Schritte ausführen, um sie zu aktivieren.

So aktivieren Sie Open MPI 5

1. Fügen Sie Open MPI 5 zur Umgebungsvariablen PATH hinzu.

   ```
   $ module load openmpi5
   ```

2. Stellen Sie sicher, dass Open MPI 5 für die Verwendung aktiviert ist.

   ```
   $ which mpicc
   ```

   Der Befehl sollte das Open-MPI-5-Installationsverzeichnis zurückgeben – `/opt/amazon/openmpi5`.

3. (Optional) Gehen Sie wie folgt vor, um sicherzustellen, dass Open MPI 5 bei jedem Start der Instance zur Umgebungsvariablen PATH hinzugefügt wird:

bash shell

Fügen Sie `module load openmpi5` zu /home/*username*/.bashrc und /home/*username*/.bash_profile hinzu.

csh and tcsh shells

Fügen Sie `module load openmpi5` zu /home/*username*/.cshrc hinzu.

Wenn Sie Open MPI 5 aus der Umgebungsvariablen PATH entfernen müssen, führen Sie den folgenden Befehl aus und entfernen Sie den Befehl aus den Shell-Startup-Skripten.

```
$ module unload openmpi5
```

Schritt 5: (Optional) Installieren von Intel MPI

> **Important**
>
> Führen Sie diesen Schritt nur aus, wenn Sie vorhaben, Intel MPI zu verwenden. Wenn Sie vorhaben, nur Open MPI zu verwenden, überspringen Sie diesen Schritt.

Intel MPI erfordert eine zusätzliche Einrichtung und Konfiguration der Umgebungsvariablen.

Voraussetzung

Stellen Sie sicher, dass der Benutzer, der die folgenden Schritte ausführt, über sudo-Berechtigungen verfügt.

So installieren Sie Intel MPI

1. Gehen Sie wie folgt vor, um das Intel MPI-Installationsskript herunterzuladen
   a. Besuchen Sie die Intel-Website.
   b. Wählen Sie im Abschnitt Intel MPI Library (Intel-MPI-Bibliothek) auf der Website den Link für Intel MPI Library for Linux, Offline-Installationsprogramm aus.
2. Führen Sie das Skript für die Installation aus, das Sie im vorherigen Schritt heruntergeladen haben.

```
$ sudo bash installation_script_name.sh
```

3. Wählen Sie im Installationsprogramm Accept & install (Akzeptieren und installieren) aus.
4. Lesen Sie das Intel-Verbesserungsprogramm durch, wählen Sie die entsprechende Option und dann Begin Installation (Mit der Installation beginnen) aus.
5. Nach abgeschlossener Installation wählen Sie Schließen aus.
6. Standardmäßig verwendet Intel MPI seine eingebettete (interne) Libfabric. Sie können Intel MPI so konfigurieren, dass stattdessen die Libfabric verwendet wird, die im EFA-Installationsprogramm enthalten ist. Typischerweise wird das EFA-Installationsprogramm mit einer neueren Version von Libfabric als Intel MPI ausgeliefert. In einigen Fällen ist Libfabric, die mit dem EFA-Installationsprogramm geliefert wird, leistungsfähiger als Intel MPI. Führen Sie je nach Shell einen der folgenden Schritte aus, um Intel MPI für die Verwendung von Libfabric zu konfigurieren, die mit dem EFA-Installationsprogramm geliefert wird.

   bash shells

   Fügen Sie die folgende Anweisung zu /home/*username*/.bashrc und /home/*username*/.bash_profile hinzu.

   ```
   export I_MPI_OFI_LIBRARY_INTERNAL=0
   ```

   csh and tcsh shells

   Fügen Sie die folgende Anweisung zu /home/*username*/.cshrc hinzu.

   ```
   setenv I_MPI_OFI_LIBRARY_INTERNAL 0
   ```

7. Fügen Sie Ihrem Shell-Skript den folgenden Quell-Befehl hinzu, um das `vars.sh`-Skript aus dem Installationsverzeichnis zum Einrichten der Compiler-Umgebung bei jedem Start der Instance zu beziehen. Führen Sie je nach Shell einen der folgenden Schritte durch.

   bash shells

   Fügen Sie die folgende Anweisung zu /home/*username*/.bashrc und /home/*username*/.bash_profile hinzu.

   ```
   source /opt/intel/oneapi/mpi/latest/env/vars.sh
   ```

csh and tcsh shells

Fügen Sie die folgende Anweisung zu /home/*username*/.cshrc hinzu.

```
source /opt/intel/oneapi/mpi/latest/env/vars.csh
```

8. Wenn EFA aufgrund einer Fehlkonfiguration nicht verfügbar ist, verwendet Intel MPI standardmäßig den TCP/IP Netzwerk-Stack, was zu einer langsameren Anwendungsleistung führen kann. Sie können dies verhindern, indem Sie `I_MPI_OFI_PROVIDER` auf `efa` setzen. Dies führt dazu, dass Intel MPI mit dem folgenden Fehler fehlschlägt, wenn EFA nicht verfügbar ist:

```
Abort (XXXXXX) on node 0 (rank 0 in comm 0): Fatal error in PMPI_Init: OtherMPI
 error,
MPIR_Init_thread (XXX).......:
MPID_Init (XXXX).............:
MPIDI_OFI_mpi_init_hook (XXXX):
open_fabric (XXXX)...........:
find_provider (XXXX).........:
OFI fi_getinfo() failed (ofi_init.c:2684:find_provider:
```

Führen Sie je nach Shell einen der folgenden Schritte durch.

bash shells

Fügen Sie die folgende Anweisung zu /home/*username*/.bashrc und /home/*username*/.bash_profile hinzu.

```
export I_MPI_OFI_PROVIDER=efa
```

csh and tcsh shells

Fügen Sie die folgende Anweisung zu /home/*username*/.cshrc hinzu.

```
setenv I_MPI_OFI_PROVIDER efa
```

9. Standardmäßig gibt Intel MPI keine Debugging-Informationen aus. Sie können verschiedene Ausführlichkeitsstufen angeben, um die Debugging-Informationen zu steuern. Mögliche Werte (in der Reihenfolge der bereitgestellten Details) sind: `0` (Standard), `1`, `2`, `3`, `4`, `5`. Level `1` und höher druckt `libfabric version` und `libfabric provider`. Verwenden Sie `libfabric`

`version`, um zu überprüfen, ob Intel MPI die interne Libfabric verwendet oder die Libfabric, die mit dem EFA-Installationsprogramm geliefert wird. Wenn es die interne Libfabric verwendet, wird der Version ein `impi` angehängt. Verwenden Sie diese `libfabric provider` Option, um zu überprüfen, ob Intel MPI EFA oder das Netzwerk verwendet. TCP/IP Wenn es EFA verwendet, ist der Wert `efa`. Wenn es TCP/IP verwendet, ist der Wert `tcp;ofi_rxm`.

Um Debugging-Informationen zu aktivieren, führen Sie je nach Shell einen der folgenden Schritte durch.

bash shells

Fügen Sie die folgende Anweisung zu /home/*username*/.bashrc und /home/*username*/.bash_profile hinzu.

```
export I_MPI_DEBUG=value
```

csh and tcsh shells

Fügen Sie die folgende Anweisung zu /home/*username*/.cshrc hinzu.

```
setenv I_MPI_DEBUG value
```

10. Standardmäßig verwendet Intel MPI den gemeinsam genutzten Speicher des Betriebssystems (`shm`) für die Kommunikation innerhalb des Knotens und verwendet Libfabric (`ofi`) nur für die Kommunikation zwischen Knoten. Im Allgemeinen bietet diese Konfiguration die beste Leistung. In einigen Fällen kann die Intel-MPI-shm-Fabric jedoch dazu führen, dass bestimmte Anwendungen auf unbestimmte Zeit hängen bleiben.

    Um dieses Problem zu lösen, können Sie Intel MPI zwingen, Libfabric sowohl für die Kommunikation innerhalb von Knoten als auch zwischen Knoten zu verwenden. Führen Sie dazu je nach Shell einen der folgenden Schritte aus.

    bash shells

    Fügen Sie die folgende Anweisung zu /home/*username*/.bashrc und /home/*username*/.bash_profile hinzu.

    ```
    export I_MPI_FABRICS=ofi
    ```

csh and tcsh shells

Fügen Sie die folgende Anweisung zu `/home/username/.cshrc` hinzu.

```
setenv I_MPI_FABRICS ofi
```

> **Note**
>
> Der EFA-Libfabric-Anbieter verwendet den gemeinsam genutzten Speicher des Betriebssystems für die Kommunikation innerhalb des Knotens. Das bedeutet, dass die Einstellung von `I_MPI_FABRICS` auf `ofi` zu einer ähnlichen Leistung führt wie die Standardkonfiguration `shm:ofi`.

11. Melden Sie sich von der Instance ab. Melden Sie sich anschließend wieder an.

Wenn Sie Intel MPI nicht mehr verwenden möchten, entfernen Sie die Umgebungsvariablen aus den Shell-Startupskripts.

Schritt 6: Ptrace-Schutz aktivieren

Um die Leistung Ihrer HPC-Anwendung zu verbessern, verwendet Libfabric den lokalen Speicher der Instance für die Kommunikation zwischen Prozessen, wenn die Prozesse auf derselben Instance ausgeführt werden.

Das Shared Memory Feature verwendet Cross Memory Attach (CMA), das mit Ptrace-Schutz nicht unterstützt wird. Wenn Sie eine Linux-Distribution verwenden, beider standardmäßig Ptrace-Schutz aktiviert hat, z. B. Ubuntu, müssen Sie ihn deaktivieren. Wenn für Ihre Linux-Distribution standardmäßig kein Ptrace-Schutz aktiviert ist, überspringen Sie diesen Schritt.

So deaktivieren Sie den Ptrace-Schutz

Führen Sie eine der folgenden Aufgaben aus:

- Führen Sie den folgenden Befehl aus, um den Ptrace-Schutz vorübergehend zu deaktivieren.

```
$ sudo sysctl -w kernel.yama.ptrace_scope=0
```

- Um den Ptrace-Schutz dauerhaft zu deaktivieren, fügen Sie `kernel.yama.ptrace_scope = 0` zu `/etc/sysctl.d/10-ptrace.conf` hinzu und starten Sie die Instance neu.

Schritt 7. Bestätigen der Installation

So bestätigen Sie die erfolgreiche Installation

1. Bestätigen Sie durch Ausführen des folgenden Befehls, dass MPI erfolgreich installiert wurde:

   ```
   $ which mpicc
   ```

   - Für Open MPI muss der zurückgegebene Pfad `/opt/amazon/` enthalten
   - Für Intel MPI muss der zurückgegebene Pfad `/opt/intel/` enthalten. Wenn Sie nicht die erwartete Ausgabe erhalten, stellen Sie sicher, dass Sie das `vars.sh`-Skript für Intel MPI bezogen haben.

2. Um zu überprüfen, ob die EFA-Softwarekomponenten und Libfabric erfolgreich installiert wurden, führen Sie den folgenden Befehl aus.

   ```
   $ fi_info -p efa -t FI_EP_RDM
   ```

   Der Befehl muss Informationen zu den Libfabric-EFA-Schnittstellen zurückgeben. Das folgende Beispiel zeigt die Befehlsausgabe.

   ```
   provider: efa
       fabric: EFA-fe80::94:3dff:fe89:1b70
       domain: efa_0-rdm
       version: 2.0
       type: FI_EP_RDM
       protocol: FI_PROTO_EFA
   ```

Schritt 8: Ihre HPC-Anwendung installieren

Installieren Sie die HPC-Anwendung auf der temporären Instance. Der Installationsvorgang unterscheidet sich je nach spezifischer HPC-Anwendung. Weitere Informationen finden Sie unter Software auf Ihrer AL2 Instance verwalten im Amazon Linux 2-Benutzerhandbuch.

> **Note**
>
> In der Dokumentation Ihrer HPC-Anwendung finden Sie Installationsanweisungen.

Schritt 9: Ein EFA-fähiges AMI erstellen

Nachdem Sie die erforderlichen Softwarekomponenten installiert haben, erstellen Sie ein AMI, das Sie erneut verwenden können, um Ihre EFA-fähigen Instances zu starten.

So erstellen Sie ein AMI aus Ihrer temporären Instance:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die temporäre Instance aus, die Sie erstellt haben, und wählen Sie anschließend Actions (Aktionen), Image und Create Image (Image erstellen) aus.
4. Gehen Sie bei Create Image (Image erstellen) wie folgt vor:
   a. Geben Sie unter Image name (Image-Name) einen beschreibenden Namen für das AMI ein.
   b. (Optional:) Geben Sie bei Image description (Image-Beschreibung) eine kurze Beschreibung des Zwecks des AMI ein.
   c. Wählen Sie Create Image (Image erstellen) aus.
5. Wählen Sie im Navigationsbereich AMIs aus.
6. Suchen Sie das AMI, das Sie erstellt haben, in der Liste. Warten Sie, bis der Status von `pending` zu `available` wechselt, bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 10: EFA-fähige Instances in einer Cluster-Placement-Gruppe starten

Starten Sie die EFA-aktivierten Instances unter Verwendung des EFA-aktiviertenAMI, das Sie in Schritt 7 erstellt haben, in einer Cluster Placement-Gruppe. Starten Sie dann die EFA-aktivierte Sicherheitsgruppe, die Sie in Schritt 1 erstellt haben.

> **Note**
>
> - Es ist keine absolute Voraussetzung, Ihre EFA-aktivierten Instances in einer Cluster-Platzierungsgruppe zu starten. Wir empfehlen allerdings, Ihre EFA-Instances in einer

Cluster-Placement-Gruppe zu starten, da die Instances dadurch in einer Gruppe mit niedriger Latenz in einer einzelnen Availability Zone gestartet werden.

- Um die Verfügbarkeit von Kapazitäten sicherzustellen, wenn Sie die Instances Ihres Clusters skalieren, können Sie eine Kapazitätsreservierung für Ihre Cluster-Placement-Gruppe erstellen. Weitere Informationen finden Sie unter Kapazitätsreservierungen mit Cluster-Placement-Gruppen verwenden.

So starten Sie eine Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Instances starten aus, um den Launch Instance Wizard zu öffnen.
3. (Optional) Geben Sie im Bereich Name and tags (Name und Tags) einen Namen für die Instance an, z. B. `EFA-instance`. Der Name wird der Instance als Ressourcen-Tag (`Name=`*`EFA-instance`*) zugewiesen.
4. Wählen Sie im Abschnitt Anwendungs- und Betriebssystemimages die Option My AMIs und dann das AMI aus, das Sie im vorherigen Schritt erstellt haben.
5. Wählen Sie im Bereich Instance type (Instance-Typ) einen supported instance type (unterstützten Instance-Typ) aus.
6. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das für die Instance verwendet werden soll.
7. Wählen Sie im Bereich Network settings (Netzwerkeinstellungen) Edit (Bearbeiten) aus und führen Sie dann Folgendes aus:

   a. Wählen Sie unter Subnetz das Subnetz aus, in dem die Instance gestartet werden soll. Wenn Sie kein Subnetz auswählen, können Sie die Instance nicht für EFA aktivieren.

   b. Wählen Sie bei Firewall (security groups) Firewall (Sicherheitsgruppen) Select existing security group (Vorhandene Sicherheitsgruppe auswählen) und dann die Sicherheitsgruppe aus, die Sie im vorherigen Schritt erstellt haben.

   c. Erweitern Sie den Abschnitt Erweiterte Netzwerkkonfiguration.

      Wählen Sie für Netzwerkschnittstelle 1 Netzwerkkartenindex = 0, Geräteindex = 0 und Schnittstellentyp = EFA mit ENA aus.

(Optional) Wenn Sie einen Instance-Typ mit mehreren Karten verwenden, z. B. `p4d.24xlarge` oder `p5.48xlarge`, wählen Sie für jede weitere erforderliche Netzwerkschnittstelle die Option Netzwerkschnittstelle hinzufügen, wählen Sie für Netzwerkkartenindex den nächsten ungenutzten Index aus und wählen Sie dann Geräteindex = 1 und Schnittstellentyp = EFA mit ENA oder Nur-EFA aus.

8. (Optional) Konfigurieren Sie im Bereich Storage (Speicher) die Volumes nach Bedarf.
9. Wählen Sie im Bereich Advanced details (Erweiterte Details) bei Placement group name (Placement-Gruppen-Name) die Cluster-Placement-Gruppe aus, in der die Instances gestartet werden sollen. Wenn Sie eine neue Cluster-Placement-Gruppe erstellen müssen, wählen Sie Create new placement group (Neue Placement-Gruppe erstellen).
10. Geben Sie im Bereich Summary (Zusammenfassung) rechts bei Number of instances (Anzahl der Instances) die Anzahl EFA-fähiger Instances ein, die Sie starten möchten, und wählen Sie dann Launch instance (Instance starten).

Schritt 11: Beenden der temporären Instance

An diesem Punkt benötigen Sie die temporäre Instance, die Sie in Schritt 2 gestartet haben, nicht mehr. Sie können die Instance beenden, damit keine weiteren Kosten dafür anfallen.

So beenden Sie die temporäre Instance:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die temporäre instance aus, die Sie erstellt haben, und wählen Sie anschließend Aktionen, Instance-Zustand und Instance beenden (löschen) aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Beenden (löschen) aus.

Schritt 12: Passwortloses SSH aktivieren

Damit Ihre Anwendungen auf allen Instances in Ihrem Cluster ausgeführt werden können, müssen Sie passwortlosen SSH-Zugriff vom Führungsknoten auf die Mitgliedsknoten aktivieren. Der Führungsknoten ist die Instance, von der aus Sie die Anwendungen ausführen. Die verbleibenden Instances im Cluster sind die Mitgliedsknoten.

So aktivieren Sie passwortloses SSH zwischen den Instances im Cluster:

1. Wählen Sie eine Instance im Cluster als Führungsknoten aus und stellen Sie eine Verbindung zu ihr her.
2. Deaktivieren Sie `strictHostKeyChecking` und aktivieren Sie `ForwardAgent` für den Führungsknoten. Öffnen Sie `~/.ssh/config` mit dem bevorzugten Texteditor und fügen Sie Folgendes hinzu.

   ```
   Host *
       ForwardAgent yes
   Host *
       StrictHostKeyChecking no
   ```

3. Generieren Sie ein RSA-Schlüsselpaar.

   ```
   $ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
   ```

   Das Schlüsselpaar wird im `$HOME/.ssh/`-Verzeichnis erstellt.
4. Ändern Sie die Berechtigungen des privaten Schlüssels auf dem Führungsknoten.

   ```
   $ chmod 600 ~/.ssh/id_rsa
   chmod 600 ~/.ssh/config
   ```

5. Öffnen Sie `~/.ssh/id_rsa.pub` mit Ihrem bevorzugten Texteditor und kopieren Sie den Schlüssel.
6. Gehen Sie für jeden Mitgliedsknoten im Cluster wie folgt vor:

   a. Stellen Sie eine Verbindung mit der Instance her.

   b. Öffnen Sie `~/.ssh/authorized_keys` mit Ihrem bevorzugten Texteditor und fügen Sie den öffentlichen Schlüssel hinzu, den Sie zuvor kopiert haben.
7. Um zu testen, ob das passwortlose SSH wie erwartet funktioniert, stellen Sie eine Verbindung zum Leaderknoten her und führen Sie den folgenden Befehl aus.

   ```
   $ ssh member_node_private_ip
   ```

   Sie sollten eine Verbindung zum Mitgliedsknoten herstellen können, ohne zur Eingabe eines Schlüssels oder Passworts aufgefordert zu werden.

Erste Schritte mit EFA und NCCL für ML-Workloads auf Amazon EC2

Die NVIDIA Collective Communications Library (NCCL) ist eine Bibliothek mit standardmäßigen kollektiven Kommunikationsroutinen für mehrere Benutzer GPUs über einen einzelnen Knoten oder mehrere Knoten. Die NCCL kann zusammen mit EFA, libfabric und MPI verwendet werden, um verschiedene Machine-Learning-Workloads zu unterstützen. Weitere Informationen finden Sie auf der NCCL-Website.

Voraussetzungen

- Nur Instance-Typen der P-Serie mit beschleunigter Datenverarbeitung werden unterstützt. Weitere Informationen finden Sie unter Amazon EC2 Accelerated Computing Instances.
- Nur Amazon Linux 2023, Amazon Linux 2, Ubuntu 24.04 und Ubuntu 22.04 Base AMIs werden unterstützt.
- Die NCCL wird erst ab Version 2.4.2 mit EFA unterstützt.

Weitere Informationen zum Ausführen von Machine-Learning-Workloads mit EFA und NCCL unter Verwendung von finden Sie unter AWS Deep Learning AMIs Using EFA on the DLAMI im Developer Guide.AWS Deep Learning AMIs

Schritte

- Schritt 1: Vorbereiten einer EFA-aktivierten Sicherheitsgruppe
- Schritt 2: Starten einer temporären Instance
- Schritt 3: Installieren der Nvidia-GPU-Treiber, des Nvidia-CUDA-Toolkits und cuDNN
- Schritt 4: Installieren GDRCopy
- Schritt 5: Installieren der EFA-Software
- Schritt 6: Installieren der NCCL
- Schritt 7: Installieren der NCCL-Tests
- Schritt 8: Testen der EFA- und NCCL-Konfiguration
- Schritt 9: Installieren der Machine-Learning-Anwendungen
- Schritt 10: Erstellen eines EFA- und NCCL-konformen AMI
- Schritt 11: Beenden der temporären Instance
- Schritt 12: Starten von EFA- und NCCL-konformen Instances in einer Cluster Placement-Gruppe

- Schritt 13: Aktivieren von passwortlosem SSH

Schritt 1: Vorbereiten einer EFA-aktivierten Sicherheitsgruppe

Ein EFA erfordert eine Sicherheitsgruppe, die allen ein- und ausgehenden Datenverkehr von und zur Sicherheitsgruppe zulässt. Mit dem folgenden Verfahren wird eine Sicherheitsgruppe erstellt, die den gesamten eingehenden und ausgehenden Datenverkehr von und zu sich selbst zulässt und die eingehenden SSH-Verkehr von jeder beliebigen Adresse für SSH-Konnektivität zulässt. IPv4

> **Important**
>
> Diese Sicherheitsgruppe dient nur zu Testzwecken. Für Produktionsumgebungen sollten Sie eine Regel für eingehenden SSH-Datenverkehr erstellen, die Datenverkehr nur von der IP-Adresse zulässt, von der aus Sie eine Verbindung herstellen, z. B. die IP-Adresse Ihres Computers oder einen Bereich von IP-Adressen im lokalen Netzwerk.

Weitere Szenarien finden Sie unter Sicherheitsgruppenregeln für verschiedene Anwendungsfälle.

So erstellen Sie eine EFA-fähige Sicherheitsgruppe:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) und anschließend Create Security Group (Sicherheitsgruppe erstellen) aus.
3. Führen Sie im Fenster Create Security Group Folgendes aus:
   a. Geben Sie für Security group name (Name der Sicherheitsgruppe) einen beschreibenden Namen für die Sicherheitsgruppe ein, wie etwa `EFA-enabled security group`.
   b. (Optional:) Geben Sie unter Description (Beschreibung) eine kurze Beschreibung der Sicherheitsgruppe ein.
   c. Wählen Sie bei VPC die VPC aus, in der Sie Ihre EFA-fähigen Instances starten möchten.
   d. Wählen Sie Sicherheitsgruppe erstellen aus.
4. Wählen Sie die von Ihnen erstellte Sicherheitsgruppe aus und kopieren Sie dann auf der Registerkarte Details die Security group ID (Sicherheitsgruppen-ID).
5. Bei noch ausgewählter Sicherheitsgruppe wählen Sie Actions (Aktionen), Edit inbound rules (Eingangsregeln bearbeiten) aus und gehen dann folgendermaßen vor:

a. Wählen Sie Regel hinzufügen aus.
b. Wählen Sie für Type (Typ) die Option All traffic (Gesamter Datenverkehr) aus.
c. Wählen Sie bei Source type (Quellentyp) Custom (Benutzerdefiniert) aus und fügen Sie die Sicherheitsgruppen-ID, die Sie kopiert hatten, ins Feld ein.
d. Wählen Sie Regel hinzufügen aus.
e. Wählen Sie unter Typ die Option SSH aus.
f. Wählen Sie als Quelltyp die Option Anywhere- IPv4.
g. Wählen Sie Save rules (Regeln speichern) aus.

6. Bei noch ausgewählter Sicherheitsgruppe wählen Sie Actions (Aktionen), Edit outbound rules (Ausgangsregeln bearbeiten) aus und gehen dann folgendermaßen vor:

a. Wählen Sie Regel hinzufügen aus.
b. Wählen Sie für Type (Typ) die Option All traffic (Gesamter Datenverkehr) aus.
c. Wählen Sie bei Destination type (Zieltyp) Custom (Benutzerdefiniert) aus und fügen Sie die Sicherheitsgruppen-ID, die Sie kopiert hatten, ins Feld ein.
d. Wählen Sie Save rules (Regeln speichern) aus.

Schritt 2: Starten einer temporären Instance

Starten Sie eine temporäre Instance, die Sie verwenden können, um die EFA-Softwarekomponenten zu installieren und zu konfigurieren. Sie können mit dieser Instance ein EFA-aktiviertes AMI erstellen, von dem Sie Ihre EFA-aktivierten Instances starten können.

So starten Sie eine temporäre Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Instances starten aus, um den Launch Instance Wizard zu öffnen.
3. (Optional) Geben Sie im Bereich Name and tags (Name und Tags) einen Namen für die Instance an, z. B. `EFA-instance`. Der Name wird der Instance als Ressourcen-Tag (`Name=`*`EFA-instance`*) zugewiesen.
4. Wählen Sie im Bereich Anwendungs- und Betriebssystem-Images ein AMI für eines der unterstützten Betriebssysteme aus.
5. Wählen Sie im Bereich Instance-Typ einen unterstützten Instance-Typ aus.

6. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das für die Instance verwendet werden soll.
7. Wählen Sie im Bereich Network settings (Netzwerkeinstellungen) Edit (Bearbeiten) aus und führen Sie dann Folgendes aus:

   a. Wählen Sie unter Subnetz das Subnetz aus, in dem die Instance gestartet werden soll. Wenn Sie kein Subnetz auswählen, können Sie die Instance nicht für EFA aktivieren.

   b. Wählen Sie bei Firewall (security groups) Firewall (Sicherheitsgruppen) Select existing security group (Vorhandene Sicherheitsgruppe auswählen) und dann die Sicherheitsgruppe aus, die Sie im vorherigen Schritt erstellt haben.

   c. Erweitern Sie den Abschnitt Erweiterte Netzwerkkonfiguration.

      Wählen Sie für Netzwerkschnittstelle 1 Netzwerkkartenindex = 0, Geräteindex = 0 und Schnittstellentyp = EFA mit ENA aus.

      (Optional) Wenn Sie einen Instance-Typ mit mehreren Karten verwenden, z. B. `p4d.24xlarge` oder `p5.48xlarge`, wählen Sie für jede weitere erforderliche Netzwerkschnittstelle die Option Netzwerkschnittstelle hinzufügen, wählen Sie für Netzwerkkartenindex den nächsten ungenutzten Index aus und wählen Sie dann Geräteindex = 1 und Schnittstellentyp = EFA mit ENA oder Nur-EFA aus.

8. Konfigurieren Sie im Bereich Storage (Speicher) die Volumes nach Bedarf.

   > **Note**
   >
   > Sie müssen zusätzliche 10 bis 20 GiB Speicher für das Nvidia CUDA Toolkit bereitstellen. Wenn Sie nicht genügend Speicherplatz bereitstellen, erhalten Sie einen `insufficient disk space`-Fehler beim Versuch, die Nvidia-Treiber und das CUDA-Toolkit zu installieren.

9. Wählen Sie im Bereich Summary (Zusammenfassung) rechts Launch instance (Instance starten) aus.

Schritt 3: Installieren der Nvidia-GPU-Treiber, des Nvidia-CUDA-Toolkits und cuDNN

Amazon Linux 2023 and Amazon Linux 2

Installieren der Nvidia GPU-Treiber, des Nvidia-CUDA-Toolkits und cuDNN

1. Um sicherzustellen, dass alle Ihre Softwarepakete aktuell sind, führen Sie ein schnelles Softwareupdate auf Ihrer Instance aus.

   ```
   $ sudo yum upgrade -y && sudo reboot
   ```

   Stellen Sie nach dem Neustart der Instance erneut eine Verbindung dazu her.

2. Installieren Sie die Dienstprogramme, die zum Installieren der Nvidia GPU-Treiber und des Nvidia CUDA-Toolkits benötigt werden.

   ```
   $ sudo yum groupinstall 'Development Tools' -y
   ```

3. Deaktivieren Sie die `nouveau`-Open-Source-Treiber.

   a. Installieren Sie die erforderlichen Dienstprogramme und das Kernel-Header-Paket für Ihre derzeit ausgeführte Kernel-Version.

      ```
      $ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -r)
      ```

   b. Fügen Sie `nouveau` der Verweigerungsliste `/etc/modprobe.d/blacklist.conf` hinzu.

      ```
      $ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
      blacklist vga16fb
      blacklist nouveau
      blacklist rivafb
      blacklist nvidiafb
      blacklist rivatv
      EOF
      ```

   c. Hängen Sie `GRUB_CMDLINE_LINUX="rdblacklist=nouveau"` an die `grub`-Datei an und erstellen Sie die Grub-Konfiguration neu.

```
$ echo 'GRUB_CMDLINE_LINUX="rdblacklist=nouveau"' | sudo tee -a /etc/
default/grub \
&& sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Starten Sie die Instance neu und stellen Sie die Verbindung zur Instance wieder her.
5. Vorbereiten der erforderlichen Repositorys

   a. Aktivieren Sie das EPEL Repository und legen Sie die Distribution auf `rhel7` fest.

   ```
   $ sudo amazon-linux-extras install epel \
   && distribution='rhel7'
   ```

   b. Richten Sie das CUDA Netzwerk-Repository ein und aktualisieren Sie den Repository-Cache.

   ```
   $ ARCH=$( /bin/arch ) \
   && sudo yum-config-manager --add-repo http://developer.download.nvidia.com/
   compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \
   && sudo yum clean expire-cache
   ```

   c. (Nur Kernel-Version 5.10) Führen Sie diese Schritte nur aus, wenn Sie Amazon Linux 2 mit Kernel-Version 5.10 nutzen. Überspringen Sie dieses Schritte, wenn Sie Amazon Linux 2 mit Kernel-Version 4.12 verwenden. Um Ihre Kernel-Version zu überprüfen, führen Sie uname -r aus.

      i. Erstellen Sie die Nvidia-Treiberkonfigurationsdatei mit dem Namen `/etc/dkms/nvidia.conf`.

      ```
      $ sudo mkdir -p /etc/dkms \
      && echo "MAKE[0]=\"'make' -j2 module SYSSRC=\${kernel_source_dir}
       IGNORE_XEN_PRESENCE=1 IGNORE_PREEMPT_RT_PRESENCE=1 IGNORE_CC_MISMATCH=1
       CC=/usr/bin/gcc10-gcc\"" | sudo tee /etc/dkms/nvidia.conf
      ```

      ii. (Nur `p4d.24xlarge` und `p5.48xlarge`) Kopieren Sie die Konfigurationsdatei des Nvidia-Treibers.

      ```
      $ sudo cp /etc/dkms/nvidia.conf /etc/dkms/nvidia-open.conf
      ```

6. Installieren Sie die Nvidia-GPU-Treiber, das NVIDIA CUDA-Toolkit und cuDNN.

```
$ sudo yum clean all \
&& sudo yum -y install nvidia-driver-latest-dkms \
&& sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
```

7. Starten Sie die Instance neu und stellen Sie die Verbindung zur Instance wieder her.
8. (Nur `p4d.24xlarge` und `p5.48xlarge`) Starten Sie den NVIDIA Fabric Manager Service und stellen Sie sicher, dass er beim Start der Instance automatisch gestartet wird. Nvidia Fabric Manager ist für das NV Switch Management erforderlich.

   ```
   $ sudo systemctl enable nvidia-fabricmanager && sudo systemctl start nvidia-
   fabricmanager
   ```

9. Stellen Sie sicher, dass die CUDA-Pfade bei jedem Start der Instance festgelegt werden.

   - Fügen Sie für Bash-Shells die folgenden Anweisungen zu /home/*username*/.bashrc und /home/*username*/.bash_profile hinzu.

     ```
     export PATH=/usr/local/cuda/bin:$PATH
     export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

   - Fügen Sie für tcsh-Shells die folgenden Anweisungen zu /home/*username*/.cshrc hinzu.

     ```
     setenv PATH=/usr/local/cuda/bin:$PATH
     setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

10. Führen Sie den folgenden Befehl aus, um zu bestätigen, dass die Nvidia GPU-Treiber funktionieren.

    ```
    $ nvidia-smi -q | head
    ```

    Der Befehl sollte Informationen über die Nvidia- GPUs, Nvidia-GPU-Treiber und das Nvidia-CUDA-Toolkit zurückgeben.

Ubuntu 24.04 and Ubuntu 22.04

Installieren der Nvidia GPU-Treiber, des Nvidia-CUDA-Toolkits und cuDNN

1. Um sicherzustellen, dass alle Ihre Softwarepakete aktuell sind, führen Sie ein schnelles Softwareupdate auf Ihrer Instance aus.

```
$ sudo apt-get update && sudo apt-get upgrade -y
```

2. Installieren Sie die Dienstprogramme, die zum Installieren der Nvidia GPU-Treiber und des Nvidia CUDA-Toolkits benötigt werden.

```
$ sudo apt-get update && sudo apt-get install build-essential -y
```

3. Um den Nvidia GPU-Treiber verwenden zu können, müssen Sie zunächst die `nouveau`-Open-Source-Treiber deaktivieren.

   a. Installieren Sie die erforderlichen Dienstprogramme und das Kernel-Header-Paket für Ihre derzeit ausgeführte Kernel-Version.

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

   b. Fügen Sie `nouveau` der Verweigerungsliste `/etc/modprobe.d/blacklist.conf` hinzu.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   c. Öffnen Sie `/etc/default/grub` mit dem bevorzugten Texteditor und fügen Sie Folgendes hinzu.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   d. Erstellen Sie die neue Grub-Konfiguration.

```
$ sudo update-grub
```

4. Starten Sie die Instance neu und stellen Sie die Verbindung zur Instance wieder her.
5. Fügen Sie das CUDA-Repository hinzu und installieren Sie die Nvidia-GPU-Treiber, das NVIDIA-CUDA-Toolkit und cuDNN.

   - `p3dn.24xlarge`

     ```
     $ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
     machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
     && wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
     machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
     ubuntu2004_1.0.0-1_amd64.deb \
     && sudo dpkg -i /tmp/deeplearning.deb \
     && wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
     repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
     && sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
     && sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
     compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
     && sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
     cuda/repos/ubuntu2004/x86_64/ /' \
     && sudo apt update \
     && sudo apt install nvidia-dkms-535 \
     && sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
      cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
     ```

   - `p4d.24xlarge` und `p5.48xlarge`

     ```
     $ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
     machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
     && wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
     machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
     ubuntu2004_1.0.0-1_amd64.deb \
     && sudo dpkg -i /tmp/deeplearning.deb \
     && wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
     repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
     && sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
     && sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
     compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
     && sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
     cuda/repos/ubuntu2004/x86_64/ /' \
     && sudo apt update \
     && sudo apt install nvidia-kernel-open-535 \
     ```

```
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
 cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

6. Starten Sie die Instance neu und stellen Sie die Verbindung zur Instance wieder her.
7. (Nur `p4d.24xlarge` und `p5.48xlarge`) Installieren Sie den NVIDIA Fabric Manager.

   a. Sie müssen die Version von Nvidia Fabric Manager installieren, die mit der Version des Nvidia-Kernelmoduls übereinstimmt, die Sie im vorherigen Schritt installiert haben.

      Führen Sie den folgenden Befehl aus, um die Version des Nvidia Kernelmoduls zu bestimmen.

      ```
      $ cat /proc/driver/nvidia/version | grep "Kernel Module"
      ```

      Es folgt eine Beispielausgabe.

      ```
      NVRM version: NVIDIA UNIX x86_64 Kernel Module  450.42.01  Tue Jun 15
       21:26:37 UTC 2021
      ```

      Im obigen Beispiel wurde die Hauptversion `450` des Kernel-Moduls installiert. Dies bedeutet, dass Sie die Nvidia Fabric Manager-Version `450` installieren müssen.

   b. Installieren Sie den Nvidia Fabric Manager. Führen Sie den folgenden Befehl aus, und geben Sie die im vorherigen Schritt angegebene Hauptversion an.

      ```
      $ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
      fabricmanager-major_version_number
      ```

      Zum Beispiel, wenn die Hauptversion `450` des Kernelmoduls installiert wurde, verwenden Sie den folgenden Befehl, um die passende Version von Nvidia Fabric Manager zu installieren.

      ```
      $ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
      fabricmanager-450
      ```

   c. Starten Sie den Dienst und stellen Sie sicher, dass er beim Start der Instance automatisch gestartet wird. Nvidia Fabric Manager ist für das NV Switch Management erforderlich.

```
$ sudo systemctl start nvidia-fabricmanager && sudo systemctl enable nvidia-
fabricmanager
```

8. Stellen Sie sicher, dass die CUDA-Pfade bei jedem Start der Instance festgelegt werden.

   - Fügen Sie für Bash-Shells die folgenden Anweisungen zu /home/*username*/.bashrc und /home/*username*/.bash_profile hinzu.

     ```
     export PATH=/usr/local/cuda/bin:$PATH
     export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

   - Fügen Sie für tcsh-Shells die folgenden Anweisungen zu /home/*username*/.cshrc hinzu.

     ```
     setenv PATH=/usr/local/cuda/bin:$PATH
     setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

9. Führen Sie den folgenden Befehl aus, um zu bestätigen, dass die Nvidia GPU-Treiber funktionieren.

   ```
   $ nvidia-smi -q | head
   ```

   Der Befehl sollte Informationen zu den Nvidia- GPUs, Nvidia-GPU-Treibern und dem Nvidia CUDA-Toolkit zurückgeben.

Schritt 4: Installieren GDRCopy

Installieren Sie GDRCopy , um die Leistung von Libfabric zu verbessern. Weitere Informationen zu GDRCopy finden Sie im GDRCopy Repository.

Amazon Linux 2023 and Amazon Linux 2

Um zu installieren GDRCopy

1. Installieren Sie die erforderlichen Abhängigkeiten.

```
$ sudo yum -y install dkms rpm-build make check check-devel subunit subunit-
devel
```

2. Laden Sie das Paket herunter und GDRCopy entpacken Sie es.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz ; cd gdrcopy-2.4/packages
```

3. Erstellen Sie das GDRCopy RPM-Paket.

```
$ CUDA=/usr/local/cuda ./build-rpm-packages.sh
```

4. Installieren Sie das GDRCopy RPM-Paket.

```
$ sudo rpm -Uvh gdrcopy-kmod-2.4-1dkms.noarch*.rpm \
&& sudo rpm -Uvh gdrcopy-2.4-1.x86_64*.rpm \
&& sudo rpm -Uvh gdrcopy-devel-2.4-1.noarch*.rpm
```

Ubuntu 24.04 and Ubuntu 22.04

Um zu installieren GDRCopy

1. Installieren Sie die erforderlichen Abhängigkeiten.

```
$ sudo apt -y install build-essential devscripts debhelper check libsubunit-dev
 fakeroot pkg-config dkms
```

2. Laden Sie das Paket herunter und GDRCopy entpacken Sie es.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz \
&& cd gdrcopy-2.4/packages
```

3. Erstellen Sie das GDRCopy RPM-Paket.

```
$ CUDA=/usr/local/cuda ./build-deb-packages.sh
```

4. Installieren Sie das GDRCopy RPM-Paket.

```
$ sudo dpkg -i gdrdrv-dkms_2.4-1_amd64.*.deb \
```

```
&& sudo dpkg -i libgdrapi_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy-tests_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy_2.4-1_amd64.*.deb
```

Schritt 5: Installieren der EFA-Software

Installieren Sie den EFA-fähigen Kernel, die EFA-Treiber, Libfabric, aws-ofi-nccl das Plugin und den Open MPI-Stack, der für die Unterstützung von EFA auf Ihrer Instance erforderlich ist.

So installieren Sie die EFA-Software

1. Stellen Sie eine Verbindung zu der Instance her, die Sie gestartet haben. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance mit SSH.
2. Laden Sie die EFA-Software-Installationsdateien herunter. Die Software-Installationsdateien sind in einer komprimierten Tarball-Datei (`.tar.gz`) verpackt. Laden Sie die neueste stabile Version mit dem folgenden Befehl herunter.

   Sie erhalten die neueste Version auch, indem Sie anstelle der Versionsnummer im vorangegangenen Befehl `latest` eingeben.

   ```
   $ curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.45.1.tar.gz
   ```

3. (Optional) Überprüfen Sie die Authentizität und Integrität der EFA-Tarball-Datei (`.tar.gz`).

   Diese Vorgehensweise wird empfohlen, um die Identität des Software-Publishers zu überprüfen und sicherzustellen, dass die Datei seit ihrer Veröffentlichung nicht verändert oder beschädigt wurde. Wenn Sie die Tarball-Datei nicht überprüfen möchten, überspringen Sie diesen Schritt.

   > **Note**
   >
   > Falls Sie es vorziehen, die Tarball-Datei stattdessen mit einer Prüfsumme oder zu verifizieren, finden Sie weitere Informationen unter. MD5 SHA256 Überprüfen des EFA-Installationsprogramms mithilfe einer Prüfsumme

   a. Laden Sie den öffentlichen GPG-Schlüssel herunter und importieren Sie ihn in Ihren Schlüsselbund.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
import aws-efa-installer.key
```

Der Befehl sollte einen Schlüsselwert zurückgeben. Notieren Sie sich den Schlüsselwert. Sie benötigen ihn im nächsten Schritt.

b. Überprüfen Sie den Fingerabdruck des GPG-Schlüssels. Führen Sie den folgenden Befehl aus und geben den Schlüsselwert aus dem vorherigen Schritt an.

```
$ gpg --fingerprint key_value
```

Der Befehl sollte einen Fingerabdruck zurückgeben, der mit `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC` identisch ist. Wenn der Fingerabdruck nicht übereinstimmt, führen Sie das EFA-Installationsskript nicht aus und wenden Sie sich an den Support.

c. Laden Sie die Signaturdatei herunter und überprüfen Sie die Signatur der EFA-Tarball-Datei.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.45.1.tar.gz.sig
 && gpg --verify ./aws-efa-installer-1.45.1.tar.gz.sig
```

Das folgende Beispiel zeigt eine Ausgabe.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Wenn das Ergebnis `Good signature` enthält und der Fingerabdruck mit dem Fingerabdruck übereinstimmt, der im vorherigen Schritt zurückgegeben wurde, fahren Sie mit dem nächsten Schritt fort. Wenn nicht, führen Sie das EFA-Installationsskript nicht aus und wenden Sie sich an den Support.

4. Extrahieren Sie die Daten aus der komprimierten `.tar.gz`-Datei und wechseln Sie in das extrahierte Verzeichnis.

```
$ tar -xf aws-efa-installer-1.45.1.tar.gz && cd aws-efa-installer
```

5. Führen Sie das EFA-Software-Installationsskript aus.

> **Note**
>
> Ab EFA 1.30.0 sind sowohl Open MPI 4.1 als auch Open MPI 5 standardmäßig installiert. Sofern Sie Open MPI 5 nicht benötigen, empfehlen wir, nur Open MPI 4.1 zu installieren. Mit dem folgenden Befehl wird nur Open MPI 4.1 installiert. Wenn Sie Open MPI 4.1 und Open MPI 5 installieren möchten, entfernen Sie es. `--mpi=openmpi4`

```
$ sudo ./efa_installer.sh -y --mpi=openmpi4
```

Libfabric ist im `/opt/amazon/efa`-Verzeichnis installiert. Das aws-ofi-nccl Plugin ist im Verzeichnis installiert. `/opt/amazon/ofi-nccl` Open MPI ist im `/opt/amazon/openmpi`-Verzeichnis installiert.

6. Wenn das EFA-Installationsprogramm Sie auffordert, die Instance neu zu starten, tun Sie dies und stellen Sie dann erneut eine Verbindung mit der Instance her. Melden Sie sich andernfalls von der Instance ab und wieder an, um die Installation abzuschließen.
7. Überprüfen Sie, ob die EFA-Softwarekomponenten erfolgreich installiert wurden.

```
$ fi_info -p efa -t FI_EP_RDM
```

Der Befehl muss Informationen zu den Libfabric-EFA-Schnittstellen zurückgeben. Das folgende Beispiel zeigt die Befehlsausgabe.

- `p3dn.24xlarge` mit einer einzigen Netzwerkschnittstelle

```
provider: efa
fabric: EFA-fe80::94:3dff:fe89:1b70
domain: efa_0-rdm
version: 2.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

- `p4d.24xlarge` und `p5.48xlarge` mit mehreren Netzwerkschnittstellen

```
provider: efa
fabric: EFA-fe80::c6e:8fff:fef6:e7ff
```

```
domain: efa_0-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c34:3eff:feb2:3c35
domain: efa_1-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c0f:7bff:fe68:a775
domain: efa_2-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::ca7:b0ff:fea6:5e99
domain: efa_3-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

Schritt 6: Installieren der NCCL

Installieren Sie die NCCL Weitere Informationen zur NCCL finden Sie im NCCL-Repository.

So installieren Sie die NCCL

1. Navigieren Sie zum Verzeichnis `/opt`.

```
$ cd /opt
```

2. Klonen Sie das offizielle NCCL-Repository in die Instance und navigieren Sie zum lokal geklonten Repository.

```
$ sudo git clone https://github.com/NVIDIA/nccl.git -b v2.23.4-1 && cd nccl
```

3. Erstellen und installieren Sie die NCCL und geben Sie das CUDA-Installationsverzeichnis an.

```
$ sudo make -j src.build CUDA_HOME=/usr/local/cuda
```

Schritt 7: Installieren der NCCL-Tests

Installieren Sie die NCCL-Tests. Mit den NCCL-Tests können Sie bestätigen, dass die NCCL richtig installiert wurde und wie erwartet funktioniert. Weitere Informationen zu den NCCL-Tests finden Sie unter nccl-tests repository.

So installieren Sie die NCCL-Tests

1. Navigieren Sie zum Stammverzeichnis.

```
$ cd $HOME
```

2. Klonen Sie das offizielle nccl-tests-Repository in die Instance und navigieren Sie zum lokal geklonten Repository.

```
$ git clone https://github.com/NVIDIA/nccl-tests.git && cd nccl-tests
```

3. Fügen Sie das libfabric-Verzeichnis in die Variable `LD_LIBRARY_PATH` ein.

   - Amazon Linux 2023 und Amazon Linux 2

```
$ export LD_LIBRARY_PATH=/opt/amazon/efa/lib64:$LD_LIBRARY_PATH
```

   - Ubuntu 24.04 und Ubuntu 22.04

```
$ export LD_LIBRARY_PATH=/opt/amazon/efa/lib:$LD_LIBRARY_PATH
```

4. Installieren Sie die NCCL-Tests und geben Sie die Installationsverzeichnisse für MPI, NCCL und CUDA an.

```
$ make MPI=1 MPI_HOME=/opt/amazon/openmpi NCCL_HOME=/opt/nccl/build CUDA_HOME=/usr/
local/cuda
```

Schritt 8: Testen der EFA- und NCCL-Konfiguration

Führen Sie einen Test durch, um sicherzustellen, dass Ihre temporäre Instance richtig für EFA und NCCL konfiguriert ist.

So testen Sie EFA- und NCCL-Konfiguration

1. Erstellen Sie eine Host-Datei, die die Hosts angibt, auf denen die Tests ausgeführt werden sollen. Der folgende Befehl erstellt eine Host-Datei namens `my-hosts`, die eine Referenz auf die Instance selbst enthält.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
   meta-data/local-ipv4 >> my-hosts
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4 >> my-
   hosts
   ```

2. Führen Sie den Test aus und geben Sie die Host-Datei (`--hostfile`) und die Anzahl der GPUs zu verwendenden Dateien () an. `-n` Der folgende Befehl führt den `all_reduce_perf` Test auf 8 GPUs auf der Instanz selbst aus und gibt die folgenden Umgebungsvariablen an.

   - `FI_EFA_USE_DEVICE_RDMA=1` – (nur `p4d.24xlarge`) verwendet die RDMA-Funktion des Geräts für einseitige und zweiseitige Übertragungen.
   - `NCCL_DEBUG=INFO`: ermöglicht eine detaillierte Debugging-Ausgabe. Sie können auch `VERSION` angeben, damit nur die NCCL-Version am Anfang des Tests ausgegeben wird oder `WARN`, damit nur Fehlermeldungen ausgegeben werden.

   Weitere Informationen zu den Argumenten für NCCL-Tests finden Sie unter NCCL Tests README im offiziellen nccl-tests-Repository.

   - `p3dn.24xlarge`

   ```
   $ /opt/amazon/openmpi/bin/mpirun \
   -x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
   lib:/opt/amazon/openmpi/lib:/opt/amazon/ofi-nccl/lib:$LD_LIBRARY_PATH \
   -x NCCL_DEBUG=INFO \
   --hostfile my-hosts -n 8 -N 8 \
   --mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to
    none \
   ```

```
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

- `p4d.24xlarge` und `p5.48xlarge`

```
$ /opt/amazon/openmpi/bin/mpirun \
-x FI_EFA_USE_DEVICE_RDMA=1 \
-x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib:/opt/amazon/openmpi/lib:/opt/amazon/ofi-nccl/lib:$LD_LIBRARY_PATH \
-x NCCL_DEBUG=INFO \
--hostfile my-hosts -n 8 -N 8 \
--mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to
 none \
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

3. Sie können bestätigen, dass EFA als zugrunde liegender Anbieter für NCCL aktiv ist, wenn das `NCCL_DEBUG`-Protokoll gedruckt wird.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Selected Provider is efa*
```

Die folgenden zusätzlichen Informationen werden angezeigt, wenn Sie eine `p4d.24xlarge`-Instance verwenden.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Running on P4d platform, Setting
 NCCL_TOPO_FILE environment variable to /home/ec2-user/install/plugin/share/aws-
ofi-nccl/xml/p4d-24xl-topo.xml
```

Schritt 9: Installieren der Machine-Learning-Anwendungen

Installieren Sie die Machine-Learning-Anwendungen auf der temporären Instance. Der Installationsvorgang variiert je nach Machine-Learning-Anwendung. Weitere Informationen zum Installieren von Software auf Ihrer Linux-Instance finden Sie unter Verwalten von Software auf einer Amazon-Linux-2-Instance.

> **Note**
>
> In der Dokumentation Ihrer Machine-Learning-Anwendung finden Sie Installationsanleitungen.

Schritt 10: Erstellen eines EFA- und NCCL-konformen AMI

Nachdem Sie die erforderlichen Softwarekomponenten installiert haben, erstellen Sie ein AMI, das Sie erneut verwenden können, um Ihre EFA-fähigen Instances zu starten.

So erstellen Sie ein AMI aus Ihrer temporären Instance:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die temporäre Instance aus, die Sie erstellt haben, und wählen Sie anschließend Actions (Aktionen), Image und Create Image (Image erstellen) aus.
4. Gehen Sie bei Create Image (Image erstellen) wie folgt vor:
   a. Geben Sie unter Image name (Image-Name) einen beschreibenden Namen für das AMI ein.
   b. (Optional:) Geben Sie bei Image description (Image-Beschreibung) eine kurze Beschreibung des Zwecks des AMI ein.
   c. Wählen Sie Create Image (Image erstellen) aus.
5. Wählen Sie im Navigationsbereich AMIs aus.
6. Suchen Sie das AMI, das Sie erstellt haben, in der Liste. Warten Sie, bis der Status von `pending` zu `available` wechselt, bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 11: Beenden der temporären Instance

An diesem Punkt benötigen Sie die temporäre Instance, die Sie gestartet haben, nicht mehr. Sie können die Instance beenden, damit keine weiteren Kosten dafür anfallen.

So beenden Sie die temporäre Instance:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die temporäre instance aus, die Sie erstellt haben, und wählen Sie anschließend Actions (Aktionen), Instance state (Instance-Zustand) und Terminate instance (Instance beenden) aus.
4. Wählen Sie Terminate (Kündigen) aus, wenn Sie zur Bestätigung aufgefordert werden.

Schritt 12: Starten von EFA- und NCCL-konformen Instances in einer Cluster Placement-Gruppe

Starten Sie die EFA- und NCCL-fähigen Instances in einer Cluster-Placement-Gruppe, indem Sie das EFA-fähige AMI und die EFA-fähige Sicherheitsgruppe verwenden, die Sie zuvor erstellt haben.

> **Note**
>
> - Es ist keine absolute Voraussetzung, Ihre EFA-aktivierten Instances in einer Cluster-Platzierungsgruppe zu starten. Wir empfehlen allerdings, Ihre EFA-Instances in einer Cluster-Placement-Gruppe zu starten, da die Instances dadurch in einer Gruppe mit niedriger Latenz in einer einzelnen Availability Zone gestartet werden.
> - Um die Verfügbarkeit von Kapazitäten sicherzustellen, wenn Sie die Instances Ihres Clusters skalieren, können Sie eine Kapazitätsreservierung für Ihre Cluster-Placement-Gruppe erstellen. Weitere Informationen finden Sie unter Kapazitätsreservierungen mit Cluster-Placement-Gruppen verwenden.

New console

So starten Sie eine temporäre Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Instances starten aus, um den Launch Instance Wizard zu öffnen.
3. (Optional) Geben Sie im Bereich Name and tags (Name und Tags) einen Namen für die Instance an, z. B. `EFA-instance`. Der Name wird der Instance als Ressourcen-Tag (`Name=`*`EFA-instance`*) zugewiesen.
4. Wählen Sie im Abschnitt Anwendungs- und Betriebssystemimages die Option My AMIs und dann das AMI aus, das Sie im vorherigen Schritt erstellt haben.
5. Wählen Sie im Bereich Instance type (Instance-Typ) entweder `p3dn.24xlarge` oder `p4d.24xlarge` aus.
6. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das für die Instance verwendet werden soll.
7. Wählen Sie im Bereich Network settings (Netzwerkeinstellungen) Edit (Bearbeiten) aus und führen Sie dann Folgendes aus:

a. Wählen Sie unter Subnetz das Subnetz aus, in dem die Instance gestartet werden soll. Wenn Sie kein Subnetz auswählen, können Sie die Instance nicht für EFA aktivieren.

b. Wählen Sie bei Firewall (security groups) Firewall (Sicherheitsgruppen) Select existing security group (Vorhandene Sicherheitsgruppe auswählen) und dann die Sicherheitsgruppe aus, die Sie im vorherigen Schritt erstellt haben.

c. Erweitern Sie den Abschnitt Erweiterte Netzwerkkonfiguration.

   Wählen Sie für Netzwerkschnittstelle 1 Netzwerkkartenindex = 0, Geräteindex = 0 und Schnittstellentyp = EFA mit ENA aus.

   (Optional) Wenn Sie einen Instance-Typ mit mehreren Karten verwenden, z. B. `p4d.24xlarge` oder `p5.48xlarge`, wählen Sie für jede weitere erforderliche Netzwerkschnittstelle die Option Netzwerkschnittstelle hinzufügen, wählen Sie für Netzwerkkartenindex den nächsten ungenutzten Index aus und wählen Sie dann Geräteindex = 1 und Schnittstellentyp = EFA mit ENA oder Nur-EFA aus.

8. (Optional) Konfigurieren Sie im Bereich Storage (Speicher) die Volumes nach Bedarf.
9. Wählen Sie im Bereich Advanced details (Erweiterte Details) bei Placement group name (Placement-Gruppen-Name) die Cluster-Placement-Gruppe aus, in der die Instance gestartet werden soll. Wenn Sie eine neue Cluster-Placement-Gruppe erstellen müssen, wählen Sie Create new placement group (Neue Placement-Gruppe erstellen).
10. Geben Sie im Bereich Summary (Zusammenfassung) rechts bei Number of instances (Anzahl der Instances) die Anzahl EFA-fähiger Instances ein, die Sie starten möchten, und wählen Sie dann Launch instance (Instance starten).

Old console

So starten Sie EFA- und NCCL-fähige Instances in einer Cluster-Placement-Gruppe:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Launch Instance aus.
3. Wählen Sie auf der Seite Choose an AMI die Option My aus AMIs, suchen Sie das AMI, das Sie zuvor erstellt haben, und wählen Sie dann Select aus.
4. Wählen Sie auf der Seite Choose an Instance Type (Instance-Typ auswählen) die Option p3dn.24xlarge und dann Next: Configure Instance Details (Weiter: Instance-Details konfigurieren) aus.

5. Führen Sie auf der Seite Configure Instance Details (Instance-Details konfigurieren) die folgenden Schritte aus:

   a. Geben Sie bei Number of instances (Anzahl der Instances) die Anzahl der EFA- und NCCL-fähigen Instances ein, die gestartet werden sollen.

   b. Wählen Sie für Network (Netzwerk) und Subnet (Subnetz) die VPC und das Subnetz an, in das Sie die Instances starten möchten.

   c. Wählen Sie für Placement group (Placement-Gruppe) die Option Add instance to placement group (Instance der Placement-Gruppe hinzufügen) aus.

   d. Wählen Sie bei Placement group name (Name der Placement-Gruppe) die Option Add to a new placement group (Zu neuer Placement-Gruppe hinzufügen) aus und geben Sie dann einen beschreibenden Namen für die Placement-Gruppe ein. Wählen Sie dann bei Placement group strategy (Strategie für Placement-Gruppe) cluster aus.

   e. Wählen Sie für EFA Enable (Aktivieren) aus.

   f. Wählen Sie im Abschnitt Network Interfaces (Netzwerkschnittstellen für das Gerät eth0 die Option New network interface (Neue Netzwerkschnittstelle) aus. Sie können optional eine primäre IPv4 Adresse und eine oder mehrere sekundäre IPv4 Adressen angeben. Wenn Sie die Instance in einem Subnetz starten, dem ein IPv6 CIDR-Block zugeordnet ist, können Sie optional eine primäre IPv6 Adresse und eine oder mehrere sekundäre IPv6 Adressen angeben.

   g. Wählen Sie Next: Add Storage aus.

6. Geben Sie auf der Seite Add Storage (Speicher hinzufügen) die Volumes an, die an die Instances angefügt werden sollen, ergänzend zu den Volumes, die vom AMI angegeben werden (z. B. der Root-Gerät-Volume). Wählen Sie dann Next: Add Tags (Weiter: Tags (Markierungen) hinzufügen) aus.

7. Geben Sie auf der Seite Add Tags (Tags (Markierungen) hinzufügen) Tags (Markierungen) für die Instances an, z. B. einen benutzerfreundlichen Namen, und wählen Sie anschließend Next: Configure Security Group (Weiter: Sicherheitsgruppe konfigurieren).

8. Wählen Sie auf der Seite Configure Security Group (Sicherheitsgruppe konfigurieren) bei Assign a security group (Sicherheitsgruppe zuweisen) die Option Select an existing security group (Vorhandene Sicherheitsgruppe auswählen) und dann die Sicherheitsgruppe aus, die Sie zuvor erstellt haben.

9. Klicken Sie auf Review and Launch.

10. Überprüfen Sie auf der Seite Review Instance Launch (Instance-Start überprüfen) Ihre Einstellungen und wählen Sie anschließend Launch (Starten) aus, um ein Schlüsselpaar auszuwählen und Ihre Instance zu starten.

Schritt 13: Aktivieren von passwortlosem SSH

Damit Ihre Anwendungen auf allen Instances in Ihrem Cluster ausgeführt werden können, müssen Sie passwortlosen SSH-Zugriff vom Führungsknoten auf die Mitgliedsknoten aktivieren. Der Führungsknoten ist die Instance, von der aus Sie die Anwendungen ausführen. Die verbleibenden Instances im Cluster sind die Mitgliedsknoten.

So aktivieren Sie passwortloses SSH zwischen den Instances im Cluster:

1. Wählen Sie eine Instance im Cluster als Führungsknoten aus und stellen Sie eine Verbindung zu ihr her.
2. Deaktivieren Sie `strictHostKeyChecking` und aktivieren Sie `ForwardAgent` für den Führungsknoten. Öffnen Sie `~/.ssh/config` mit dem bevorzugten Texteditor und fügen Sie Folgendes hinzu.

   ```
   Host *
       ForwardAgent yes
   Host *
       StrictHostKeyChecking no
   ```

3. Generieren Sie ein RSA-Schlüsselpaar.

   ```
   $ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
   ```

   Das Schlüsselpaar wird im `$HOME/.ssh/`-Verzeichnis erstellt.
4. Ändern Sie die Berechtigungen des privaten Schlüssels auf dem Führungsknoten.

   ```
   $ chmod 600 ~/.ssh/id_rsa
   chmod 600 ~/.ssh/config
   ```

5. Öffnen Sie `~/.ssh/id_rsa.pub` mit Ihrem bevorzugten Texteditor und kopieren Sie den Schlüssel.
6. Gehen Sie für jeden Mitgliedsknoten im Cluster wie folgt vor:

a. Stellen Sie eine Verbindung mit der Instance her.

b. Öffnen Sie `~/.ssh/authorized_keys` mit Ihrem bevorzugten Texteditor und fügen Sie den öffentlichen Schlüssel hinzu, den Sie zuvor kopiert haben.

7. Um zu testen, ob das passwortlose SSH wie erwartet funktioniert, stellen Sie eine Verbindung zum Leaderknoten her und führen Sie den folgenden Befehl aus.

```
$ ssh member_node_private_ip
```

Sie sollten eine Verbindung zum Mitgliedsknoten herstellen können, ohne zur Eingabe eines Schlüssels oder Passworts aufgefordert zu werden.

Maximieren Sie die Netzwerkbandbreite auf EC2 Amazon-Instances mit mehreren Netzwerkkarten

Viele Instance-Typen, die EFA unterstützen, verfügen auch über mehrere Netzwerkkarten. Weitere Informationen finden Sie unter Netzwerkkarten. Wenn Sie EFA mit einem dieser Instance-Typen verwenden möchten, empfehlen wir die folgende Grundkonfiguration:

- Erstellen Sie für die primäre Netzwerkschnittstelle (Netzwerkkartenindex `0`, Geräteindex `0`) eine EFA-Schnittstelle (EFA mit ENA). Sie können eine Nur-EFA-Netzwerkschnittstelle nicht als primäre Netzwerkschnittstelle verwenden.
- Verwenden Sie für jede weitere Netzwerkschnittstelle den nächsten ungenutzten Netzwerkkartenindex, Geräteindex 1 und entweder eine EFA (EFA mit ENA) oder eine Nur-EFA-Netzwerkschnittstelle, je nach Anwendungsfall, z. B. ENA-Bandbreitenanforderungen oder IP-Adressraum. Anwendungs-Fallbeispiele finden Sie unter EFA-Konfiguration für P5- und P5e-Instances.

> **Note**
>
> P5-Instances erfordern, dass Netzwerkschnittstellen auf eine bestimmte Weise konfiguriert werden, um eine maximale Netzwerkbandbreite zu ermöglichen. Weitere Informationen finden Sie unter EFA-Konfiguration für P5- und P5e-Instances.

Die folgenden Beispiele zeigen, wie eine Instance auf der Grundlage dieser Empfehlungen gestartet wird.

Instance launch

Um dies EFAs während des Instance-Starts mithilfe des Launch-Instance-Assistenten festzulegen

1. Wählen Sie im Abschnitt Netzwerkeinstellungen die Option Bearbeiten aus.
2. Erweiterte Netzwerkkonfiguration erweitert
3. Wählen Sie für die primäre Netzwerkschnittstelle (Netzwerkschnittstelle 1) Netzwerkkartenindex = 0, Geräteindex = 0 und Schnittstellentyp = EFA mit ENA aus.
4. Wählen Sie für jede weitere erforderliche Netzwerkschnittstelle die Option Netzwerkschnittstelle hinzufügen aus. Wählen Sie für Netzwerkkartenindex den nächsten ungenutzten Index aus und wählen Sie dann Geräteindex = 1 und Schnittstellentyp = EFA mit ENA oder Nur-EFA aus.

Um dies EFAs beim Start der Instanz mit dem Befehl run-instances anzugeben

Geben Sie für `--network-interfaces` die erforderliche Anzahl von Netzwerkschnittstellen an. Geben Sie für die primäre Netzwerkschnittstelle `NetworkCardIndex=0`, `DeviceIndex=0` und `InterfaceType=efa` an. Geben Sie für alle weiteren Netzwerkschnittstellen für `NetworkCardIndex` den nächsten unbenutzten Index, `DeviceIndex=1`, `InterfaceType=efa` oder `efa-only` an.

Der folgende Ausschnitt eines Beispielbefehls zeigt eine Anfrage mit 32 EFA-Netzwerkschnittstellen und einem ENA-Gerät.

```
$ aws ec2 run-instances \
 --instance-type p5.48xlarge \
 --count 1 \
 --key-name key_pair_name \
 --image-id ami-0abcdef1234567890 \
 --network-interfaces
 "NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 \
"NetworkCardIndex=1,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
"NetworkCardIndex=2,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
```

```
"NetworkCardIndex=3,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
"NetworkCardIndex=4,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
"NetworkCardIndex=5,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
"NetworkCardIndex=6,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
"NetworkCardIndex=7,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
"NetworkCardIndex=8,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
"NetworkCardIndex=9,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=
 or efa-only" \
"NetworkCardIndex=10,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=11,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=12,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=13,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=14,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=15,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=16,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=17,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=18,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=19,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=20,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=21,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=22,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=23,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=24,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
```

```
"NetworkCardIndex=25,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=26,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=27,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=28,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=29,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=30,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only" \
"NetworkCardIndex=31,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType
 or efa-only"
...
```

Launch templates

So fügen Sie EFAs es mithilfe der EC2 Amazon-Konsole zu einer Startvorlage hinzu

1. Erweitern Sie unter Netzwerkeinstellungen Erweiterte Netzwerkkonfiguration.
2. Wählen Sie für die primäre Netzwerkschnittstelle (Netzwerkschnittstelle 1) Netzwerkschnittstelle hinzufügen und dann Netzwerkkartenindex = 0, Geräteindex = 0 und Schnittstellentyp = EFA mit ENA aus.
3. Wählen Sie Netzwerkschnittstelle hinzufügen aus, um weitere Netzwerkschnittstellen hinzuzufügen. Wählen Sie für Netzwerkkartenindex den nächsten ungenutzten Index aus und wählen Sie dann Geräteindex = 1 und Schnittstellentyp = EFA mit ENA oder Nur-EFA aus.

Um sie mit dem create-launch-templateBefehl EFAs zu einer Startvorlage hinzuzufügen

Geben Sie für `NetworkInterfaces` die erforderliche Anzahl von Netzwerkschnittstellen an. Geben Sie für die primäre Netzwerkschnittstelle `NetworkCardIndex=0`, `DeviceIndex=0` und `InterfaceType=efa` an. Geben Sie für alle weiteren Netzwerkschnittstellen für `NetworkCardIndex` den nächsten unbenutzten Index, `DeviceIndex=1`, `InterfaceType=efa` oder `efa-only` an.

Der folgende Ausschnitt zeigt ein Beispiel mit 3 Netzwerkschnittstellen (von möglichen 32 Netzwerkschnittstellen).

```
"NetworkInterfaces":[
```

```
{
  "NetworkCardIndex":0,
  "DeviceIndex":0,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 1,
  "DeviceIndex": 1,
  "InterfaceType": "efa or efa-only",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 2,
  "DeviceIndex": 1,
  "InterfaceType": "efa or efa-only",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 3,
  "DeviceIndex": 1,
  "InterfaceType": "efa or efa-only",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
}
...
```

EFA-Konfiguration für P5- und P5e-Instances

`p5.48xlarge`- und `p5e.48xlarge`-Instances unterstützen 32 Netzwerkkarten und haben eine gesamte Netzwerkbandbreitenkapazität von 3 200 Gbit/s, wovon bis zu 800 Gbit/s für IP-Netzwerkdatenverkehr genutzt werden können. Da EFA- und IP-Netzwerkverkehr dieselben zugrunde liegenden Ressourcen gemeinsam nutzen, reduziert die Bandbreite, die von der einen verwendet wird, die Bandbreite, die der anderen zur Verfügung steht. Das bedeutet, dass Sie die Netzwerkbandbreite in beliebiger Kombination zwischen EFA-Verkehr und IP-Verkehr verteilen können, sofern die Gesamtbandbreite 3 200 Gbit/s und die IP-Bandbreite 800 Gbit/s nicht überschreitet. Wenn Sie beispielsweise 400 Gbit/s für die IP-Bandbreite verwenden, können Sie bis zu 2 800 Gbit/s EFA-Bandbreite gleichzeitig erreichen.

Anwendungsfall 1: IP-Adressen speichern und potenzielle Linux-IP-Probleme vermeiden

Diese Konfiguration bietet bis zu 3 200 Gbit/s EFA-Netzwerkbandbreite und bis zu 100 Gbit/s IP-Netzwerkbandbreite mit einer privaten IP-Adresse. Diese Konfiguration trägt auch dazu bei, potenzielle Linux-IP-Probleme zu vermeiden, wie z. B. die unzulässige automatische Zuweisung öffentlicher IP-Adressen und IP-Routing-Herausforderungen (Probleme bei der Zuordnung von Host-Namen zu IP-Adressen und Nichtübereinstimmungen der Quell-IP-Adressen), die auftreten können, wenn eine Instance über mehrere Netzwerkschnittstellen verfügt.

- Erstellen Sie für die primäre Netzwerkschnittstelle (Netzwerkkartenindex 0, Geräteindex 0) eine EFA-Netzwerkschnittstelle (EFA mit ENA).
- Verwenden Sie für die übrigen Netzwerkschnittstellen (Netzwerkkartenindizes 1–31, Geräteindex 1) Nur-EFA-Netzwerkschnittstellen.

Anwendungsfall 2: Maximale EFA- und IP-Netzwerkbandbreite

Diese Konfiguration bietet bis zu 3 200 Gbit/s EFA-Netzwerkbandbreite und bis zu 800 Gbit/s IP-Netzwerkbandbreite mit 8 privaten IP-Adressen. Mit dieser Konfiguration können Sie öffentliche IP-Adressen nicht automatisch zuweisen. Sie können jedoch nach dem Start eine elastische IP-Adresse an die primäre Netzwerkschnittstelle anhängen (Netzwerkkartenindex=0, Geräteindex=0), um eine Internetverbindung herzustellen.

- Erstellen Sie für die primäre Netzwerkschnittstelle (Netzwerkkartenindex 0, Geräteindex 0) eine EFA-Netzwerkschnittstelle (EFA mit ENA).
- Führen Sie für die verbleibenden Schnittstellen die folgenden Schritte aus:

- Geben Sie Nur-EFA-Netzwerkschnittstellen für die Netzwerkkartenindizes 1, 2 und 3 an und verwenden Sie den Geräteindex 1.
- Geben Sie eine EFA-Netzwerkschnittstelle (EFA mit ENA) und drei reine EFA-Netzwerkschnittstellen in jeder der folgenden Netzwerkkarten-Index-Untergruppen an und verwenden Sie für alle den Geräteindex 1:
  - [4,5,6,7]
  - [8,9,10,11]
  - [12,13,14,15]
  - [16,17,18,19]
  - [20,21,22,23]
  - [24,25,26,27]
  - [28,29,30,31]

Das folgende Beispiel veranschaulicht diese Konfiguration:

```
$ aws --region $REGION ec2 run-instances \
 --instance-type p5.48xlarge \
 --count 1 \
 --key-name key_pair_name \
 --image-id ami_id \
 --network-interfaces
 "NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \
"NetworkCardIndex=1,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=2,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=3,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=4,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
 \
"NetworkCardIndex=5,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=6,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=7,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
```

```
"NetworkCardIndex=8,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
 \
"NetworkCardIndex=9,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=10,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=11,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=12,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \
"NetworkCardIndex=13,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=14,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=15,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=16,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \
"NetworkCardIndex=17,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=18,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=19,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=20,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \
"NetworkCardIndex=21,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=22,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=23,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=24,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \
"NetworkCardIndex=25,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=26,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=27,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=28,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \
"NetworkCardIndex=29,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
```

```
"NetworkCardIndex=30,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=31,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only"
...
```

EFA-Konfiguration für P6-B200-Instances

P6-B200-Instances haben eine gesamte Netzwerkbandbreitenkapazität von 3 200 Gbit/s, wovon bis zu 1 600 Gbit/s für ENA genutzt werden können. Sie verfügen über 8 GPUs und 8 Netzwerkkarten, wobei jede Netzwerkkarte bis zu 400 Gbit/s EFA-Bandbreite und 200 Gbit/s ENA-Bandbreite unterstützt. Da EFA- und ENA-Netzwerkverkehr dieselben zugrunde liegenden Ressourcen gemeinsam nutzen, reduziert die Bandbreite, die von der einen verwendet wird, die Bandbreite, die der anderen zur Verfügung steht.

Anwendungsfall 1: IP-Adressen speichern

Diese Konfiguration verbraucht mindestens eine private IP-Adresse pro Instance und unterstützt bis zu 3 200 Gbit/s EFA-Bandbreite und 200 Gbit/s ENA-Bandbreite.

- Erstellen Sie für die primäre Netzwerkschnittstelle (Netzwerkkartenindex 0, Geräteindex 0) eine EFA-Netzwerkschnittstelle (EFA mit ENA).
- Verwenden Sie für die übrigen 7 Netzwerkkarten (Netzwerkkartenindizes 1–7, Geräteindex 1) Nur-EFA-Netzwerkschnittstellen.

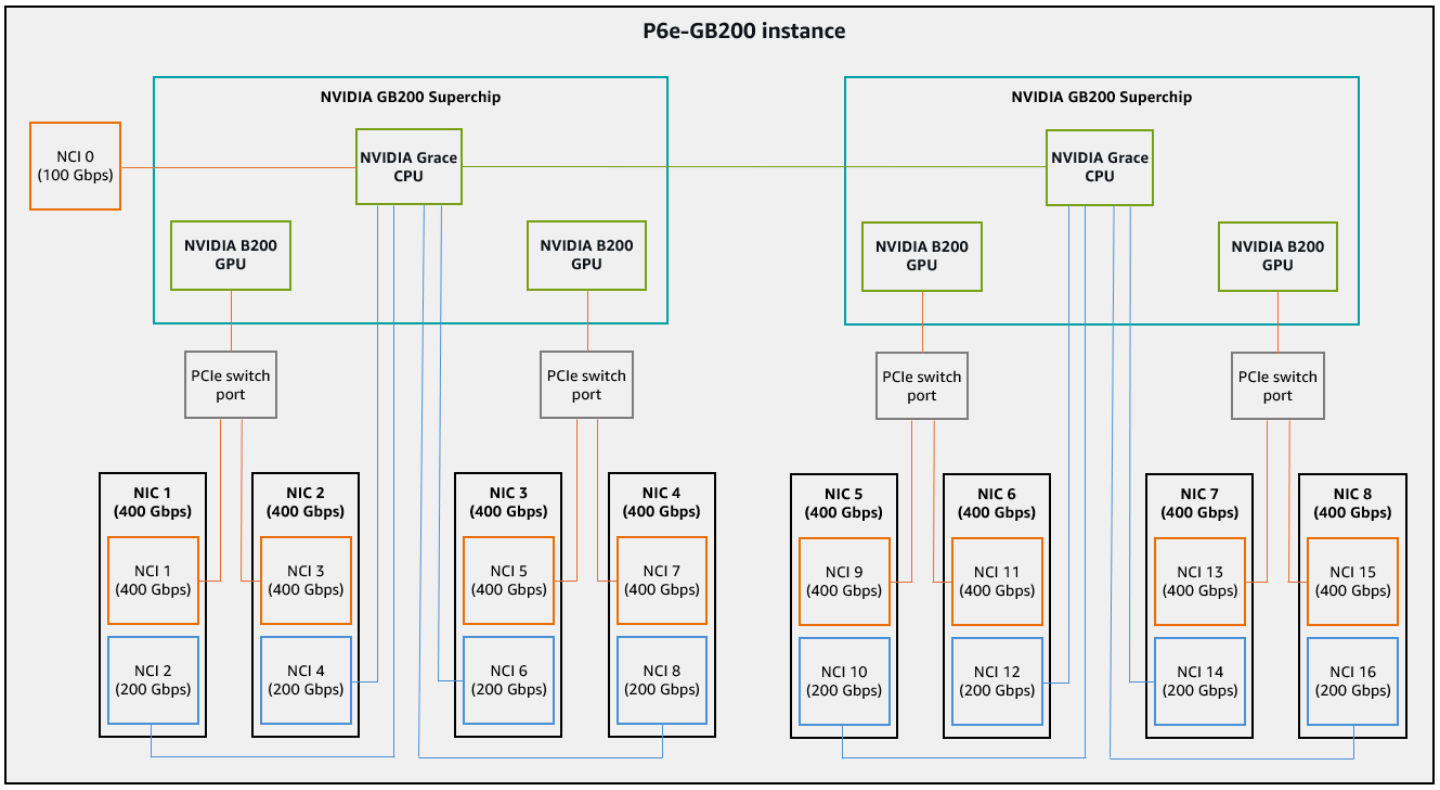
Anwendungsfall 2: Maximale EFA- und ENA-Bandbreite

Diese Konfiguration verbraucht mindestens 8 private IP-Adressen pro Instance und unterstützt bis zu 3 200 Gbit/s EFA-Bandbreite und 1600 Gbit/s ENA-Bandbreite.

- Verwenden Sie EFA-Netzwerkschnittstellen (EFA mit ENA) für die primäre Netzwerkschnittstelle (Netzwerkkartenindex 0, Geräteindex 0) und die anderen 7 Netzwerkkarten (Netzwerkkartenindizes 1–7, Geräteindex 1).

EFA-Konfiguration für P6e-00-Instances GB2

P6e- GB2 00-Instances können mit bis zu 17 Netzwerkkarten konfiguriert werden. Die folgende Abbildung zeigt das Layout der physischen Netzwerkschnittstellenkarte (NIC) für GB2 P6e-00-Instances zusammen mit der Zuordnung der Netzwerkkartenindizes (). NCIs



Das primäre NCI (Index 0) unterstützt bis zu 100 Gbit/s ENA-Bandbreite. NCIs mit den folgenden Indizes werden ausschließlich EFA-Netzwerkschnittstellen und eine EFA-Bandbreite von 400 Gbit/s unterstützt: [1, 3, 5, 7, 9, 11, 13, 15]. NCIs mit den folgenden Indizes werden bis zu 200 Gbit/s ENA- oder EFA-Bandbreite unterstützt: [2, 4, 6, 8, 10, 12, 14, 16].

Die folgenden Gruppen teilen NCIs sich eine zugrunde liegende physische Netzwerkkarte auf dem Host:

- [1 und 2]
- [3 und 4]
- [5 und 6]
- [7 und 8]
- [9 und 10]
- [11 und 12]
- [13 und 14]
- [15 und 16]

Jede physische NIC unterstützt eine Bandbreite von bis zu 400 Gbit/s. Da NCIs sich die Gruppen dieselbe zugrunde liegende physische Netzwerkkarte teilen, reduziert die von einer Gruppe verwendete Bandbreite die Bandbreite, die der anderen zur Verfügung steht. Wenn beispielsweise NIC 2 200 Gbit/s ENA-Bandbreite verwendet, kann NCI 1 gleichzeitig bis zu 200 Gbit/s EFA-Bandbreite verwenden.

Jede zugrunde liegende GPU auf dem Host kann Datenverkehr direkt über die folgenden Paare sendenNCIs:

- [1 und 3]
- [5 und 7]
- [9 und 11]
- [13 und 15]

Jede GPU unterstützt bis zu 400 Gbit/s EFA-Bandbreite. Da die Netzwerkkarten in diesen Gruppen dieselbe GPU gemeinsam nutzen, reduziert die Bandbreite, die von der einen verwendet wird, die Bandbreite, die der anderen zur Verfügung steht- Wenn beispielsweise NIC 1 200 Gbit/s EFA-Bandbreite verwendet, kann NCI 3 gleichzeitig bis zu 200 Gbit/s EFA-Bandbreite verwenden. Um eine maximale EFA-Leistung zu erzielen, empfehlen wir Ihnen daher, einen der folgenden Schritte durchzuführen, um eine EFA-Bandbreite von insgesamt 1 600 Gbit/s zu erreichen:

- Fügen Sie nur einer NCI in jeder Gruppe eine reine EFA-Netzwerkschnittstelle hinzu, um 400 Gbit/s pro Netzwerkschnittstelle zu erreichen (4 EFA-Netzwerkschnittstellen x 400 Gbit/s).
- Fügen Sie jeder NCI in jeder Gruppe eine reine EFA-Netzwerkschnittstelle hinzu, um 200 Gbit/s pro Netzwerkschnittstelle zu erreichen (8 EFA-Netzwerkschnittstellen x 200 Gbit/s).

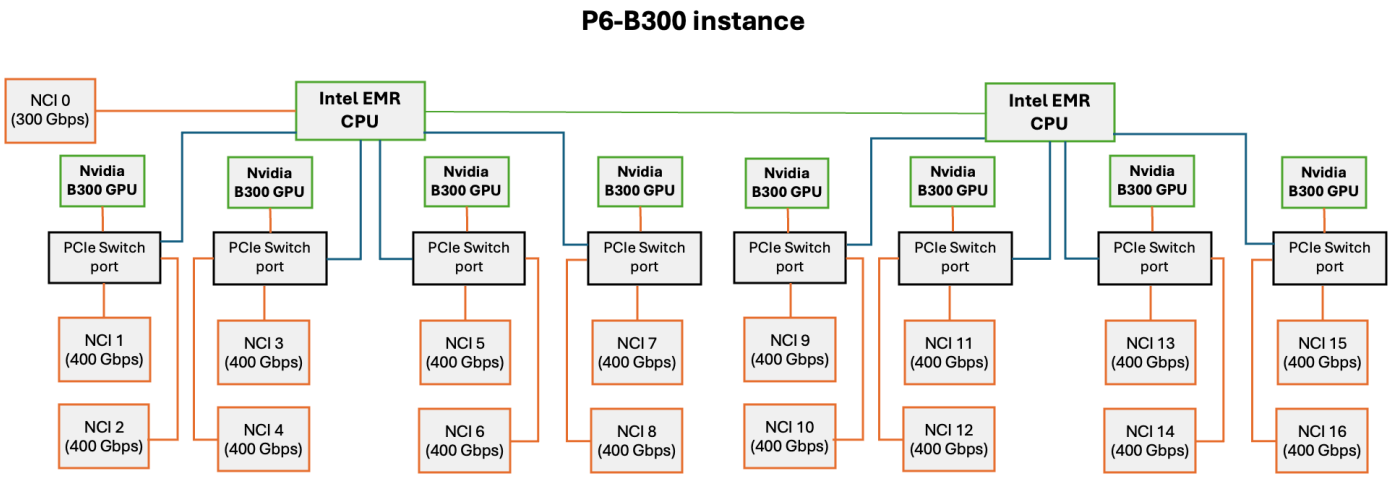
Die folgende Konfiguration bietet beispielsweise bis zu 1 600 Gbit/s EFA-Bandbreite mit einer einzigen reinen EFA-Netzwerkschnittstelle in jeder NCI-Gruppe und bis zu 100 Gbit/s ENA-Netzwerkbandbreite, wenn nur die primäre NCI verwendet wird (Index 0).

- Verwenden Sie für die primäre NCI (Netzwerkkartenindex 0, Geräteindex 0) eine EFA-Netzwerkschnittstelle.
- Fügen Sie den Folgenden eine reine EFA-Netzwerkschnittstellen hinzu:
  - NCI 1, Geräteindex 0
  - NCI 5, Geräteindex 0
  - NCI 9, Geräteindex 0

- NCI 13, Geräteindex 0

EFA-Konfiguration für P6-B300-Instanzen

P6-B300-Instances haben eine gesamte Netzwerkbandbreitenkapazität von bis zu 6400 Gbit/s für EFA-Verkehr und bis zu 3870 Gbit/s für ENA-Verkehr. Sie verfügen über 8 GPUs und 17 Netzwerkkarten, wobei die primäre Netzwerkkarte nur eine ENA-Netzwerkschnittstelle mit bis zu 350 Gbit/s Bandbreite unterstützt. Die sekundären Netzwerkkarten unterstützen bis zu 400 Gbit/s EFA und bis zu 220 Gbit/s ENA-Bandbreite. Da EFA- und ENA-Netzwerkverkehr dieselben zugrunde liegenden Ressourcen gemeinsam nutzen, reduziert die Bandbreite, die von der einen verwendet wird, die Bandbreite, die der anderen zur Verfügung steht.



Anwendungsfall 1: IP-Adressen speichern

Diese Konfiguration verbraucht mindestens eine private IP-Adresse pro Instanz und unterstützt bis zu 6400 Gbit/s EFA-Bandbreite und bis zu 350 Gbit/s ENA-Bandbreite.

- Verwenden Sie für die primäre Netzwerkschnittstelle (Netzwerkkartenindex 0, Geräteindex 0) eine ENA-Netzwerkschnittstelle.
- Verwenden Sie für die übrigen Netzwerkkarten (Netzwerkkartenindizes 1—16, Geräteindex 1) ausschließlich EFA-Netzwerkschnittstellen.

```
--network-interfaces \
"NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
```

```
"NetworkCardIndex=1,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=2,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=3,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=4,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=5,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=6,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=7,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=8,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=9,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=10,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=11,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=12,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=13,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=14,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=15,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=16,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only
```

Anwendungsfall 2: Maximale EFA- und ENA-Bandbreite

Diese Konfiguration verbraucht mindestens 17 private IP-Adressen pro Instanz und unterstützt bis zu 6400 Gbit/s EFA-Bandbreite und bis zu 3870 Gbit/s ENA-Bandbreite.

- Verwenden Sie für die primäre Netzwerkschnittstelle (Netzwerkkartenindex 0, Geräteindex 0) eine ENA-Netzwerkschnittstelle.
- Erstellen Sie für die übrigen Netzwerkkarten eine reine EFA-Schnittstelle (Netzwerkkartenindizes 1—16, Geräteindex 1) und eine ENA-Schnittstelle (Netzwerkkartenindizes 1—16, Geräteindex 2).

```
--network-interfaces \
"NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=int
 \
"NetworkCardIndex=1,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=2,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=3,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=4,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=5,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=6,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=7,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=8,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=9,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=efa
only" \
"NetworkCardIndex=10,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=11,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=12,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=13,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=14,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=15,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=16,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
only" \
"NetworkCardIndex=1,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
"NetworkCardIndex=2,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
"NetworkCardIndex=3,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
"NetworkCardIndex=4,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
```

```
"NetworkCardIndex=5,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
"NetworkCardIndex=6,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
"NetworkCardIndex=7,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
"NetworkCardIndex=8,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
"NetworkCardIndex=9,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ena
 \
"NetworkCardIndex=10,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=en
 \
"NetworkCardIndex=11,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=en
 \
"NetworkCardIndex=12,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=en
 \
"NetworkCardIndex=13,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=en
 \
"NetworkCardIndex=14,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=en
 \
"NetworkCardIndex=15,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=en
 \
"NetworkCardIndex=16,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=en
```

Einen Elastic Fabric-Adapter erstellen und an eine EC2 Amazon-Instance anhängen

Sie können eine EFA erstellen und sie an eine EC2 Amazon-Instance anhängen, genau wie jede andere elastic network interface in Amazon EC2. Im Gegensatz zu elastischen Netzwerkschnittstellen EFAs können sie jedoch nicht an eine Instance in einem bestimmten `running` Bundesstaat angehängt oder von dieser getrennt werden.

Überlegungen

- Sie können die Sicherheitsgruppe ändern, die einem EFA zugeordnet ist. Zum Aktivieren der Funktion der Betriebssystemumgehung muss das EFA zu einer Sicherheitsgruppe gehören, die allen eingehenden und ausgehenden Datenverkehr von und zu der Sicherheitsgruppe selbst zulässt. Weitere Informationen finden Sie unter Schritt 1: Vorbereiten einer EFA-aktivierten Sicherheitsgruppe.

Sie können die Sicherheitsgruppe, die einem EFA zugewiesen ist, auf gleiche Weise ändern, wie Sie die Sicherheitsgruppe ändern, die einer Elastic Network Interface zugewiesen ist. Weitere Informationen finden Sie unter the section called “Ändern der Netzwerkschnittstellen-Attribute”.

- Sie weisen einer EFA-Netzwerkschnittstelle (EFA mit ENAIPv4) eine Elastic IP () und eine IPv6 Adresse auf die gleiche Weise zu, wie Sie einer elastic network interface eine IP-Adresse zuweisen. Weitere Informationen finden Sie unter Verwalten von IP-Adressen.

  Sie können einer Nur-EFA-Netzwerkschnittstelle keine IP-Adresse zuweisen.

Aufgaben

- Erstellen eines EFA
- Anfügen eines EFA an eine gestoppte Instance
- Anfügen einer EFA beim Starten einer Instance
- Hinzufügen eines EFA zu einer Startvorlage

Erstellen eines EFA

Sie können ein EFA in einem Subnetz in einer VPC erstellen. Sie können das EFA nach der Erstellung nicht in ein anderes Subnetz verschieben und Sie können es nur an Instances in der gleichen Availability Zone anfügen.

Console

So erstellen Sie eine EFA-Netzwerkschnittstelle (EFA mit ENA oder nur ENA)

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Network Interfaces (Netzwerkschnittstellen) und wählen Sie dann Netzwerkschnittstelle erstellen aus.
3. Geben Sie unter Description (Beschreibung) einen aussagekräftigen Namen für das EFA ein.
4. Wählen Sie für Subnet (Subnetz) das Subnetz aus, in das Sie das EFA erstellen möchten.
5. Wählen Sie für Schnittstellentyp eine der folgenden Optionen:

   - EFA mit ENA – Um eine Netzwerkschnittstelle zu erstellen, die sowohl ENA- als auch EFA-Geräte unterstützt.
   - Nur EFA – Um eine Netzwerkschnittstelle nur mit einem EFA-Gerät zu erstellen.

6. (Nur für EFA mit ENA) Konfigurieren Sie die IP-Adresse und die Präfixzuweisung für die Netzwerkschnittstelle. Die Art der IP-Adressen und Präfixe, die Sie zuweisen können, hängt vom ausgewählten Subnetz ab. Für IPv4 reine Subnetze können Sie nur IPv4 IP-Adressen und Präfixe zuweisen. Für Subnetze, die IPv6 nur den Status „-Status“ haben, können Sie nur IPv6 IP-Adressen und Präfixe zuweisen. Dual-Stack-Subnetzen können Sie sowohl IP-Adressen als auch Präfixe IPv4 zuweisen. IPv6

   > **Note**
   >
   > Sie können einer reinen EFA-Netzwerkschnittstelle keine IP-Adressen zuweisen.

   a. Wählen Sie für Private IPv4 and/or IPv6 Adressadresse die Option Automatisch zuweisen, damit Amazon EC2 automatisch eine IP-Adresse aus dem ausgewählten Subnetz zuweist, oder wählen Sie Benutzerdefiniert, um die zuzuweisende IP-Adresse manuell anzugeben.

   b. Wenn Sie eine IPv6 Adresse zuweisen, können Sie optional die Option Primäre IPv6 IP zuweisen aktivieren. Dadurch wird der Netzwerkschnittstelle eine primäre IPv6 globale Unicast-Adresse (GUA) zugewiesen. Durch die Zuweisung einer primären IPv6 Adresse können Sie verhindern, dass der Datenverkehr zu den Instances oder unterbrochen wird. ENIs Weitere Informationen finden Sie unter IPv6 Adressen.

   c. Wählen Sie für IPv4 die and/or IPv6 Präfix-Delegierung der Präfix-Delegierung Automatisch zuweisen, damit Amazon EC2 automatisch ein Präfix aus dem CIDR-Block des Subnetzes zuweist, oder wählen Sie Benutzerdefiniert, um manuell ein Präfix aus dem CIDR-Block des Subnetzes anzugeben. Wenn Sie ein Präfix angeben, wird AWS überprüft, ob es nicht bereits einer anderen Ressource zugewiesen ist. Weitere Informationen finden Sie unter Präfix-Delegierung von Amazon-EC2-Netzwerkschnittstellen.

   d. (Optional) Konfigurieren Sie die Timeout-Einstellungen für die Nachverfolgung von Verbindungen im Leerlauf. Weitere Informationen finden Sie unter Timeout für die Nachverfolgung von Leerlaufverbindungen.

      - Timeout für bestehende TCP-Verbindungen – Die Timeout-Zeit in Sekunden für bestehende TCP-Verbindungen im Leerlauf. Min: 60 Sekunden. Max: 432 000 Sekunden (fünf Tage). Standard: 432 000 Sekunden. Empfohlen: Weniger als 432 000 Sekunden.

- UDP-Timeout –Die Timeout-Zeit in Sekunden für UDP-Datenflüsse im Leerlauf, bei denen Datenverkehr nur in eine Richtung oder nur in einer einzelnen Anforderung-Antwort-Transaktion übermittelt wurde. Min: 30 Sekunden. Max: 60 Sekunden. Standard: 30 Sekunden.
- UDP-Stream-Timeout – Die Timeout-Zeit in Sekunden für UDP-Datenflüsse im Leerlauf, die als Streams klassifiziert sind, bei denen mehr als eine Anforderung-Antwort-Transaktion stattgefunden hat. Min: 60 Sekunden. Max: 180 Sekunden (3 Minuten) Standard: 180 Sekunden.

7. Wählen Sie unter Security groups (Sicherheitsgruppen) eine oder mehrere Sicherheitsgruppen aus.
8. Klicken Sie auf Create network interface (Netzwerkschnittstellen erstellen).

AWS CLI

So erstellen Sie ein EFA

Verwenden Sie den Befehl create-network-interface. Geben Sie für `--interface-type` entweder `efa` für eine EFA-Netzwerkschnittstelle oder `efa-only` für eine reine EFA-Netzwerkschnittstelle an.

```
aws ec2 create-network-interface \
    --subnet-id subnet-0abcdef1234567890 \
    --interface-type efa \
    --description "my efa"
```

PowerShell

So erstellen Sie ein EFA

Verwenden Sie das cmdlet New-EC2NetworkInterface. Geben Sie für `-InterfaceType` entweder `efa` für eine EFA-Netzwerkschnittstelle oder `efa-only` für eine reine EFA-Netzwerkschnittstelle an.

```
New-EC2NetworkInterface `
    -SubnetId subnet-0abcdef1234567890 `
    -InterfaceType efa `
    -Description "my efa"
```

Anfügen eines EFA an eine gestoppte Instance

Sie können ein EFA an jede unterstützte Instance anfügen, die sich im Zustand `stopped` befindet. Sie können keine EFA an eine Instance anfügen, die sich im Zustand `running` befindet. Weitere Informationen zu den unterstützten Instance-Typen finden Sie unter Unterstützte Instance-Typen.

Sie fügen einen EFA auf gleiche Weise an eine Instance an, wie Sie eine Schnittstelle an eine Instance anfügen. Weitere Informationen finden Sie unter Netzwerkschnittstelle anhängen.

Anfügen einer EFA beim Starten einer Instance

AWS CLI

So fügen Sie beim Starten einer Instance eine vorhandene EFA an

Verwenden den Befehl run-instances mit der Option `--network-interfaces`. Geben Sie für die primäre Netzwerkschnittstelle eine EFA-Netzwerkschnittstelle und `NetworkCardIndex=0` und `DeviceIndex=0` an. Um mehrere EFA-Netzwerkschnittstellen anzuschließen, finden Sie Informationen unter Maximierung der Netzwerkbandbreite.

```
--network-interfaces "NetworkCardIndex=0, \
    DeviceIndex=0, \
    NetworkInterfaceId=eni-1234567890abcdef0, \
    Groups=sg-1234567890abcdef0, \
    SubnetId=subnet-0abcdef1234567890"
```

So fügen Sie beim Starten einer Instance eine neue EFA an

Verwenden den Befehl run-instances mit der Option `--network-interfaces`. Verwenden Sie für die primäre Netzwerkschnittstelle `NetworkCardIndex=0`, `DeviceIndex=0` und `InterfaceType=efa` an. Wenn Sie mehrere EFA-Netzwerkschnittstellen anschließen, finden Sie weitere Informationen unter Maximierung der Netzwerkbandbreite.

```
--network-interfaces "NetworkCardIndex=0, \
    DeviceIndex=0, \
    InterfaceType=efa, \
    Groups=sg-1234567890abcdef0, \
    SubnetId=subnet-0abcdef1234567890"
```

PowerShell

So fügen Sie beim Starten einer Instance eine vorhandene EFA an

Verwenden Sie das New-EC2InstanceCmdlet mit dem Parameter. `-NetworkInterfaces`

```
-NetworkInterface $networkInterface
```

Definieren Sie die Netzwerkschnittstelle wie folgt.

```
$networkInterface = New-Object
 Amazon.EC2.Model.InstanceNetworkInterfaceSpecification
$networkInterface.DeviceIndex = 0
$networkInterface.NetworkInterfaceId = "eni-1234567890abcdef0"
$networkInterface.Groups = @("sg-1234567890abcdef0")
$networkInterface.SubnetId = "subnet-0abcdef1234567890"
```

So fügen Sie beim Starten einer Instance eine neue EFA an

Verwenden Sie das New-EC2InstanceCmdlet mit dem Parameter. `-NetworkInterfaces`

```
-NetworkInterface $networkInterface
```

Definieren Sie die Netzwerkschnittstelle wie folgt.

```
$networkInterface = New-Object
 Amazon.EC2.Model.InstanceNetworkInterfaceSpecification
$networkInterface.DeviceIndex = 0
$networkInterface.InterfaceType = "efa"
$networkInterface.Groups = @("sg-1234567890abcdef0")
$networkInterface.SubnetId = "subnet-0abcdef1234567890"
```

Hinzufügen eines EFA zu einer Startvorlage

Sie können eine Startvorlage erstellen, die die Konfigurationsdaten zum Starten einer EFA-aktivierten Instance enthält. Sie können sowohl EFA- als auch Nur-EFA-Netzwerkschnittstellen in der Startvorlage angeben. Zum Erstellen einer EFA-aktivierten Startvorlage erstellen Sie eine neue Startvorlage und geben einen unterstützten Instance-Typen, Ihr EFA-aktiviertes AMI und eine EFA-aktivierte Sicherheitsgruppe an. Geben Sie für `NetworkInterfaces` die anzuschließenden EFA-Netzwerkschnittstellen an. Verwenden Sie für die primäre Netzwerkschnittstelle `NetworkCardIndex=0`, `DeviceIndex=0` und `InterfaceType=efa` an. Wenn Sie mehrere EFA-Netzwerkschnittstellen anschließen, finden Sie weitere Informationen unter Maximieren Sie die Netzwerkbandbreite auf EC2 Amazon-Instances mit mehreren Netzwerkkarten.

Sie können Startvorlagen verwenden, um EFA-fähige Instances mit anderen AWS Diensten wie oder zu starten. AWS BatchAWS ParallelCluster

Weitere Informationen zum Erstellen von Startvorlagen finden Sie unter Erstellen Sie eine EC2 Amazon-Startvorlage.

Trennen und löschen Sie eine EFA von einer Amazon-Instance EC2

Sie können eine EFA von einer EC2 Amazon-Instance trennen und sie auf die gleiche Weise löschen wie jede andere elastic network interface in Amazon. EC2

Trennen eines EFA

Zum Trennen eines EFA von der Instance müssen Sie zuerst die Instance stoppen. Sie können kein EFA von einer Instance trennen, die sich in einem laufenden Zustand befindet.

Sie trennen ein EFA auf gleiche Weise von einer Instance, wie Sie eine Elastic Network-Schnittstelle von einer Instance trennen. Weitere Informationen finden Sie unter Netzwerkschnittstelle abhängen.

Löschen eines EFA

Zum Löschen eines EFA müssen Sie es zuerst von der Instance trennen. Sie können keinen EFA löschen, während er an eine Instance angefügt ist.

Sie löschen EFAs auf die gleiche Weise wie Elastic Network-Schnittstellen. Weitere Informationen finden Sie unter Löschen einer Netzwerkschnittstelle.

Überwachen Sie einen Elastic Fabric-Adapter bei Amazon EC2

Sie können die folgenden Features zum Überwachen der Leistung Ihrer Elastic Fabric Adapter verwenden.

Themen

- EFA-Treibermetriken für eine Amazon-Instance EC2
- Amazon VPC-Flussprotokolle
- Amazon CloudWatch

EFA-Treibermetriken für eine Amazon-Instance EC2

Der Elastic Fabric Adapter (EFA)-Treiber veröffentlicht mehrere Metriken von den Instances, an die EFA-Schnittstellen angeschlossen sind, in Echtzeit. Sie können diese Metriken verwenden, um Probleme mit der Instance-Leistung zu beheben, die richtige Cluster-Größe für einen Workload auszuwählen, Skalierungsaktivitäten proaktiv zu planen und Anwendungen zu vergleichen, um zu bestimmen, ob sie die auf einer Instance verfügbare EFA-Leistung maximieren.

Themen

- Verfügbare EFA-Treibermetriken
- EFA-Treibermetriken für Ihre Instance abrufen

Verfügbare EFA-Treibermetriken

Die ENA-Treiber publizieren die folgenden Metriken in Echtzeit an die Instance. Dabei geben Sie die Gesamtzahl der Fehler, Verbindungsereignisse und Pakete oder Bytes an, die seit dem Start der Instance oder dem letzten Treiber-Reset von den angehängten EFA-Geräten gesendet, empfangen oder gelöscht wurden.

Metrik	Description	Unterstützte Instance-Typen
`tx_bytes`	Die Anzahl der übertragenen Bytes. Einheit: Bytes	Alle Instance-Typen, die EFA unterstützen
`rx_bytes`	Die Anzahl der empfangenen Bytes. Einheit: Bytes	Alle Instance-Typen, die EFA unterstützen
`tx_pkts`	Die Anzahl der übertragenen Pakete. Einheit: Anzahl	Alle Instance-Typen, die EFA unterstützen
`rx_pkts`	Die Anzahl der empfangenen Pakete. Einheit: Anzahl	Alle Instance-Typen, die EFA unterstützen

Metrik	Description	Unterstützte Instance-Typen
`rx_drops`	Die Anzahl der empfangenen und dann verworfenen Pakete. Einheit: Anzahl	Alle Instance-Typen, die EFA unterstützen
`send_bytes`	Die Anzahl der über Sendevorgänge gesendeten Bytes. Einheit: Bytes	Alle Instance-Typen, die EFA unterstützen
`recv_bytes`	Die Anzahl der von Sendevorgängen empfangenen Bytes. Einheit: Bytes	Alle Instance-Typen, die EFA unterstützen
`send_wrs`	Die Anzahl der über Sendevorgängen gesendeten Pakete. Einheit: Anzahl	Alle Instance-Typen, die EFA unterstützen
`recv_wrs`	Die Anzahl der von Sendevorgängen empfangenen Pakete. Einheit: Anzahl	Alle Instance-Typen, die EFA unterstützen
`rdma_write_wrs`	Die Anzahl der abgeschlossenen RDMA-Schreibvorgänge. Einheit: Anzahl	Alle Instance-Typen, die EFA unterstützen
`rdma_read_wrs`	Die Anzahl der abgeschlossenen RDMA-Schreibvorgänge. Einheit: Anzahl	Alle Instance-Typen, die EFA unterstützen

Metrik	Description	Unterstützte Instance-Typen
`rdma_write_bytes`	Die Anzahl der von anderen Instances mithilfe von RDMA-Schreibvorgängen darauf geschriebenen Bytes. Einheit: Bytes	Alle Instance-Typen, die EFA unterstützen
`rdma_read_bytes`	Die Anzahl der über RDMA-Lesevorgänge empfangenen Bytes. Einheit: Bytes	Alle Instance-Typen, die EFA unterstützen
`rdma_write_wr_err`	Die Anzahl der RDMA-Schreibvorgänge, bei denen lokale oder externe Fehler aufgetreten sind. Einheit: Anzahl	Alle Instance-Typen, die EFA unterstützen
`rdma_read_wr_err`	Die Anzahl der RDMA-Schreibvorgänge, bei denen lokale oder externe Fehler aufgetreten sind. Einheit: Anzahl	Alle Instance-Typen, die EFA unterstützen
`rdma_read_resp_bytes`	Die Anzahl der als Antwort auf RDMA-Lesevorgänge gesendeten Bytes. Einheit: Bytes	Alle Instance-Typen, die EFA unterstützen
`rdma_write_recv_bytes`	Die Anzahl der von Sendevorgängen empfangenen Bytes. Einheit: Bytes	Alle Instance-Typen, die EFA unterstützen

Metrik	Description	Unterstützte Instance-Typen
`retrans_bytes`	Die Anzahl der erneut übertragenen EFA-SRD-Bytes. Einheit: Anzahl	Instance-Typen von Nitro v4 und höher, die EFA unterstützen
`retrans_pkts`	Die Anzahl der erneut übertragenen EFA-SRD-Pakete. Einheit: Bytes	Instance-Typen von Nitro v4 und höher, die EFA unterstützen
`retrans_timeout_events`	Die Häufigkeit, mit der EFA-SRD-Datenverkehr das Zeitlimit überschritten hat und zu einer Änderung des Netzwerkpfads geführt hat. Einheit: Anzahl	Instance-Typen von Nitro v4 und höher, die EFA unterstützen
`impaired_remote_conn_events`	Wie oft EFA-SRD-Verbindungen in einen beeinträchtigten Status übergegangen sind, was zu einer verringerten Durchsatzrate geführt hat. Einheit: Anzahl	Instance-Typen von Nitro v4 und höher, die EFA unterstützen
`unresponsive_remote_events`	Wie oft eine EFA-SRD-Remoteverbindung nicht reagiert hat. Einheit: Anzahl	Instance-Typen von Nitro v4 und höher, die EFA unterstützen

Weitere Informationen zu den Instance-Typen, die EFA unterstützen, finden Sie unter Unterstützte Instance-Typen.

EFA-Treibermetriken für Ihre Instance abrufen

Sie können das Befehlszeilentool rdma-tool verwenden, um die Metriken für alle mit einer Instance verbundenen EFA-Schnittstellen wie folgt abzurufen:

```
$ rdma -p statistic show
link rdmap0s31/1
    tx_bytes 0
    tx_pkts 0
    rx_bytes 0
    rx_pkts 0
    rx_drops 0
    send_bytes 0
    send_wrs 0
    recv_bytes 0
    recv_wrs 0
    rdma_read_wrs 0
    rdma_read_bytes 0
    rdma_read_wr_err 0
    rdma_read_resp_bytes 0
    rdma_write_wrs 0
    rdma_write_bytes 0
    rdma_write_wr_err 0
    retrans_bytes 0
    retrans_pkts 0
    retrans_timeout_events 0
    unresponsive_remote_events 0
    impaired_remote_conn_events 0
```

Alternativ können Sie die Metriken für jede EFA-Schnittstelle, die an eine Instance angefügt ist, mit dem folgenden Befehl aus den SYS-Dateien abrufen.

```
$ more /sys/class/infiniband/device_number/ports/port_number/hw_counters/* | cat
```

Beispiel

```
$ more /sys/class/infiniband/rdmap0s31/ports/1/hw_counters/* | cat
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/lifespan
::::::::::::::
12
::::::::::::::
```

```
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_read_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_read_resp_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_read_wr_err
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_read_wrs
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_write_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_write_recv_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_write_wr_err
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rdma_write_wrs
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/recv_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/recv_wrs
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rx_bytes
::::::::::::::
0
::::::::::::::
```

```
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rx_drops
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/rx_pkts
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/send_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/send_wrs
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/tx_bytes
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/tx_pkts
::::::::::::::
0
::::::::::::::
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/retrans_bytes
::::::::::::::
0
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/retrans_pkts
::::::::::::::
0
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/retrans_timeout_events
::::::::::::::
0
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/unresponsive_remote_events
::::::::::::::
0
/sys/class/infiniband/rdmap0s31/ports/1/hw_counters/impaired_remote_conn_events
::::::::::::::
0
```

Amazon VPC-Flussprotokolle

Sie können ein Amazon VPC-Flow-Protokoll erstellen, um Informationen über den Datenverkehr zu und von Ihrem EFA zu erfassen. Flow-Protokolldaten können in Amazon CloudWatch Logs und Amazon S3 veröffentlicht werden. Nachdem Sie ein Flow-Protokoll erstellt haben, können Sie die darin enthaltenen Daten abrufen und an dem gewählten Ziel anzeigen. Weitere Informationen finden Sie unter VPC-Flow-Protokolle im Amazon VPC Benutzerhandbuch.

Sie erstellen ein Flow-Protokoll für einen EFA auf gleiche Weise, wie Sie ein Flow-Protokoll für eine Elastic Network Interface erstellen. Weitere Informationen finden Sie unter Erstellen eines Flow-Protokolls im Amazon-VPC-Benutzerhandbuch.

In den Flow-Protokolleinträgen wird EFA-Datenverkehr von `srcAddress` und `destAddress` identifiziert, die beide als MAC-Adressen formatiert sind, wie im folgenden Beispiel veranschaulicht.

```
version accountId  eniId        srcAddress        destAddress       sourcePort destPort
 protocol packets bytes start      end        action log-status
2       3794735123 eni-10000001 01:23:45:67:89:ab 05:23:45:67:89:ab -          -
 -        9       5689  1521232534 1524512343 ACCEPT OK
```

Amazon CloudWatch

Wenn Sie EFA in einem Amazon EKS-Cluster verwenden, können Sie Ihre EFAs Nutzung von CloudWatch Container Insights überwachen. Amazon CloudWatch Container Insights unterstützt alle EFA-Treibermetriken mit Ausnahme von: `retrans_bytesretrans_pkts`,`retrans_timeout_events`,`unresponsive_remote_events`, `undimpaired_remote_conn_events`.

Weitere Informationen finden Sie unter Amazon EKS- und Kubernetes Container Insights-Metriken im CloudWatch Amazon-Benutzerhandbuch.

Überprüfen des EFA-Installationsprogramms mithilfe einer Prüfsumme

Sie können den EFA-Tarball (`.tar.gz`Datei) optional mit einer OR-Prüfsumme verifizieren. MD5 SHA256 Diese Vorgehensweise wird empfohlen, um die Identität des Software-Publishers zu überprüfen und zu prüfen, ob die Anwendung seit der Veröffentlichung nicht verändert oder beschädigt wurde.

So überprüfen Sie die Tarball

Verwenden Sie das Hilfsprogramm md5sum für die MD5 Prüfsumme oder das Hilfsprogramm sha256sum für die Prüfsumme und geben Sie den SHA256 Tarball-Dateinamen an. Sie müssen den Befehl aus dem Verzeichnis heraus ausführen, in dem Sie die Tarball-Datei gespeichert haben.

- MD5

```
$  md5sum tarball_filename.tar.gz
```

- SHA256

```
$  sha256sum tarball_filename.tar.gz
```

Die Befehle sollten einen Prüfsummenwert im folgenden Format zurückgeben.

```
checksum_value tarball_filename.tar.gz
```

Vergleichen Sie den vom Befehl zurückgegebenen Prüfsummenwert mit dem in der folgenden Tabelle angegebenen Prüfsummenwert. Wenn die Prüfsummen übereinstimmen, ist es sicher, das Installationsskript auszuführen. Wenn die Prüfsummen nicht übereinstimmen, führen Sie das Installationsskript nicht aus, und wenden Sie sich an den Support Support.

Mit dem folgenden Befehl wird beispielsweise der EFA 1.9.4-Tarball anhand der Prüfsumme verifiziert. SHA256

```
$  sha256sum aws-efa-installer-1.9.4.tar.gz
```

Beispielausgabe:

```
1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14 aws-efa-
installer-1.9.4.tar.gz
```

In der folgenden Tabelle sind die Prüfsummen für aktuelle Versionen von EFA aufgeführt.

Version	Prüfsummen
EFA 1.45.1	MD5: 91c3c87e16bbcaca1513252c38b771bb

Version	Prüfsummen
	SHA256: 9aeb20c645135b6039 cc08986d8f14e63280f7839e882 a74df5e83627ffeaa17
EFA 1.45.0	MD5: 800aeddfa9d9c5f139a7b8f7c4fec627 SHA256: 25ba26a0877fe33173 90dc126aad2f23e27fc461cf0b9 40004f032cb342fa539
EFA 1,44.0	MD5: d024f6bebe080db42745103b84ca7c43 SHA256: f129a5b44a49d593d2 47e55a59eb9bcb57121566e1c2e 42b832a4e794fa83d8a
EFA 1.43.3	MD5: 4dbc6eeecc516760253c10cbedb 6319d SHA256: 6c470ebce254c71653 47b5048895ac2996c8856727164 2297f4c597738300652
EFA 1.43.2	MD5: 7287b25a07c9747c0d4001e8fc5 f59b2 SHA256: de15c5bdbc83b952af bde876110830c604ad0796680e5 157c05f7c1979a41069
EFA 1.43.1	MD5: 7cfafc8debaea51dd4966fa0b2b ba673 SHA256: 54211eda0c193138ee8ed09b5fb 41c41fc76fe0a77935fa4ec8d989466342740

Version	Prüfsummen
EFA 1,43,0	MD5: f2b3dd7dc8670b541f7c23fd58e5e503 SHA256: 786df3458c499237be33bb8e50ffd4da7c18c20e254380ffc80fb90833d8cc73
EFA 1.42.0	MD5: 94b2b1db09da1dde08ec049db1f24370 SHA256: 4114fe612905ee05083ae5cb391a00a012510f3abfecc642d86c9a5ae4be9008
EFA 1.41.0	MD5: 086181c3ee3f8da512fc6e1c795e8936 SHA256: 3506354cdfbe31ff552fe75f5d0d9bb7efd29cf79bd99457347d29c751c38f9f
EFA 1.40.0	MD5: f3ec6f73fbeaccba082327507581157c SHA256: 30491b0fe7c3470d4439594538855c981b05fa69862d74f8c05eb9b97912368a
EFA 1.39.0	MD5: c223d5954a85a7fbcd248c942b866e43 SHA256: 2cbc028c03064633bb990782b47c36156637769e2f48704417a9c700a7a32101

Version	Prüfsummen
EFA 1.38.1	MD5: f112569e828ab65187777f794bab542c SHA256: 83923374afd388b1cfcf4b3a21a2b1ba7cf46a01a587f7b519b8386cb95e4f81
EFA 1.38.0	MD5: 43a2a446b33a2506f40853d55059f1ea SHA256: 4f436954f35ad53754b4d005fd8d0be63de3b4184de41a695b504bdce0fecb22
EFA 1.37.0	MD5: 6328070192bae920eca45797ad4c1db1 SHA256: 2584fc3c8bb99f29b3285e275747ff09d67c18e162c2a652e36c976b72154bfb
EFA 1.36.0	MD5: 1bec83180fbffb23452ab6469ca21dfa SHA256: de183f333cfb58aeb7908a67bf9106985ba3ccb7f8638b851d2a0d8dbfacaec4
EFA 1.35.0	MD5: 252f03c978dca5f8e8d9f34e488b256e SHA256: 432b6ad4368ba0cd8b902729d14a908a97be7a3dcc5239422ea994a47f35a5e1

Version	Prüfsummen
EFA 1.34.0	MD5: `5cd4b28d27a31677c16139b54c9acb45` SHA256: `bd68839e741b0afd3ec2e37d50603803cfa7a279c120f0a736cc57c2ff2d7fdc`
EFA 1.33.0	MD5: `e2f61fccbcaa11e2ccfddd3660522276` SHA256: `0372877b87c6a7337bb7791d255e1053b907d030489fb2c3732ba70069185fce`
EFA 1.32.0	MD5: `db8d65cc028d8d08b5a9f2d88881c1b1` SHA256: `5f7233760be57f6fee6de8c09acbfbf59238de848e06048dc54d156ef578fc66`
EFA 1.31.0	MD5: `856352f12bef2ccbadcd75e35aa52aaf` SHA256: `943325bd37902a4300ac9e5715163537d56ecb4e7b87b37827c3e547aa1897bf`
EFA 1.30.0	MD5: `31f48e1a47fe93ede8ebd273fb747358` SHA256: `876ab9403e07a0c3c91a1a34685a52eced890ae052df94857f6081c5f6c78a0a`

Version	Prüfsummen
EFA 1.29.1	MD5: e1872ca815d752c1d7c2b5c175e52a16 SHA256: 178b263b8c25845b63dc93b25bcdff5870df5204ec509af26f43e8d283488744
EFA 1.29.0	MD5: 39d06a002154d94cd982ed348133f385 SHA256: 836655f87015547e733e7d9f7c760e4e24697f8bbc261bb5f3560abd4206bc36
EFA 1.28.0	MD5: 9dc13b7446665822605e66febe074035 SHA256: 2e625d2d6d3e073b5178e8e861891273d896b66d03cb1a32244fd56789f1c435
EFA 1.27.0	MD5: 98bfb515ea3e8d93f554020f3837fa15 SHA256: 1d49a97b0bf8d964d91652a79ac851f2550e33a5bf9d0cf86ec9357ff6579aa3
EFA 1.26.1	MD5: 884e74671fdef4725501f7cd2d451d0c SHA256: c616994c924f54ebfabfab32b7fe8ac56947fae00a0ff453d975e298d174fc96

Version	Prüfsummen
EFA 1.26.0	MD5: f8839f12ff2e3b9ba09ae8a82b30e663 SHA256: bc1abc1f76e97d204d3755d2a9ca307fc423e51c63141f798c2f15be3715aa11
EFA 1.25.1	MD5: 6d876b894547847a45bb8854d4431f18 SHA256: d2abc553d22b89a4ce92882052c1fa6de450d3a801fe005da718b7d4b9602b06
EFA 1.25.0	MD5: 1993836ca749596051da04694ea0d00c SHA256: 98b7b26ce031a2d6a93de2297cc71b03af647194866369ca53b60d82d45ad342
EFA 1.24.1	MD5: 211b249f39d53086f3cb0c07665f4e6f SHA256: 120cfeec233af0955623ac7133b674143329f9561a9a8193e473060f596aec62
EFA 1.24.0	MD5: 7afe0187951e2dd2c9cc4b572e62f924 SHA256: 878623f819a0d9099d76ecd41cf4f569d4c3aac0c9bb7ba9536347c50b6bf88e

Version	Prüfsummen
EFA 1.23.1	MD5: 22491e114b6ee7160a8290145dca0c28 SHA256: 5ca848d8e0ff4d1571cd443c36f8d27c8cdf2a0c97e9068ebf000c303fc40797
EFA 1.23.0	MD5: 38a6d7c1861f5038dba4e441ca7683ca SHA256: 555d497a60f22e3857fdeb3dfc53aa86d05926023c68c916d15d2dc3df6525bd
EFA 1.22.1	MD5: 600c0ad7cdbc06e8e846cb763f92901b SHA256: f90f3d5f59c031b9a964466b5401e86fd0429272408f6c207c3f9048254e9665
EFA 1.22.0	MD5: 8f100c93dc8ab519c2aeb5dab89e98f8 SHA256: f329e7d54a86a03ea51da6ea9a5b68fb354fbae4a57a02f9592e21fce431dc3a
EFA 1.21.0	MD5: 959ccc3a4347461909ec02ed3ba7c372 SHA256: c64e6ca34ccfc3ebe8e82d08899ae8442b3ef552541cf5429c43d11a04333050

Version	Prüfsummen
EFA 1.20.0	MD5: `7ebfbb8e85f1b94709df4ab3db47913b` SHA256: `aeefd2681ffd5c4c631d1502867db5b831621d6eb85b61fe3ec80df983d1dcf0`
EFA 1.19.0	MD5: `2fd45324953347ec5518da7e3fefa0ec` SHA256: `99b77821b9e72c8dea015cc92c96193e8db307deee05b91a58094cc331f16709`
EFA 1.18.0	MD5: `fc2571a72f5d3c7b7b576ce2de38d91e` SHA256: `acb18a0808aedb9a5e485f1469225b9ac97f21db9af78e4cd6939700debe1cb6`
EFA 1.17.3	MD5: `0517df4a190356ab559235147174cafd` SHA256: `5130998b0d2883bbae189b21ab215ecbc1b01ae0231659a9b4a17b0a33ebc6ca`
EFA 1.17.2	MD5: `a329dedab53c4832df218a24449f4c9a` SHA256: `bca1fdde8b32b00346e175e597ffab32a09a08ee9ab136875fb38283cc4cd099`

Version	Prüfsummen
EFA 1.17.1	MD5: `733ae2cfc9d14b52017eaf0a2ab6b0ff` SHA256: `f29322640a88ae9279805993cb836276ea240623820848463ca686c8ce02136f`
EFA 1.17.0	MD5: `d430fc841563c11c3805c5f82a4746b1` SHA256: `75ab0cee4fb6bd38889dce313183f5d3a83bd233e0a6ef6205d8352821ea901d`
EFA 1.16.0	MD5: `399548d3b0d2e812d74dd67937b696b4` SHA256: `cecec36495a1bc6fdc82f97761a541e4fb6c9a3cbf3cfcb145acf25ea5dbd45b`
EFA 1.15.2	MD5: `955fea580d5170b05823d51acde7ca21` SHA256: `84df4fbc1b3741b6c073176287789a601a589313accc8e6653434e8d4c20bd49`
EFA 1.15.1	MD5: `c4610267039f72bbe4e35d7bf53519bc` SHA256: `be871781a1b9a15fca342a9d169219260069942a8bda7a8ad06d4baeb5e2efd7`

Version	Prüfsummen
EFA 1.15.0	MD5: 9861694e1cc00d884fadac07d22898be SHA256: b329862dd5729d2d098d0507fb486bf859d7c70ce18b61c302982234a3a5c88f
EFA 1.14.1	MD5: 50ba56397d359e57872fde1f74d4168a SHA256: c7b1b48e86fe4b3eaa4299d3600930919c4fe6d88cc6e2c7e4a408a3f16452c7
EFA 1.14.0	MD5: 40805e7fd842c36ececb9fd7f921b1ae SHA256: 662d62c12de85116df33780d40e0533ef7dad92709f4f613907475a7a1b60a97
EFA 1.13.0	MD5: c91d16556f4fd53becadbb345828221e SHA256: ad6705eb23a3fce44af3afc0f7643091595653a723ad0374084f4f2b715192e1
EFA 1.12.3	MD5: 818aee81f097918cfaebd724eddea678 SHA256: 2c225321824788b8ca3fbc118207b944cdb096b847e1e0d1d853ef2f0d727172

Version	Prüfsummen
EFA 1.12.2	MD5: 956bb1fc5ae0d6f0f87d2e481d49fccf SHA256: 083a868a2c212a5a4fcf3e4d732b685ce39cceb3ca7e5d50d0b74e7788d06259
EFA 1.12.1	MD5: f5bfe52779df435188b0a2874d0633ea SHA256: 5665795c2b4f09d5f3f767506d4d4c429695b36d4a17e5758b27f033aee58900
EFA 1.12.0	MD5: d6c6b49fafb39b770297e1cc44fe68a6 SHA256: 28256c57e9ecc0b0778b41c1f777a9982b4e8eae782343dfe1246079933dca59
EFA 1.11.2	MD5: 2376cf18d1353a4551e35c33d269c404 SHA256: a25786f98a3628f7f54f7f74ee2b39bc6734ea9374720507d37d3e8bf8ee1371
EFA 1.11.1	MD5: 026b0d9a0a48780cc7406bd51997b1c0 SHA256: 6cb04baf5ffc58ddf319e956b5461289199c8dd805fe216f8f9ab8d102f6d02a

Version	Prüfsummen
EFA 1.11.0	MD5: 7d9058e010ad65bf2e14259214a36949 SHA256: 7891f6d45ae33e822189511c4ea1d14c9d54d000f6696f97be54e915ce2c9dfa
EFA 1.10.1	MD5: 78521d3d668be22976f46c6fecc7b730 SHA256: 61564582de7320b21de319f532c3a677d26cc46785378eb3b95c636506b9bcb4
EFA 1.10.0	MD5: 46f73f5a7afe41b4bb918c81888fefa9 SHA256: 136612f96f2a085a7d98296da0afb6fa807b38142e2fc0c548fa986c41186282
EFA 1.9.5	MD5: 95edb8a209c18ba8d250409846eb6ef4 SHA256: a4343308d7ea4dc943ccc21bcebed913e8868e59bfb2ac93599c61a7c87d7d25
EFA 1.9.4	MD5: f26dd5c350422c1a985e35947fa5aa28 SHA256: 1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14

Version	Prüfsummen
EFA 1.9.3	MD5: `95755765a097802d3e6d5018d1a5d3d6` SHA256: `46ce732d6f3fcc9edf6a6e9f9df0ad136054328e24675567f7029edab90c68f1`
EFA 1.8.4	MD5: `85d594c41e831afc6c9305263140457e` SHA256: `0d974655a09b213d7859e658965e56dc4f23a0eee2dc44bb41b6d039cc5bab45`

Versionshinweise zu Elastic Fabric Adapter

In der folgenden Tabelle werden der Versionsverlauf und das Änderungsprotokoll für die Elastic-Fabric-Adapter-Software beschrieben.

Version	Änderungen	Datum der Veröffentlichung
1,45,1	• Führen Sie ein Upgrade auf libfabric 2.3.1amzn3.0 durch • Es wurde ein Fehler behoben, durch den cq_data auf 2 Byte gekürzt wurde, obwohl der Anbieter die Unterstützung für 4 Byte angekündigt hatte	26. November 2025
1.45.0	• Führen Sie ein Upgrade auf rdma-core 60.amzn0 durch • Erweitern Sie die DV-Abfrage CQ, um die Türklingel zurückzugeben •	17. November 2025

Version	Änderungen	Datum der Veröffentlichung
	Führen Sie ein Upgrade auf libfabric 2.3.1amzn2.0 durch • Support den FI_RX_CQ_DATA-Modus für efa-direct • Optimieren Sie den WQE-Post-in-Datenpfad (direkter Pfad) • Korrigieren Sie die Rennbedingung im laufenden Modus • Verbessern Sie die Protokollierung von Warnmeldungen • Verarbeitet den RMA-Abschluss für entfernte Peers korrekt • Entfernt AH-Einträge aus dem impliziten AV, wenn das AH-Limit erreicht ist • Führen Sie ein Upgrade auf libnccl-ofi 1.17.2 durch • Es wurde ein Absturz mit NCCL v2.28.x behoben, bei dem die Libfabric-Initialisierung fehlschlug • Unterstützung für die G7E-Instance-Familie hinzugefügt • Es wurde ein Problem behoben, bei dem NCCL fälschlic herweise versuchen konnte, einen GPUDirect RDMA-Pfad auf Plattformen zu verwenden, die DMA-BUF unterstützen • Das Problem mit der Reihenfolge beim Herunterfahren, für das eine Speicherregistrierung pro Endpunkt erforderlich war NICs , wurde behoben (Cray Slingshot)	

Version	Änderungen	Datum der Veröffentlichung

1,44,0	• Upgrade auf rdma-core 59.amzn0
	  • Unterstützung für Bind QPs - und CQs Thread-Domänen hinzufügen
	  • Unterstützung für die Zuweisung einer übergeordneten Domain hinzufügen
	  • Unterstützung für die Zuweisung von Thread-Domains hinzufügen
	  • Direkte Verbanfragen zu QP und CQ hinzufügen
	  • Option zum Erstellen von CQ mit externem Arbeitsspeicher hinzufügen
	  • CQ-Umfrage nach der QP-Zerstörung korrigieren
	• Upgrade auf libfabric 2.3.1amzn1.0
	• Upgrade auf Open MPI 5.0.8amzn1
	  • Funktionserweiterungen
	  • Fehlerbehebungen
	• Upgrade auf libnccl-ofi 1.17.1
	  • Unterstützt NCCL v2.28.3-1 unter Beibehaltung der Abwärtskompatibilität mit NCCL v2.17.1 und höher.
	  •
		29. Oktober 2025

Version	Änderungen	Datum der Veröffentlichung
	Für das Entwickeln mit platform-aws ist Libfabric v1.22.0amzn4.0 oder höher erforderlich. Wurde mit Versionen bis Libfabric v2.3.1amzn1.0 getestet. • Korrekturen zur Unterstützung der Kompatibilität zwischen CUDA12 und CUDA13.	
1.43.3	• Upgrade auf EFA-Treiber 2.17.3 • P2P mit NVIDIA-580-Treibern unterstützen • Die MR-Registrierung für 6.17 und auf Kernels anpassen	1. Oktober 2025
1.43,2	• Upgrade auf libnccl-ofi 1.16.3 • Unterstützt NCCL v2.27.7-1 unter Beibehaltung der Abwärtskompatibilität mit NCCL v2.17.1 und höher. • Für das Entwickeln mit platform-aws ist Libfabric v1.22.0amzn4.0 oder höher erforderlich. Wurde mit Versionen bis Libfabric v2.1.0amzn5.0 getestet. • domain-per-threadStandardmäßig auf allen EC2 Amazon-Instance-Typen aktiviert, um die Leistung einiger Anwendungen zu verbessern, bei denen NCCL mehrere Proxy-Threads erstellt	15. August 2025

Version	Änderungen	Datum der Veröffentlichung

1.43.1	• Upgrade auf libnccl-ofi 1.16.2
	  • Unterstützt NCCL v2.27.6-1 unter Beibehaltung der Abwärtskompatibilität mit NCCL v2.17.1 und höher.
	  • Für das Entwickeln mit platform-aws ist Libfabric v1.22.0amzn4.0 oder höher erforderlich. Wurde mit Versionen bis Libfabric v2.1.0amzn4.0 getestet.
	  • Es wurde eine neue Plattformkonfiguration hinzugefügt, um die Verwendung des OFI NCCL-Plug-ins auf dem Amazon EC2 p5.4xlarge-Instance-Typ zu unterstützen
	• Upgrade auf libfabric 2.1.0amzn5.0
		31. Juli 2025

Version	Änderungen	Datum der Veröffentlichung

1.43.0	• Upgrade auf libnccl-ofi 1.16.1
	  • Unterstützt NCCL v2.27.6-1 unter Beibehaltung der Abwärtskompatibilität mit NCCL v2.17.1 und höher.
	  • Für das Entwickeln mit platform-aws ist Libfabric v1.22.0amzn4.0 oder höher erforderlich. Wurde mit Versionen bis Libfabric 2.1.0amzn3 getestet.
	  • Aktualisieren Sie das in der Topologiedatei angegebene PCI-Link-Speed-Format, sodass es mit Kernel 5.7+ übereinstimmt
	  • SKIP_NICS_WITHOUT_ACCEL_AT_SAME_PCI_LEVEL wurde hinzugefügt, um libfabric-NICs zu überspringen, die keinen Beschleuniger auf derselben PCI-Ebene haben
	• Upgrade auf EFA-Treiber 2.17.2
	• Führen Sie ein Upgrade auf 1.2.2 durch efa-nv-peermem
	• Upgrade auf libfabric 2.1.0amzn4.0
	• Upgrade auf rdma-core 58.amzn0
	  • Doppelte Verwendung des Arbeitsanforderungsindexes behoben
	  • WQE-Länge zum Nachverfolgungspunkt post_send hinzufügen
	• Optimierungen für Graviton-Plattformen ermöglichen
	•
		25 Juli 2025

Version	Änderungen	Datum der Veröffentlichung
	Außerbetriebnahme der Unterstützung für Ubuntu 20.04	

Version	Änderungen	Datum der Veröffentlichung

1.42.0	• Upgrade auf EFA-Treiber 2.15.3
	• Führen Sie ein Upgrade auf 1.2.1 durch efa-nv-peermem
	• Upgrade auf rdma-core 57.amzn1
	  • Doppelte Verwendung des Arbeitsanforderungsindexes behoben
	• Upgrade auf libfabric 2.1.0amzn3.0
	• Upgrade auf libnccl-ofi 1.15.0
	  • Unterstützt NCCL v2.26.6-1 unter Beibehaltung der Abwärtskompatibilität mit NCCL v2.17.1 und höher.
	  • Für das Entwickeln mit platform-aws ist Libfabric v1.22.0amzn4.0 oder höher erforderlich. Wurde mit Versionen bis Libfabric 2.1.0amzn3 getestet.
	  • Build-System- und Plattformunterstützung
	  • Unterstützung für die Amazon EC2 P6-B200-Plattform hinzugefügt
	  • Der Standardname der Plugin-Bibliothek wurde in libnccl-net-ofi .so geändert und standardmäßig ein Symlink von .so zu libnccl-net-ofi libnccl-net.so erstellt, um die Abwärtskompatibilität aufrechtzuerhalten. Dadurch können Benutzer NCCL_NET_PLUGIN=ofi setzen, um NCCL zu zwingen, das OFI-Plug-In für die Kommunikation zu verwenden. Wenn Sie bei der Konfiguration --angebendisable-nccl-net-symlink , wird der Symlink übersprungen, sodass mehrere Plugins im selben Container installiert werden können.
	  • Tuning- und Leistungsverbesserungen
		6. Juni 2025

Version	Änderungen	Datum der Veröffentlichung
	• Tuner-Unterstützung auf P6-B200 für AllReduce, und ReduceScatter Regionen für 0x0- und AllGather 0x7-Bitmasken hinzugefügt • Die Standardlatenz für die Plattformen P5en und P6-B200 wurde auf der Grundlage empirischer Ergebnisse und Analysen aktualisiert • Aktualisierung zur Verwendung der NCCL-v10-API mit TrafficClass-Parameterunterstützung für die zukünftige Priorisierung des Datenverkehrs • Die Plugin-Codebasis wurde von C nach C++ migriert • Unterstützung für Jobs hinzugefügt, bei denen die Anzahl der pro GPU von NICs System zu System unterschiedlich ist. Weitere Informationen finden Sie in der Dokumentation zur Laufzeitumgebungsvariablen OFI_NCCL_FORCE_NUM_RAILS.	
1.41.0	• Upgrade auf rdma-core 57.amzn0	16. Mai 2025
1.40.0	• Upgrade auf libfabric 2.1.0amzn2.0 • Upgrade auf rdma-core 56.0 • Upgrade auf efa-config 1.18 • Außerbetriebnahme der Unterstützung für Debian 10 • Upgrade auf libnccl-ofi 1.14.2 • CUDA-Unterstützung in Libfabric in ARM für Ubuntu und Amazon Linux 2023 aktivieren • libnccl-ofi in ARM für Ubuntu und Amazon Linux 2023 hinzufügen	2. Mai 2025

Version	Änderungen	Datum der Veröffentlichung
1.39.0	• Upgrade auf libfabric 2.1.0 • Upgrade auf Open MPI 5.0.6 • Upgrade auf libnccl-ofi 1.14.1 • Upgrade auf EFA-Treiber 2.15.0	16. April 2025
1,38,1	• Auf `Libfabric 1.22.0amzn5.0` aktualisieren	03. März 2025
1,38,0	• Add `libnccl-ofi 1.13.2-1`	8. Januar 2025
1.37.0	• Aktualisieren auf `libfabric 1.22.0amzn4.0` • Aktualisieren auf `rdma-core 54.amzn0`	18. November 2024
1.36.0	• Unterstützung für Debian 12 hinzufügen • `efa_test.sh` als Hilfsprogramm-Skript unter `/opt/amazon/efa/bin` verteilen • Upgrade auf EFA-Treiber 2.13.0 • Aktualisieren auf `libfabric 1.22.0amzn3.0` • Aktualisieren auf `rdma-core 54.0` • Upgrade auf Open MPI 4.1.7	7. November 2024
1.35.0	• Upgrade auf Open MPI 5.0.5 • Upgrade auf PRRTE 3.0.6 und Umbenennung des RPM-Pakets in prrte-aws • Benennen Sie das Open PMIx RPM-Paket in pmix-aws um • Build-Optionen für dpkg- und RPM-Builds konfigurieren • Aktualisieren auf `Libfabric 1.22.0amzn2.0` • Upgrade auf EFA-Treiber 2.12.1	14. Oktober 2024

Version	Änderungen	Datum der Veröffentlichung
1.34.0	• Unterstützung für CentOS 7 und RHEL 7 einstellen • `Libfabric 1.22.0amzn1.0` erfassen • Das Paket efa-config auf Version 1.17 aktualisieren	6. August 2024
1,33,0	• Upgrade auf EFA-Treiber 2.10.0 • Aktualisieren auf `rdma-core 52.0` • Upgrade auf PRRTE 3.0.5 • Upgrade auf Open MPI 5.0.3 • Unterstützung für Ubuntu 24.04 LTS hinzufügen • Entfernen Sie die HTML-Dokumentation zu OpenPMIx, PRRTE und Open MPI. Benutzer sollten sich auf die offizielle Website beziehen. • Unterstützung für openSUSE 15.4 oder älter einstellen	20. Juni 2024
1.32.0	• Upgrade auf EFA-Treiber 2.8.0 • Führen Sie ein Upgrade auf Treiber 1.1.1 efa-nv-peermem durch • Upgrade auf efa-config-Paket 1.16 • Upgrade auf efa-profile-Paket 1.7 • Aktualisieren auf `rdma-core 50.0` • Aktualisieren auf `libfabric 1.21.0amzn1.0` • `efa_test.sh` durch die Portauswahl `fi_pingpong` erweitern • Bei Bedarf einen neueren rdma-core vom System installieren	18. April 2024

Version	Änderungen	Datum der Veröffentlichung
1.31.0	• Führen Sie ein Upgrade auf Open 4.2.8 durch PMIx • Upgrade auf PRRTE 3.0.3 • Führen Sie ein Upgrade auf Open MPI 5.0.2 durch und konvertieren Sie die MCA-Komponenten in DSO. • Aktualisieren auf `Libfabric 1.20.1amzn1.0`	7. März 2024
1.30.0	• Schließt Open PMIx 4.2.7 ein, das standardmäßig unter `/opt/amazon/pmix` installiert ist • PRRTE 3.0.2 einschließen, das standardmäßig unter `/opt/amazon/prrte` installiert ist • OpenMPI 5.0.0 einschließen, das standardmäßig unter `/opt/amazon/openmpi5` installiert ist • efa-profile auf Version 1.6 aktualisieren	Dezember 2023
1.29.1	• `libfabric 1.19.0amzn4.0` erfassen	Dezember 2023
1.29.0	• EFA-Kernel-Treiber 2.6.0 erfassen • `libfabric 1.19.0amzn3.0` erfassen	November 2023
1.28.0	• Upgrade auf Open MPI 4.1.6 • `libfabric 1.19.0amzn2.0` erfassen	Oktober 2023
1.27.0	• `Libfabric 1.19.0amzn1.0` zum Installer hinzufügen • GCC-integrierte Atomics für Open MPI 4 ermöglichen	September 2023
1.26.1	• `efa_test.sh` : Fehler bei unendlichen Wiederholungsversuchen beheben	September 2023

Version	Änderungen	Datum der Veröffentlichung
1.26.0	• Unterstützung für RHEL 9 hinzufügen • Debug-Build auf mehreren Distributionen behoben • `libfabric 1.18.2amzn1.0` erfassen • `efa_test.sh` : Wiederholungsversuch für `fi_pingpong` hinzufügen	September 2023
1.25.1	• `libfabric 1.18.1amzn1.0` erfassen • Timeouts in EFA-Installationsskripten aktualisieren	September 2023
1.25.0	• Unterstützung für Amazon Linux 2023 hinzufügen • Bugfix beim Test nach der Installation	Juli 2023
1.24.1	• Upgrade auf libfabric 1.18.1 • Upgrade auf EFA-Treiber 2.5.0	Juli 2023
1.24.0	• `rdma-core 46.0` erfassen • EFA-Treiber 2.4.1 erfassen • Unterstützung für Debian 11	Juni 2023
1.23.1	• `libfabric 1.18.0amzn2.0` erfassen	Juni 2023
1.23.0	• Unterstützung für Debian 10 hinzufügen • Unterstützung für Ubuntu 18.04 LTS einstellen • Upgrade auf efa-config-Paket 1.14 • `libfabric 1.18.0amzn1.0` erfassen	Mai 2023
1.22.1	• Upgrade auf libfabric 1.17.1	März 2023
1.22.0	• Upgrade auf Open MPI 4.1.5 • Upgrade auf libfabric 1.17.0 • Upgrade auf efa-config-Paket 1.13	Februar 2023

Version	Änderungen	Datum der Veröffentlichung
1.21.0	• Unterstützung für das Betriebssystem Rocky Linux 9 hinzufügen • EFA-Treiber 2.1.1 erfassen • `libfabric 1.16.1amzn3.0` erfassen • Upgrade auf efa-config-Paket 1.12	Dezember 2022
1.20.0	• Unterstützung für das Betriebssystem Rocky Linux 8 hinzufügen. • EFA-Treiber 2.1.0 erfassen • `rdma-core 43.0` erfassen • `libfabric 1.16.1amzn1.0` erfassen	November 2022
1.19.0	• `libfabric 1.16.0` erfassen • Open MPI mit `--enable-orterun-prefix-by-default` erstellen	Oktober 2022
1.18.0	• Unterstützung für Ubuntu 22.04 hinzugefügt	August 2022
1.17.3	• libfabric auf `1.16.0~amzn4.0` aktualisieren. Das ~ weist darauf hin, dass es sich um eine Vorabversion von libfabric 1.16.0 handelt. • Verlängern Sie das Timeout für den Pingpong-Test nach der Installation auf 20 Sekunden.	August 2022
1.17.2	• libfabric auf `1.16.0~amzn3.0` aktualisieren. Das ~ weist darauf hin, dass es sich um eine Vorabversion von libfabric 1.16.0 handelt.	Juli 2022

Version	Änderungen	Datum der Veröffentlichung
1.17.1	• libfabric auf `1.16.0~amzn2.0` aktualisieren. Das ~ weist darauf hin, dass es sich um eine Vorabversion von libfabric 1.16.0 handelt. • Den experimentellen Netzanbieter beim Erstellen von libfabric deaktivieren	Juli 2022
1.17.0	• `rdma-core` auf v41.0 aktualisieren • Open MPI auf 4.1.4 aktualisieren • libfabric auf `1.16.0~amzn1.0` aktualisieren. Das ~ weist darauf hin, dass es sich um eine Vorabversion von libfabric 1.16.0 handelt.	Juli 2022
1.16.0	• libfabric auf `1.15.1amzn1.0` aktualisieren, enthält eine Änderung des Namens der Neuron-Bibliothek • Upgrade auf efa-config 1.10 • Anbieter opx und rxd im libfabric-Build ausschließen	Juni 2022
1.15.2	• libfabric auf 1.14.1 aktualisieren	Mai 2022
1.15.1	• libfabric auf `1.14.0amzn1.0` aktualisieren	März 2022
1.15.0	• Behebt einen Fehler, der dazu führte, dass die Installation auf Open SuSE 15.3 fehlschlug • Unterstützung für Open SuSE 15.2 einstellen (da Open SuSE 15.2 das Ende seiner Lebensdauer erreicht hat) • Unterstützung für CentOS 8 einstellen (da CentOS 8 das Ende seiner Lebensdauer erreicht hat) • libfabric auf 1.14.0 aktualisieren • EFA-Kerneltreibers auf 1.16.0 aktualisieren • `rdma-core` auf v39.0 aktualisieren • Aktualisieren Sie Open MPI auf Version 4.1.2.	Februar 2022

Version	Änderungen	Datum der Veröffentlichung
1.14.1	• libfabric auf `1.13.2amzn1.0` aktualisieren.	Oktober 2021
1.14.0	• EFA-Kernel-Treiber 1.14.2 erfassen • Legen Sie `-g, --enable-gdr` in `efa_installer.sh` als no-op-Option fest, da der neueste EFA-Kerneltreiber die GDR-Unterstützung standardmäßig aktiviert. • `rdma-core v37.0` erfassen • `libfabric 1.13.2` erfassen • Fügen Sie während der Installation eine Paketliste hinzu und vergleichen Sie RPM/DEB sie mit der Liste, um unbekannte Paketinstallationen zu verhindern. • Fügen Sie dem Installationsskript sleep hinzu, um zu warten, bis die udev-Regel nach dem erneuten Laden des EFA-Treibers angewendet wird.	Oktober 2021
1.13.0	• Aktualisieren Sie `rdma-core` auf v35.0. • `libfabric` auf v1.13.0amzn1.0 aktualisieren • Fügen Sie EFA-Unterstützung für CentOS/RHEL 8 auf der Gravition2-Plattform hinzu. • Fügen Sie dem Installationsskript eine Logik für den Versionsvergleich hinzu, um die lokale Paketinstallation zu überspringen, wenn auf dem System eines mit einer höheren Version installiert ist.	August 2021
1.12.3	• Aktualisieren Sie das EFA-Kernelmodul auf 1.13.0. • Aktualisieren Sie das efa-config-Paket auf Version 1.9. Verbessern Sie die Berechnung großer Seitenreservierungen, um große Standardseitengrößen verarbeiten zu können.	Juli 2021

Version	Änderungen	Datum der Veröffentlichung
1.12.2	• Aktualisieren Sie das EFA-Kernelmodul auf 1.12.3. • Erstellen Sie Open-MPI-Debian-Pakete mit `--with-libevent=external` und `--with-hwloc=external` . • Erhöhen Sie die OpenMPI-RPM-Build-ID auf 2, um das Abwärtskompatibilitätsproblem von HWLOC auf CentOS 8 zu beheben. • Entfernen Sie die Installation der Pakete kernel-devel und kernel-source auf openSUSE 15.2. SLES15 SP2	Juni 2021
1.12.1	• Aktualisieren Sie Libfabric auf Version 1.11.2amzon1.1. • Aktualisieren Sie das EFA-Kernelmodul auf 1.12.1.	Mai 2021

Version	Änderungen	Datum der Veröffentlichung
1.12.0	• Aktualisieren Sie Open MPI auf Version 4.1.1. • Aktualisieren Sie Libfabric auf Version 1.11.2amzon1.0. • Erstellen Sie RDMA-Core für Amazon Linux 2 mit derselben Verpackungskonfiguration wie RDMA-Core. AL2 • Wenden Sie `-Wl,--enable-new-dtags` beim Erstellen von Open MPI keinen Zwang an. RPMs • Erstellen Sie Open MPI mit Systembibliotheken für hwloc und libevent. • Aktualisieren Sie das EFA-Kernelmodul auf 1.12.0. • Aktualisieren Sie das efa-config-Paket auf Version 1.8. Verbessern Sie die Berechnung großer Seitenreservierungen für langlebige Instances. • Aktualisieren Sie das efa-profile-Paket auf Version 1.5. Entfernen Sie die Datei open mpi collective tuning, die als Problemumgehung diente, um das Einfrieren von Open MPI 4.1.0 auf P4d zu Beheben. • Aktualisieren Sie `rdma-core` auf v32.1. • Stellen Sie die Unterstützung für Amazon 1 und Ubuntu 16.04 ein.	Mai 2021
1.11.2	• Behebung eines Fehlers bei dem Open MPI bei der Verwendung auf P4d einfriert, indem der Standardalgorithmus für die Implementierung von MPI_BARRIER über eine Konfigurationsdatei geändert wurde. • Deaktivieren Sie die Verwendung der integrierten Atomics in Open MPI in ARM über `--disable-builtin-atomics`, um das Compiler-Problem zu umgehen.	Februar 2021

Version	Änderungen	Datum der Veröffentlichung
1.11.1	• Aktualisieren Sie Open MPI auf Version 4.1.0. • Aktualisieren Sie das efa-config-Paket auf Version 1.7. Verbessern Sie die Berechnung der Anzahl von riesigen Seitenreservierungen. • Aktualisieren Sie das efa-profile-Paket auf Version 1.3. Entfernt jetzt, da Open MPI 4.1.0 verwendet wird, nicht mehr benötigte Dateien für kollektive Entscheidungen.	Dezember 2020
1.11.0	• Fügen Sie Unterstützung für die Gravition2-Plattform hinzu. • Aktualisieren Sie `rdma-core` auf Version 31.2amzn. • Aktualisieren Sie Libfabric auf Version 1.11.1amzon1.0. • Aktualisieren Sie efa-config auf Version 1.6. • Aktualisieren Sie efa-profile auf Version 1.2.	Dezember 2020
1.10.1	• Fügen Sie Unterstützung für CentOS/RHEL 8 hinzu. • Fügen Sie Unterstützung für Ubuntu 20.04 hinzu. • Fügen Sie Unterstützung für SUSE Linux Enterprise 15 hinzu.	November 2020
1.10.0	• GPUDirect RDMA-Unterstützung für die P4d-Plattform hinzufügen. Verwenden Sie die Installationsoption `--enable-gdr`, um das GDR-fähige Kernelmodul und den Userspace zu installieren. • Aktualisieren Sie das EFA-Kernelmodul auf Version 1.10.2. • Aktualisieren Sie `rdma-core` auf Version 31.amzn0. • Aktualisieren Sie Libfabric auf Version 1.11.1. • Aktualisieren Sie Open MPI auf Version 4.0.5. • Aktualisieren Sie efa-config auf Version 1.5. • Aktualisieren Sie efa-profile auf Version 1.1. Beinhaltet eine verbesserte Entscheidungsdatei für Open MPI Collectives.	Oktober 2020

Version	Änderungen	Datum der Veröffentlichung
1.9.5	• Aktualisieren Sie efa-config auf Version 1.4. Behebt einen Fehler in der Entscheidungsdatei für Open MPI Collective.	September 2020
1.9.4	• Aktualisieren Sie Open MPI auf Version 4.0.3. • Aktualisieren Sie Libfabric auf Version 1.10.2amzn1.1. • Aktualisieren Sie `rdma-core` auf Version 28.amzn0.	Juli 2020
1.9.3	• Aktualisieren Sie das EFA-Kernelmodul auf Version 1.6.0. • Aktualisieren Sie `rdma-core` auf Version 28.amzn0. • Aktualisieren Sie Libfabric auf Version 1.10.1amzn1.1. • Aktualisieren Sie efa-config auf Version 1.3. Fügt eine kollektive Tuning-Datei für Open MPI hinzu. • Überspringen Sie die dkms-Installation, wenn sie bereits installiert ist. • Korrigieren Sie den `--skip-kmod` -Installationsmodus so, dass er tatsächlich funktioniert.	Juni 2020
1.8.4	• Verschieben Sie die Konfigurationsdateien in die Pakete efa-config und efa-profile, sodass sie vom Paketmanager des Betriebssystems nachverfolgt werden. • Aktualisieren Sie Open MPI auf Version 4.0.3.	April 2020
1.8.3	• Aktualisieren Sie das EFA-Kernelmodul auf Version 1.5.1. • Um die Zuverlässigkeit der Installation zu erhöhen, wurde DKMS auf einigen Plattformen verteilt, anstatt sich auf EPEL-Repositorys zu verlassen. • Installieren Sie auf RHEL 7 RPMs die Installation auf CentOS 7 statt RPMs auf Amazon Linux 2.	Februar 2020
1.8.2	• Stellen Sie `rdma-core` auf die Version 25 zurück, da die Gerätenamen zwischen dem Kernelmodul und `rdma-core` nicht übereinstimmen.	Januar 2020

Version	Änderungen	Datum der Veröffentlichung
1.8.1	• Aktualisieren Sie Libfabric auf Version 1.9.0amzn1.1.	Januar 2020
1.8.0	• Aktualisieren Sie `rdma-core` auf Version 27.0. • Aktualisieren Sie das EFA-Kernelmodul auf Version 1.5.0. • Aktualisieren Sie Libfabric auf Version 1.9.0amzn1.0. • Fügen Sie die Option `--minimal` hinzu, um nur das EFA-Kernelmodul zu installieren und `rdma-core` zu installieren.	Dezember 2019
1.7.1	• Aktualisieren Sie Libfabric auf Version 1.8.1amzn1.3.	Dezember 2019
1.7.0	• Fügen Sie die Libfabric-Moduldatei hinzu. • Aktualisieren Sie Libfabric auf Version 1.8.1amzn1.1.	November 2019
1.6.2	• Aktualisieren Sie Open MPI auf Version 1.6.2.	Oktober 2019
1.6.1	• Aktualisieren Sie Libfabric auf Version 1.8.1amzn1.0. • Aktualisieren Sie Open MPI auf Version 4.0.1. • Aktualisieren Sie `rdma-core` auf Version 26.0.	Oktober 2019
1.5.4	• Aktualisieren Sie das EFA-Kernelmodul auf Version 1.4.1.	September 2019
1.5.3	• Aktualisieren Sie das EFA-Kernelmodul auf Version 1.3.1. • Vermeiden Sie die Installation von `kernel-devel` - oder `linux-headers` -Paketen, es sei denn, Sie installieren den Kernel-Treiber.	September 2019
1.5.1	• Konfigurieren Sie riesige Seiten nur, wenn ein EFA-Gerät vorhanden ist.	August 2019
1.5.0	• Aktualisieren Sie Libfabric auf Version 1.8.0amzn1.1. • Aktualisieren Sie `rmda-core` auf Version 25.0.	August 2019

Version	Änderungen	Datum der Veröffentlichung
1.4.1	• Fügen Sie die Bibliothekspfade (`/opt/amazon/efa/lib64` und `/opt/amazon/efa/openmpi/lib`) für Libfabric und Open MPI zu `/etc/ld.so.conf.d/efa.conf` hinzu, um sicherzustellen, dass die gemeinsam genutzten Bibliotheken von Open MPI und Libfabric korrekt gefunden werden.	Juli 2019
1.4.0	• Aktualisieren Sie das EFA-Kernelmodul auf Version 1.3.0. • Aktualisieren Sie Libfabric auf Version 1.8.0amzn1.0. • Erste Version zur Unterstützung von Intel MPI 2019 Update 4.	Juli 2019

EC2 Amazon-Topologie

Die EC2 Amazon-Topologie bietet eine hierarchische Ansicht der relativen Nähe Ihrer Rechenkapazität. Sie können diese Informationen verwenden, um die Recheninfrastruktur für High Performance Computing (HPC), maschinelles Lernen (ML) und generative KI in großem Umfang zu verwalten.

Verfügbar APIs

Amazon EC2 bietet zwei APIs zum Verständnis Ihrer EC2 Topologie:

- DescribeInstanceTopology
  - Zeigt, wo sich Ihre laufenden Instances relativ zueinander in der Netzwerkhierarchie befinden.
  - Hilft bei der Optimierung, wo Ihre Workloads auf Ihren vorhandenen Instances ausgeführt werden sollen.
- DescribeCapacityReservationTopology
  - Zeigt an, wo sich Ihre reservierten Kapazitäten relativ zueinander in der Netzwerkhierarchie befinden werden, bevor Sie Instances starten.
  - Hilft bei der Kapazitätsplanung, indem es Sie vor dem Start von Instances über die Platzierung der reservierten Kapazität informiert.

Wichtigste Vorteile

EC2 Die Topologie bietet die folgenden Hauptvorteile:

- Kapazitätsmanagement – Optimierung der Ressourcennutzung.
- Auftragsplanung – Treffen Sie fundierte Entscheidungen über die Platzierung von Workloads.
- Knotenrangfolge – Achten Sie auf die relative Nähe, um die Leistung auf eng gekoppelten Instances zu optimieren.

Überlegungen

- Topologie-Ansichten sind nur verfügbar für:
  - Instances im Status `running`
  - Kapazitätsreservierungen im Status `pending` oder `active`
- Jede Topologieansicht ist für sich einzigartig. AWS-Konto
- Das unterstützt AWS-Managementkonsole nicht die Anzeige der Topologie.
- Topologie-Informationen helfen Ihnen zwar, die Instance-Platzierung zu verstehen, Sie können sie aber nicht verwenden, um eine neue Instance in der physischen Nähe einer bereits vorhandenen Instance zu starten. Um die Instance-Platzierung zu beeinflussen, können Sie Kapazitätsreservierungen in Cluster-Placement-Gruppen erstellen.

Preisgestaltung

Für die Beschreibung Ihrer EC2 Topologie fallen keine zusätzlichen Kosten an.

Inhalt

- So funktioniert die EC2 Amazon-Topologie
- Voraussetzungen für die EC2 Amazon-Topologie
- Beispiele für die EC2 Amazon-Instance-Topologie

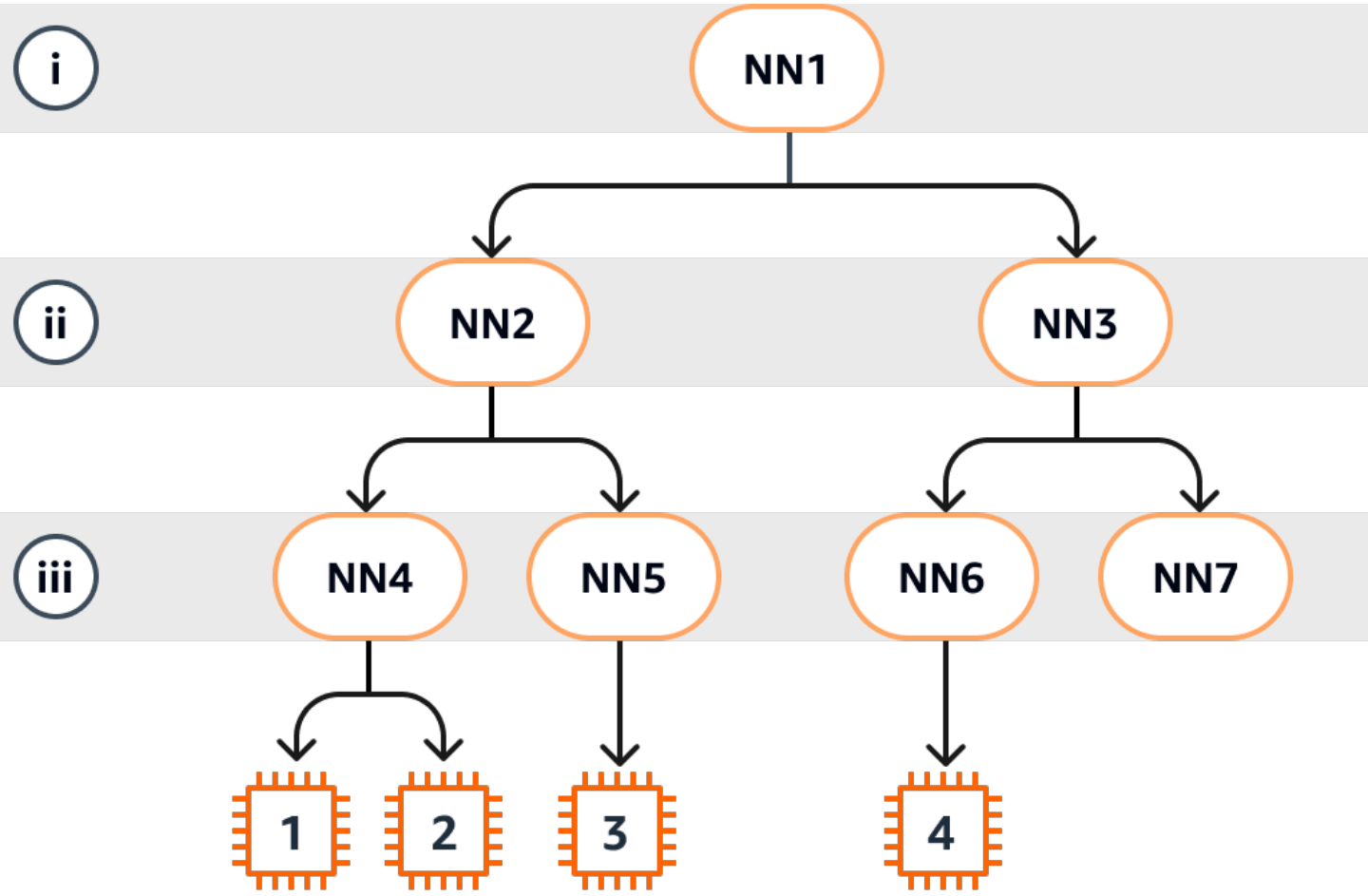
So funktioniert die EC2 Amazon-Topologie

Das AWS Netzwerk ist in einer Hierarchie von Ebenen angeordnet. EC2 Instanzen stellen je nach Instanztyp eine Verbindung zum Netzwerk auf oder unter der dritten Ebene her. Die Topologie einer Instance wird durch eine Gruppe von Knoten beschrieben, wobei sich in

jeder Netzwerkschicht ein Knoten befindet. Der in der Antwort DescribeInstanceTopologyoder der DescribeCapacityReservationTopologyAPI festgelegte Knoten bietet eine Ansicht der Netzwerkhierarchie von oben nach unten, wobei der unterste Knoten mit einer Instanz verbunden ist.

> **Note**
>
> Einige Instance-Typen bestehen aus 4 Netzwerkknoten in einem Knotensatz, der 4 Schichten im Netzwerk repräsentiert, während andere aus 3 Netzwerkknoten bestehen, die 3 Schichten im Netzwerk repräsentieren. Weitere Informationen zu den unterstützten Instance-Typen finden Sie unter Instance-Typen.
> Je nach der Art der Kapazitätsreservierung werden möglicherweise nur 1, 2 oder 3 Netzwerkknoten angezeigt.

Das folgende Diagramm bietet eine visuelle Darstellung, anhand derer Sie die EC2 Topologie verstehen können. Die Netzwerkknoten werden als NN1— NN7identifiziert. Die Angaben i, ii und iii identifizieren die verschiedenen Netzwerkschichten. Die Zahlen 1, 2, 3 und 4 identifizieren die EC2 Instanzen. Instances stellen eine Verbindung mit einem Knoten in der untersten Schicht her, wie im folgenden Diagramm als iii identifiziert. Mehrere Instances können eine Verbindung mit dem gleichen Knoten herstellen.



In diesem Beispiel:

- Instanz 1 stellt eine Verbindung zum Netzwerkknoten 4 (NN4) in Schicht III her. NN4 stellt eine Verbindung zu Netzwerkknoten 2 (NN2) in Schicht ii NN2 her und stellt eine Verbindung zu Netzwerkknoten 1 (NN1) in Schicht i her, der in diesem Beispiel an der Spitze der Netzwerkhierarchie steht. Der Netzwerkknotensatz umfasst NN1 NN2, und NN4, hierarchisch ausgedrückt von den oberen Schichten bis zur unteren Schicht.
- Instanz 2 stellt auch eine Verbindung zum Netzwerkknoten 4 (NN4) her. Instanz 1 und Instanz 2 teilen sich den gleichen Netzwerkknotensatz: NN1 NN2, und NN4.
- Instanz 3 stellt eine Verbindung mit Netzwerkknoten 5 (NN5) her. NN5 stellt eine Verbindung zu NN2 her und NN2 stellt eine Verbindung zu her NN1. Der Netzwerkknotensatz für Instanz 3 ist NN1, NN2, und NN5.
- Instanz 4 stellt eine Verbindung zum Netzwerkknoten 6 (NN6) her. Ihr Netzwerkknotensatz ist NN1, NN3, und NN6.

Betrachtet man die Nähe der Instanzen 1, 2 und 3, liegen die Instanzen 1 und 2 näher beieinander, weil sie mit demselben Netzwerkknoten (NN4) verbunden sind, während Instanz 3 weiter entfernt ist, weil sie eine Verbindung zu einem anderen Netzwerkknoten (NN5) herstellt.

Betrachtet man die Nähe aller Instanzen in diesem Diagramm, liegen die Instanzen 1, 2 und 3 näher beieinander als Instanz 4, da sie sich ihren Netzwerkknotensatz teilen NN2 .

Faustregel: Wenn zwei beliebige Instances mit dem gleichen Netzwerkknoten verbunden sind, befinden sie sich physisch nahe beieinander (wie bei den Instances 1 und 2). Außerdem gilt: Je weniger Hops zwischen Netzwerkknoten liegen, desto näher sind die Instances beieinander. Beispielsweise haben die Instanzen 1 und 3 weniger Hops zu einem gemeinsamen Netzwerkknoten (NN2) als zu dem Netzwerkknoten (NN1), den sie mit Instanz 4 gemeinsam haben, und liegen daher näher beieinander als an Instanz 4.

In diesem Beispiel werden keine Instanzen unter Netzwerkknoten 7 (NN7) ausgeführt, weshalb die API-Ausgabe nicht enthalten ist NN7.

Wie interpretiert man die DescribeInstanceTopology Ausgabe

Sie können die Instanztopologie mithilfe der DescribeInstanceTopologyAPI beschreiben. Die Ausgabe enthält eine hierarchische Ansicht der zugrunde liegenden Netzwerktopologie für eine Instance.

Die folgende Beispielausgabe entspricht den Netzwerktopologie-Informationen der vier Instances aus dem vorherigen Diagramm. Für dieses Beispiel wurden der Beispielausgabe Kommentare hinzugefügt.

Beachten Sie folgende wichtige Informationen in der Ausgabe:

- `NetworkNodes` beschreibt den Netzwerkknotensatz einer einzelnen Instance.
- In jedem Netzwerkknotensatz sind die Netzwerkknoten absteigend in hierarchischer Reihenfolge aufgeführt.
- Der mit der Instance verbundene Netzwerkknoten ist der letzte Netzwerkknoten in der Liste (die unterste Schicht).
- Um zu ermitteln, welche Instances nahe beieinander liegen, suchen Sie zuerst nach gemeinsamen Netzwerkknoten in der untersten Schicht. Wenn es in der untersten Schicht keine gemeinsamen Netzwerkknoten gibt, suchen Sie nach gemeinsamen Netzwerkknoten in den oberen Schichten.

In der folgenden Beispielausgabe befinden sich `i-1111111111example` und `i-2222222222example` am nächsten beieinander (verglichen mit den anderen Instances des Beispiels), da sie den Netzwerkknoten `nn-4444444444example` in der untersten Schicht gemeinsam haben.

> **Note**
>
> Die Antwort enthält 3 oder mehr Netzwerkknoten. Mehr Informationen zur Anzahl der Netzwerkknoten in der Antwort für jeden unterstützten Instance-Typ finden Sie unter Instance-Typen.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",  //Corresponds to instance 1
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 in layer i
                "nn-2222222222example",           //Corresponds to NN2 in layer ii
                "nn-4444444444example"            //Corresponds to NN4 in layer iii -
 bottom layer, connected to the instance
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",  //Corresponds to instance 2
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
                "nn-4444444444example"            //Corresponds to NN4 - layer iii -
 connected to instance
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
```

```
            "InstanceId": "i-3333333333example",  //Corresponds to instance 3
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
                "nn-5555555555example"            //Corresponds to NN5 - layer iii -
 connected to instance
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-444444444example",  //Corresponds to instance 4
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",          //Corresponds to NN1 - layer i
                "nn-3333333333example",          //Corresponds to NN3 - layer ii
                "nn-6666666666example"           //Corresponds to NN6 - layer iii -
 connected to instance
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Wie interpretiert man die Ausgabe DescribeCapacityReservationTopology

Sie können die Topologie der Kapazitätsreservierung mithilfe der DescribeCapacityReservationTopologyAPI beschreiben. Die Ausgabe enthält eine hierarchische Ansicht der zugrunde liegenden Netzwerktopologie für die reservierte Kapazität.

Die folgende Beispielausgabe entspricht den Netzwerktopologie-Informationen aus dem vorherigen Diagramm. Für dieses Beispiel wurden der Beispielausgabe Kommentare hinzugefügt.

Beachten Sie folgende wichtige Informationen in der Ausgabe:

- `NetworkNodes` beschreibt den Netzwerkknotensatz einer einzelnen Kapazitätsreservierung.
- In jedem Netzwerkknotensatz sind die Netzwerkknoten absteigend in hierarchischer Reihenfolge aufgeführt.

- Der mit der Kapazitätsreservierung verbundene Netzwerkknoten ist der letzte Netzwerkknoten in der Liste (die unterste Schicht).
- Um zu ermitteln, ob Kapazitätsreservierungen nahe beieinander liegen, suchen Sie zuerst nach gemeinsamen Netzwerkknoten in der untersten Schicht in der Ausgabe. Wenn es in der untersten Schicht keine gemeinsamen Netzwerkknoten gibt, suchen Sie nach gemeinsamen Netzwerkknoten in den oberen Schichten.

In der folgenden Beispielsausgabe befindet sich `cr-1111111111example` am Standort `nn-2222222222example` und `cr-2222222222example` befindet sich auf `nn-3333333333example`. Da sich die Kapazitätsreservierungen auf verschiedenen Netzwerkknoten in `layer ii` befinden, ist die Kommunikation von Instances in einer Kapazitätsreservierung zu Instances in der anderen Kapazitätsreservierung ineffizient.

> **Note**
>
> Die Antwort enthält je nach Art der Kapazitätsreservierung 1, 2 oder 3 Netzwerkknoten.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1111111111example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",      //Corresponds to NN1 - layer i
                "nn-2222222222example"       //Corresponds to NN2 - layer ii
                // Visibility of additional nodes requires an instance launch and
                // the DescribeInstanceTopology API
            ],
            "AvailabilityZone": "us-west-2a"
        },
        {
            "CapacityReservationId": "cr-2222222222example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",      //Corresponds to NN1 - layer i
```

```
                "nn-3333333333example"       //Corresponds to NN3 - layer ii
                // Visibility of additional nodes requires an instance launch and
                // the DescribeInstanceTopology API
            ],
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Unterschiede zwischen und DescribeInstanceTopology DescribeCapacityReservationTopology

In der folgenden Tabelle werden die wichtigsten Unterschiede zwischen DescribeInstanceTopology und verglichen DescribeCapacityReservationTopology APIs:

Vergleichspunkt	DescribeInstanceTopology	DescribeCapacityReservation Topology
Nutzungsphase	Nach dem Start (Ausführu ngsmodus)	Vor dem Start (Planungs- und Verwaltungsmodus)
Hauptzweck	Workloads auf laufenden Instances optimieren	Kapazitätsplanung und Verwaltung der Kapazität sreservierung (Zusammen führen, Teilen, Zuweisen) vor dem Start der Instance
Anzahl der Netzwerkknoten	Zeigt alle Knoten für eine laufende Instance an. Wenn sich die Instance in einer Kapazitätsreservierung befindet, entsprechen die ersten Knoten der entsprech enden Kapazitätsreservie rungs-Topologie, gefolgt von weiteren Knoten, die eine Verbindung zur Instance herstellen.	Zeigt einen Teil der Knoten an, die je nach Status (`pending` oder `active`) und Typ der Kapazitätsreservierung variieren.*

Vergleichspunkt	DescribeInstanceTopology	DescribeCapacityReservationTopology
Status	Instances müssen sich im Status `running` befinden	Kapazitätsreservierungen müssen im Status `pending` oder `active` sein
Anwendungsfälle	• Optimierung von Workloads • Leistungsoptimierung • Analyse der Laufzeit-Topologie	• Kapazitätsplanung • Verwaltung von Kapazitätsreservierungen (merge/split/assign) • Topologie-Bewertung vor dem Start

* Bei Kapazitätsblöcken für Ultraserver ist der Netzwerkknotensatz derselbe wie bei der Beschreibung der Topologie für eine `active`-Kapazitätsreservierung oder deren laufende Instance.

Voraussetzungen für die EC2 Amazon-Topologie

Um Ihre EC2 Amazon-Topologie zu beschreiben, stellen Sie sicher, dass Ihre Instances und Kapazitätsreservierungen die folgenden Voraussetzungen erfüllen.

Voraussetzungen für:

- AWS-Regionen
- Instance-Typen
- Status
- IAM-Berechtigungen

AWS-Regionen

Unterstützt AWS-Regionen:

- USA Ost (Nord-Virginia), USA Ost (Ohio), USA West (Nordkalifornien), USA West (Oregon)
- Afrika (Kapstadt)

- Asien-Pazifik (Jakarta), Asien-Pazifik (Hongkong), Asien-Pazifik (Hyderabad), Asien-Pazifik (Melbourne), Asien-Pazifik (Mumbai), Asien-Pazifik (Osaka), Asien-Pazifik (Seoul), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Asien-Pazifik (Tokio)
- Kanada (Zentral)
- Europa (Frankfurt), Europa (Irland), Europa (London), Europa (Paris), Europa (Spanien), Europa (Stockholm), Europa (Zürich)
- Israel (Tel Aviv)
- Naher Osten (Bahrain), Naher Osten (UAE)
- Südamerika (São Paulo)
- AWS GovCloud (US-West)

Die DescribeCapacityReservationTopology API wird in Israel (Tel Aviv) und AWS GovCloud (US-West) nicht unterstützt.

Instance-Typen

Unterstützte Instance-Typen:

- Gibt in der Antwort 3* Netzwerkknoten zurück
  - `g6e.xlarge` | `g6e.2xlarge` | `g6e.4xlarge` | `g6e.8xlarge` | `g6e.12xlarge` | `g6e.16xlarge` | `g6e.24xlarge` | `g6e.48xlarge`
  - `hpc6a.48xlarge` | `hpc6id.32xlarge` | `hpc7a.12xlarge` | `hpc7a.24xlarge` | `hpc7a.48xlarge` | `hpc7a.96xlarge` | `hpc7g.4xlarge` | `hpc7g.8xlarge` | `hpc7g.16xlarge`
  - `p3dn.24xlarge` | `p4d.24xlarge` | `p4de.24xlarge` | `p5.48xlarge` | `p5e.48xlarge` | `p5en.48xlarge` | `p6e-gb200.36xlarge`
  - `trn1.2xlarge` | `trn1.32xlarge` | `trn1n.32xlarge` | `trn2.48xlarge` | `trn2u.48xlarge`
- Gibt in der Antwort 4* Netzwerkknoten zurück
  - `p6-b200.48xlarge` | `p6-b300.48xlarge`

* Die Anzahl der zurückgegebenen Netzwerkknoten gilt nur bei Verwendung der DescribeInstanceTopology API. Bei der DescribeCapacityReservationTopology API variiert die Anzahl der zurückgegebenen Netzwerkknoten je nach Art und Status der Kapazitätsreservierung.

Die verfügbaren Instance-Typen variieren je nach Region. Weitere Informationen finden Sie unter EC2 Amazon-Instance-Typen nach Regionen.

Status

- Für `DescribeInstanceTopology` – Instances müssen sich im Status `running` befinden.
- Für `DescribeCapacityReservationTopology` – Kapazitätsreservierungen müssen sich im Status `pending` oder `active` befinden.

Sie können keine Informationen zur Topologie für Instances oder Kapazitätsreservierungen in einem anderen Status abrufen.

IAM-Berechtigungen

Ihre IAM-Identität (Benutzer, Gruppe oder Rolle) erfordert die folgenden Berechtigungen:

- `ec2:DescribeInstanceTopology`
- `ec2:DescribeCapacityReservationTopology`

Beispiele für die EC2 Amazon-Instance-Topologie

Sie können den describe-instance-topologyBefehl verwenden, um die Topologie für Ihre EC2 Instances zu beschreiben. Sie können auch den Befehl describe-capacity-reservation-topology verwenden, um die Topologie Ihrer Kapazitätsreservierungen zu beschreiben.

Wenn Sie den Befehl `describe-instance-topology` oder `describe-capacity-reservation-topology` ohne Parameter oder Filter verwenden, umfasst die Antwort alle Ihre Instances oder Kapazitätsreservierungen (je nachdem, welchen Befehl Sie verwendet haben), die den unterstützten Instance-Typen für diesen Befehl in der angegebenen Region entsprechen. Sie können die Region angeben, indem Sie den `--region`-Parameter einschließen oder eine Standardregion festlegen. Weitere Informationen zum Festlegen einer Standardregion finden Sie unter Wählen Sie eine Region für Ihre EC2 Amazon-Ressourcen.

Sie können Parameter angeben, um Instances oder Kapazitätsreservierungen zurückzugeben, die den angegebenen Instance- oder Kapazitätsreservierungs IDs - oder Platzierungsgruppennamen entsprechen. Sie können auch Filter einschließen, um Instances oder Kapazitätsreservierungen zurückzugeben, die einem angegebenen Instance-Typ oder einer angegebenen Instance-

Familie entsprechen, oder Instances in einer angegebenen Availability Zone oder Local Zone. Sie können einen einzelnen Parameter oder Filter oder eine Kombination aus Parametern und Filtern einschließen.

Die Ausgabe ist paginiert und umfasst standardmäßig bis zu 20 Instances oder Kapazitätsreservierungen pro Seite. Mit dem Parameter `--max-results` können Sie bis zu 100 Instances oder Kapazitätsreservierungen pro Seite angeben.

Weitere Informationen erhalten Sie unter describe-instance-topology und describe-reservation-topology-topology.

Erforderliche Berechtigungen

Die folgenden Berechtigungen sind erforderlich:

- `ec2:DescribeInstanceTopology` – Zur Beschreibung der Instance-Topologie
- `ec2:DescribeCapacityReservationTopology` – Zur Beschreibung der Topologie der Kapazitätsreservierung

Beispiele

- Beispiel 1: DescribeInstanceTopology — Instanz IDs
- Beispiel 2: DescribeInstanceTopology - Parameter für den Namen der Platzierungsgruppe
- Beispiel 3: DescribeInstanceTopology - Filter für den Instanztyp
  - Beispiel 3a — Filter mit exakter Übereinstimmung für einen bestimmten Instance-Typ
  - Beispiel 3b — Platzhalterfilter für eine Instance-Familie
  - Beispiel 3c — Kombinierter Instance-Familien- und Exact-Match-Filter
- Beispiel 4: DescribeInstanceTopology - Zonen-ID-Filter
  - Beispiel 4a — Filter für die Verfügbarkeitszone
  - Beispiel 4b — Lokaler Zonenfilter
  - Beispiel 4c — Kombinierte Filter für Availability Zone und Local Zone
- Beispiel 5: DescribeInstanceTopology - Instanztyp- und Zonen-ID-Filter
- Beispiel 6: DescribeCapacityReservationTopology - Kapazitätsreservierung IDs
- Beispiel 7: DescribeCapacityReservationTopology — Filter für den Instanztyp

Beispiel 1: DescribeInstanceTopology — Instanz IDs

AWS CLI

So beschreiben Sie die Topologie angegebener Instances

Verwenden Sie den Befehl describe-instance-topology mit dem Parameter `--instance-ids`. Die Ausgabe umfasst nur die Instanzen, die der angegebenen Instanz entsprechen IDs.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --instance-ids i-1111111111example i-2222222222example
```

Es folgt eine Beispielausgabe.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
```

```
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

So beschreiben Sie die Topologie angegebener Instances

Verwenden Sie das cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -InstanceId i-1111111111example, i-2222222222example
```

Beispiel 2: DescribeInstanceTopology - Parameter für den Namen der Platzierungsgruppe

AWS CLI

So beschreiben Sie die Topologie von Instances in einer bestimmten Placement-Gruppe

Verwenden Sie den Befehl describe-instance-topology mit dem Parameter `group-names`. Die Ausgabe enthält nur die Instances, die sich in einer der angegebenen Placement-Gruppen befinden.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --group-names ML-group HPC-group
```

Es folgt eine Beispielausgabe.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
```

```
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

So beschreiben Sie die Topologie von Instances in einer bestimmten Placement-Gruppe

Verwenden Sie das cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -GroupName ML-group, HPC-group
```

Beispiel 3: DescribeInstanceTopology - Filter für den Instanztyp

Sie können nach einem angegebenen Instance-Typ (exakte Übereinstimmung) oder nach einer Instance-Familie (mit einem Platzhalter) filtern. Sie können auch einen Filter für einen angegebenen Instance-Typ und einen Filter für eine Instance-Familie miteinander kombinieren.

Beispiel 3a — Filter mit exakter Übereinstimmung für einen bestimmten Instance-Typ

AWS CLI

So beschreiben Sie die Topologie von Instances mit einem bestimmten Instance-Typ

Verwenden Sie den Befehl describe-instance-topology mit dem Filter `instance-type`. Die Ausgabe enthält nur die Instances, die dem angegebenen Instance-Typ entsprechen.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1n.32xlarge
```

Es folgt eine Beispielausgabe.

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

So beschreiben Sie die Topologie von Instances mit einem bestimmten Instance-Typ

Verwenden Sie das cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="instance-type"; Values="trn1n.32xlarge"}
```

Beispiel 3b — Platzhalterfilter für eine Instance-Familie

AWS CLI

So beschreiben Sie die Topologie von Instances mit einer bestimmten Instance-Familie

Verwenden Sie den Befehl describe-instance-topology mit dem Filter `instance-type`. Die Ausgabe enthält nur die Instances, die der angegebenen Instance-Familie entsprechen.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1*
```

Es folgt eine Beispielausgabe.

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1212121212example",
                "nn-1211122211example",
                "nn-1311133311example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az4",
            "AvailabilityZone": "us-west-2d"
        },
        {
            "InstanceId": "i-444444444example",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-5434334334example",
                "nn-1235301234example"
            ],
```

```
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

So beschreiben Sie die Topologie von Instances mit einer bestimmten Instance-Familie

Verwenden Sie das cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="instance-type"; Values="trn1*"}
```

Beispiel 3c — Kombinierter Instance-Familien- und Exact-Match-Filter

AWS CLI

So beschreiben Sie die Topologie von Instances mit einer Instance-Familie oder einem Instance-Typ

Verwenden Sie den Befehl describe-instance-topology mit dem Filter `instance-type`. Die Ausgabe enthält nur die Instances, die den angegebenen Kriterien entsprechen.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge"
```

Es folgt eine Beispielausgabe.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
```

```
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-4343434343example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

So beschreiben Sie die Topologie von Instances mit einer Instance-Familie oder einem Instance-Typ

Verwenden Sie das cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="instance-type"; Values="p4d*", "trn1n.32xlarge"}
```

Beispiel 4: DescribeInstanceTopology - Zonen-ID-Filter

Mit dem Filter `zone-id` können Sie nach einer Availability Zone oder nach einer lokalen Zone filtern. Sie können auch einen Availability-Zone-Filter und einen Filter für die lokale Zone miteinander kombinieren.

Beispiel 4a — Filter für die Verfügbarkeitszone

AWS CLI

So beschreiben Sie die Topologie von Instances in einer bestimmten Availability Zone

Verwenden Sie den Befehl describe-instance-topology mit dem Filter `zone-id`. Die Ausgabe enthält nur Instances in der angegebenen Availability Zone.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1
```

Es folgt eine Beispielausgabe.

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

So beschreiben Sie die Topologie von Instances in einer bestimmten Availability Zone

Verwenden Sie das cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="zone-id"; Values="use1-az1"}
```

Beispiel 4b — Lokaler Zonenfilter

AWS CLI

So beschreiben Sie die Topologie von Instances in einer bestimmten Local Zone

Verwenden Sie den Befehl describe-instance-topology mit dem Filter `zone-id`. Die Ausgabe enthält nur Instances in der angegebenen Local Zone.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-atl2-az1
```

Es folgt eine Beispielausgabe.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

So beschreiben Sie die Topologie von Instances in einer bestimmten Local Zone

Verwenden Sie das cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="zone-id"; Values="use1-atl2-az1"}
```

Beispiel 4c — Kombinierte Filter für Availability Zone und Local Zone

AWS CLI

So beschreiben Sie die Topologie von Instances in einer bestimmten Zone

Verwenden Sie den Befehl describe-instance-topology mit dem Filter `zone-id`. Die Ausgabe enthält nur die Instances, die sich in einer der angegebenen Zonen befinden.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1,use1-atl2-az1
```

Es folgt eine Beispielausgabe.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
```

```
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

So beschreiben Sie die Topologie von Instances in einer bestimmten Zone

Verwenden Sie das cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="zone-id"; Values="use1-az1", "use1-atl2-az1"}
```

Beispiel 5: DescribeInstanceTopology - Instanztyp- und Zonen-ID-Filter

Sie können Filter in einem einzelnen Befehl miteinander kombinieren.

AWS CLI

So beschreiben Sie die Topologie von Instances mit bestimmten Instance-Typen, Instance-Familien und Zonen

Verwenden Sie den Befehl describe-instance-topology mit den Filtern `instance-type` und `zone-id`. Die Antwort enthält alle Instances mit einem der angegebenen Instance-Typen, die sich in einer der angegebenen Zonen befinden.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge" \
              "Name=zone-id,Values=use1-az1,use1-atl2-az1"
```

Es folgt eine Beispielausgabe.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
```

```
                "nn-3333333333example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "CapacityBlockId": "null",
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

So beschreiben Sie die Topologie von Instances mit bestimmten Instance-Typen, Instance-Familien und Zonen

Verwenden Sie das cmdlet Get-EC2InstanceTopology.

```
Get-EC2InstanceTopology `
    -Filter @{Name="instance-type"; Values="p4d*", "trn1n.32xlarge"} `
            @{Name="zone-id"; Values="use1-az1", "use1-atl2-az1"}
```

Beispiel 6: DescribeCapacityReservationTopology - Kapazitätsreservierung IDs

AWS CLI

So beschreiben Sie die Topologie bestimmter Kapazitätsreservierungen

Verwenden Sie den Befehl describe-capacity-reservation-topology mit dem Parameter `capacity-reservation-id`. Die Ausgabe umfasst nur die Kapazitätsreservierungen, die der angegebenen Kapazitätsreservierung entsprechen IDs.

```
aws ec2 describe-capacity-reservation-topology \
    --region us-east-1 \
    --capacity-reservation-id cr-1111111111example cr-2222222222example
```

Es folgt eine Beispielausgabe.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1111111111example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "p5.48xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example"
            ],
            "AvailabilityZone": "us-east-1a"
        },
        {
            "CapacityReservationId": "cr-2222222222example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "p5en.48xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example"
            ],
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

So beschreiben Sie die Topologie bestimmter Kapazitätsreservierungen

Verwenden Sie das cmdlet Get-EC2CapacityReservationTopology.

```
Get-EC2CapacityReservationTopology `
    -CapacityReservationId cr-1111111111example cr-2222222222example
```

Beispiel 7: DescribeCapacityReservationTopology — Filter für den Instanztyp

Sie können nach einem angegebenen Instance-Typ (exakte Übereinstimmung) oder nach einer Instance-Familie (mit einem Platzhalter) filtern. Sie können auch einen Filter für einen angegebenen Instance-Typ und einen Filter für eine Instance-Familie miteinander kombinieren.

AWS CLI

So beschreiben Sie die Topologie von Kapazitätsreservierungen mit einem bestimmten Instance-Typ

Verwenden Sie den Befehl describe-capacity-reservation-topology mit dem Filter `instance-type`. Die Antwort enthält alle Instances mit dem angegebenen Instance-Typ.

```
aws ec2 describe-capacity-reservation-topology \
    --region us-east-1 \
    --filters Name=instance-type,Values=p5en.48xlarge
```

Es folgt eine Beispielausgabe.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-2222222222example",
            "CapacityBlockId": "null",
            "State": "active",
            "InstanceType": "p5en.48xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example"
            ],
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

PowerShell

So beschreiben Sie die Topologie von Kapazitätsreservierungen mit einem bestimmten Instance-Typ

Verwenden Sie das cmdlet Get-EC2CapacityReservationTopology.

```
Get-EC2CapacityReservationTopology `
    -Filter @{Name="instance-type"; Values="p5en.48xlarge"}
```

Platzierungsgruppen für Ihre Amazon-EC2-Instances

Um den Anforderungen Ihres Workloads nachzukommen, können Sie eine Gruppe von untereinander abhängigen EC2-Instances in eine Placement-Gruppe starten, um ihre Platzierung zu beeinflussen.

Je nach Art des Workloads können Sie eine Placement-Gruppe mithilfe einer der folgenden Platzierungsstrategien erstellen:

- Cluster – Verpackt Instances nahe zusammen in einer Availability Zone. Mit dieser Strategie können Workloads die Netzwerkleistung mit geringer Latenz erreichen, die für eine eng gekoppelte Knoten-zu-Knoten-Kommunikation erforderlich ist, wie sie für High-Performance Computing (HPC)-Anwendungen typisch ist.
- Partition – Verteilt Instances auf logische Partitionen und gewährleistet dabei, dass Gruppen von Instances in einer Partition keine zugrunde liegende Hardware mit Instances in anderen Partitionen teilen. Diese Strategie wird in der Regel für große verteilte und replizierte Workloads wie Hadoop, Cassandra und Kafka verwendet.
- Spread – Verteilt eine kleine Gruppe von Instances strikt über verschiedene zugrundeliegende Hardware, um korrelierte Fehler zu reduzieren.

Placement-Gruppen sind optional. Wenn Sie eine neue EC2-Instance starten, versucht der EC2-Service die Instance auf eine Weise zu platzieren, dass alle Ihre Instances über die zugrundeliegende Hardware verbreitet werden, um korrelierte Fehler zu minimieren.

Preisgestaltung

Für die Erstellung einer Placement-Gruppe fallen keine Gebühren an.

Regeln und Einschränkungen

Beachten Sie vor der Verwendung von Placement-Gruppen die folgenden Regeln:

- Eine Instance kann jeweils einer Platzierungsgruppe zugeordnet werden. Sie können eine Instance nicht mehreren Platzierungsgruppen zuordnen.

- Es ist nicht möglich, Placement-Gruppen zusammenzuführen.
- On-Demand-Kapazitätsreservierungen und zonale Reserved Instances ermöglichen eine Kapazitätsreservierung für EC2-Instances in Availability Zones. Wenn Sie eine Instance starten und die Instance-Attribute denen entsprechen, die in einer On-Demand-Kapazitätsreservierung oder einer zonalen Reserved Instance angegeben wurden, wird die reservierte Kapazität automatisch von der Instance verwendet. Dies gilt auch, wenn Sie die Instance in eine Platzierungsgruppe starten.
- Sie können Dedicated Hosts nicht in Placement-Gruppen starten.
- Sie können keine Spot-Instance starten, die so konfiguriert ist, dass sie bei einer Unterbrechung in einer Platzierungsgruppe angehalten oder in den Ruhezustand versetzt wird.

Inhalt

- Platzierungsstrategien für Ihre Platzierungsgruppen
- Eine Platzierungsgruppe für Ihre EC2-Instances erstellen
- Platzierung für eine EC2-Instance ändern
- Erstellen einer Platzierungsgruppe
- Freigegebene Platzierungsgruppen
- Platzierungsgruppen auf AWS Outposts

Platzierungsstrategien für Ihre Platzierungsgruppen

Sie können eine Platzierungsgruppe für Ihre EC2-Instances mithilfe einer der folgenden Platzierungsstrategien erstellen.

Platzierungsstrategien

- Cluster Placement-Gruppen
- Partitions-Placement-Gruppen
- Spread Placement-Gruppen

Cluster Placement-Gruppen

Eine Cluster Placement-Gruppe ist eine logische Gruppierung von Instances innerhalb einer einzelnen Availability Zone. Instances sind nicht auf ein einzelnes Rack beschränkt. Eine Cluster-

Placement-Gruppe kann per Peering verbundene Virtual Private Networks (VPCs) in der gleichen Region umfassen. Instances in derselben Cluster Placement-Gruppe verfügen über ein höheres Durchsatzlimit pro Flow von bis zu 10 Gbit/s für TCP/IP-Datenverkehr und befinden sich in demselben Bandbreitensegment mit hoher Bisektion des Netzwerks.

Im folgenden Image werden Instances dargestellt, die in einer Cluster-Placement-Gruppe platziert sind.

Cluster-Placement-Gruppen sind für Anwendungen zu empfehlen, die von niedriger Netzwerklatenz, hohem Netzwerkdurchsatz oder von beidem profitieren. Sie werden auch empfohlen, wenn der Großteil des Netzwerkdatenverkehrs zwischen den Instances in der Gruppe liegt. Zur Bereitstellung der niedrigsten Latenz und höchsten Netzwerkleistung (Pakete pro Sekunde) für Ihre Placement-Gruppe sollten Sie einen Instance-Typ wählen, der Enhanced Networking unterstützt. Weitere Informationen erhalten Sie unter Enhanced Networking.

Wir empfehlen Ihnen, Ihre Instances folgendermaßen zu starten:

- Verwenden Sie eine einzelne Startanforderung, um die Anzahl der benötigten Instances in der Placement-Gruppe zu starten.
- Verwenden Sie denselben Instance-Typ für alle Instances in der Placement-Gruppe.

Wenn Sie versuchen, der Placement-Gruppe später weitere Instances hinzuzufügen oder mehr als einen Instance-Typ in der Placement-Gruppe zu starten, steigt das Risiko, dass die Kapazität nicht ausreicht und ein entsprechender Fehler auftritt.

Wenn Sie eine Instance in einer Placement-Gruppe anhalten und dann wieder starten, wird sie in der Placement-Gruppe weiterhin ausgeführt. Der Startvorgang schlägt aber fehl, wenn für die Instance nicht genügend Kapazität vorhanden ist.

Wenn Sie beim Starten einer Instance in einer Placement-Gruppe, die bereits laufende Instances enthält, einen Kapazitätsfehler erhalten, sollten Sie alle Instances der Placement-Gruppe beenden und erneut starten und dann versuchen, den Vorgang zu wiederholen. Wenn Sie die Instances starten, werden diese unter Umständen zu Hardware migriert, die über Kapazität für alle angeforderten Instances verfügt.

Regeln und Einschränkungen

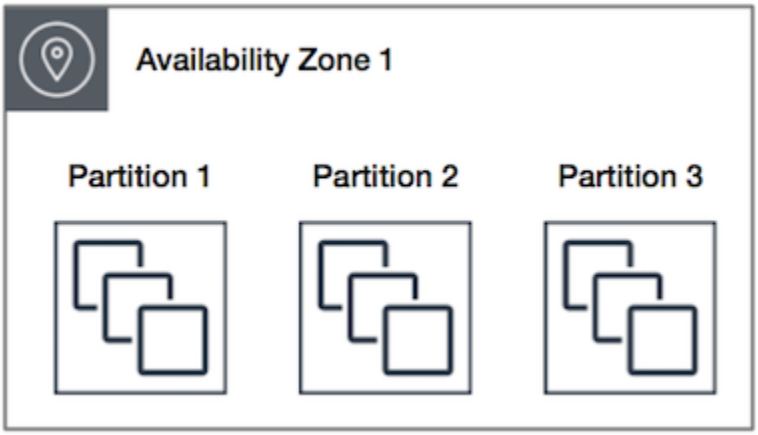
Für Cluster Placement-Gruppen gelten die folgenden Regeln:

- Die folgenden Instance-Typen werden unterstützt:
  - Instances der aktuellen Generation mit Ausnahme von Instances mit Spitzenlastleistung (z. B. T2), Mac1-Instances und M7i-flex-Instances.
  - Die folgenden Instances der vorherigen Generation: A1, C3, C4, I2, M4, R3 und R4.
- Eine Cluster Placement-Gruppe kann nicht übergreifend für mehrere Availability Zones gelten.
- Die maximale Netzwerk-Durchsatzgeschwindigkeit von Datenverkehr zwischen zwei Instances einer Cluster Placement-Gruppe richtet sich nach der langsameren der beiden Instances und ist entsprechend begrenzt. Wählen Sie für Anwendungen, die einen hohen Durchsatz erfordern, einen Instance-Typ mit einer Netzwerkkonnektivität, die Ihren Anforderungen entspricht.
- Für Instances, die Enhanced Networking unterstützen, gelten die folgenden Regeln:
  - Instances innerhalb einer Cluster Placement-Gruppe können bis zu 10 Gbit/s für Single-Flow-Verkehr verwenden. Instances außerhalb einer Cluster-Placement-Gruppe können bis zu 5 Gbit/s für Single-Flow-Verkehr verwenden.
  - Datenverkehr zu und von Amazon S3-Buckets innerhalb der gleichen Region über den öffentlichen IP-Adressraum oder durch einen VPC-Endpunkt kann die gesamte verfügbare aggregierte Bandbreite der Instance nutzen.
- In einer Cluster Placement-Gruppe können mehrere Instance-Typen gestartet werden. Dadurch verringert sich aber die Wahrscheinlichkeit, dass die erforderliche Kapazität vorhanden und der Startvorgang erfolgreich ist. Wir empfehlen Ihnen, für alle Instances einer Cluster Placement-Gruppe den gleichen Instance-Typ zu verwenden.
- Wir empfehlen Ihnen, die Kapazität explizit in der Cluster-Placement-Gruppe zu reservieren, indem Sie eine On-Demand-Kapazitätsreservierung in der Cluster-Placement-Gruppe anlegen. Beachten Sie, dass Sie mit zonalen Reserved Instances keine Kapazität reservieren können, da sie Kapazität nicht explizit in einer Platzierungsgruppe reservieren können.
- Netzwerkverkehr in das Internet und über eine Direct Connect-Verbindung zu On-Premises-Ressourcen ist auf 5 Gbit/s für Cluster-Placement-Gruppen beschränkt.

Partitions-Placement-Gruppen

Partitions-Placement-Gruppen tragen zu einer verringerten Wahrscheinlichkeit korrelierter Hardwarefehler für Ihre Anwendung bei. Beim Verwenden von Partitions-Placement-Gruppen unterteilt Amazon EC2 jede Gruppe in logische Segmente, die als Partitionen bezeichnet werden. Amazon EC2 stellt sicher, dass jede Partition in einer Placement-Gruppe über einen eigenen Satz von Racks verfügt. Dabei verfügt jedes Rack über sein eigenes Netzwerk und seine eigene Stromquelle. Da keine der Partitionen innerhalb einer Placement-Gruppe dieselben Racks nutzen, können die Auswirkung von Hardwarefehlern auf Ihre Anwendungen reduziert werden.

Das folgende Image ist eine einfache visuelle Darstellung einer Partition-Placement-Gruppe in einer einzelnen Availability Zone. Es zeigt Instances in einer Partition-Placement-Gruppe mit drei Partitionen – Partition 1, Partition 2 und Partition 3. Jede Partition umfasst mehrere Instances. Die Instances in der jeweiligen Partition nutzen keine Racks mit den Instances in den anderen Partitionen gemeinsam. Die Auswirkungen eines einzelnen Hardwarefehlers werden somit auf nur die zugehörige Partition eingeschränkt.



Partitions-Placement-Gruppen können verwendet werden, um große verteilte und replizierte Workloads, wie beispielsweise HDFS, HBase und Cassandra, auf unterschiedlicher Hardware bereitzustellen. Wenn Sie Instances in einer Partition-Placement-Gruppe starten, versucht Amazon EC2, die Instances gleichmäßig auf die Anzahl der von Ihnen angegebenen Partitionen zu verteilen. Sie können Instances auch in einer bestimmten Partition starten, um eine bessere Kontrolle darüber zu haben, wo die Instances platziert werden.

Eine Partition-Placement-Gruppe kann Partitionen in mehreren Availability Zones in der gleichen Region umfassen. Eine Partition-Placement-Gruppe kann maximal sieben Partitionen pro Availability Zone aufweisen. Die Anzahl von Instances, die in einer Partition-Placement-Gruppe gestartet werden können, ist nur durch die Begrenzungen in Ihrem Konto limitiert.

Partitions-Placement-Gruppen bieten außerdem Einsicht in die Partitionen. Sie können sehen, welche Instances sich in welchen Partitionen befinden. Sie können diese Angaben an topologiegestützte Anwendungen wie HDFS, HBase und Cassandra übermitteln, die anhand dieser Informationen intelligente Datenreplikationsentscheidungen zur Steigerung der Verfügbarkeit und Lebensdauer von Daten treffen.

Wenn Sie eine Instance in einer Partitions-Placement-Gruppe starten und es nicht genügend eindeutige Hardware zur Erfüllung der Anforderung gibt, schlägt die Anforderung fehl. Amazon EC2 stellt mit der Zeit mehr eindeutig identifizierbare Hardware zur Verfügung, sodass Sie die Anforderung später erneut versuchen können.

Regeln und Einschränkungen

Für Partitions-Placement-Gruppen gelten die folgenden Regeln:

- Eine Partition-Placement-Gruppe unterstützt maximal sieben Partitionen pro Availability Zone. Die Anzahl von Instances, die Sie in einer Partition-Placement-Gruppe starten können, ist nur durch die Begrenzungen in Ihrem Konto limitiert.
- Wenn Instances in einer Partitions-Placement-Gruppe gestartet werden, versucht Amazon EC2, die Instances gleichmäßig auf alle Partitionen zu verteilen. Amazon EC2 garantiert keine gleichmäßige Verteilung von Instances auf alle Partitionen.
- Eine Partition-Placement-Gruppe mit Dedicated Instances kann maximal zwei Partitionen umfassen.
- Kapazitätsreservierungen reservieren keine Kapazität in einer Partition-Placement-Gruppe.

Spread Placement-Gruppen

Eine Spread-Placement-Gruppe ist eine Gruppe von Instances, die jeweils auf einer bestimmten Hardware platziert werden.

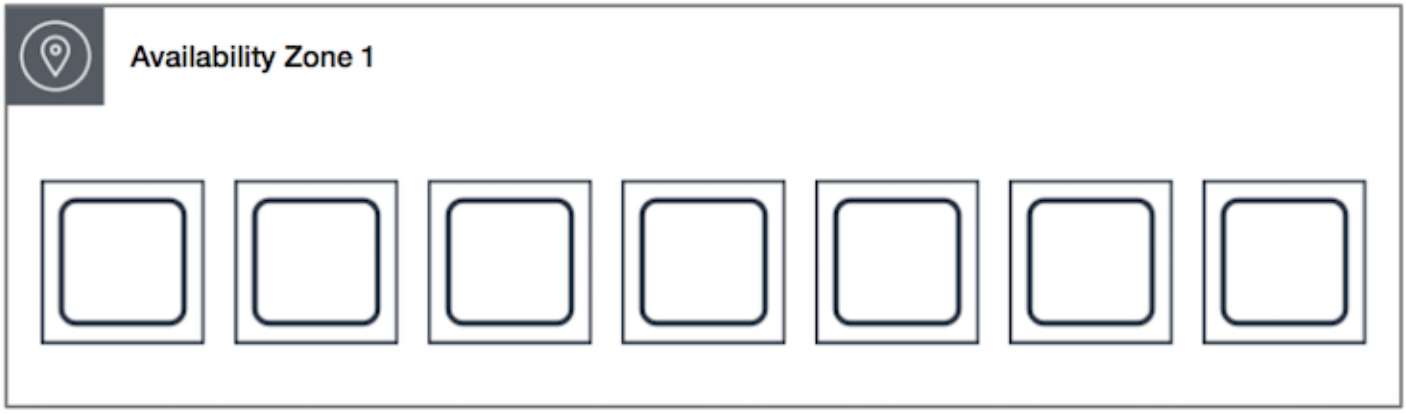
Spread Placement-Gruppen werden für Anwendungen mit einer geringen Anzahl kritischer Instances empfohlen, die getrennt voneinander gehalten werden sollten. Das Launchen von Instances in einer Placement-Gruppe auf Spread-Ebene reduziert das Risiko gleichzeitiger Ausfälle, die auftreten können, wenn Instances dieselbe Ausstattung nutzen. Placement-Gruppen auf Spread-Ebene bieten Zugriff auf separate Hardware und eignen sich daher für die Vermischung von Instance-Typen oder das Launchen über eine Zeit hinweg.

Wenn Sie eine Instance in einer Spread-Placement-Gruppe starten und es nicht genügend eindeutige Hardware zur Erfüllung der Anforderung gibt, schlägt die Anforderung fehl. Amazon EC2 stellt mit

der Zeit mehr eindeutig identifizierbare Hardware zur Verfügung, sodass Sie die Anforderung später erneut versuchen können. Placement-Gruppen können Instances auf Racks oder Hosts verteilen. Spread-Placement-Gruppen auf Rack-Level können in verschiedenen AWS-Regionen und in AWS Outposts verwendet werden. Spread-Placement-Gruppen auf Host-Ebene können nur mit AWS Outposts verwendet werden.

Spread-Placement-Gruppen auf Rack-Ebene

Das folgende Image zeigt sieben Instances in einer einzelnen Availability Zone, die in einer Spread Placement-Gruppe platziert sind. Die sieben Instances sind in sieben verschiedenen Racks untergebracht, wobei jedes Rack über ein eigenes Netzwerk und eine eigene Stromquelle verfügt.



Eine Spread-Placement-Gruppe auf Rack-Ebene kann mehrere Availability Zones in derselben Region umfassen. In einer Region kann eine Spread-Placement-Gruppe auf Rack-Ebene maximal sieben laufende Instances pro Availability Zone pro Gruppe haben. Ihre Spread-Placement-Gruppe auf Rack-Ebene kann so viele Instances aufnehmen, wie Sie Racks in Ihrer Outpost-Bereitstellung haben.

Spread-Placement-Gruppen auf Host-Ebene

Spread-Placement-Gruppen auf Host-Ebene sind nur mit AWS Outposts verfügbar. Ihre Spread-Placement-Gruppe auf Host-Ebene kann so viele Instances aufnehmen, wie Sie Hosts in Ihrer Outpost-Bereitstellung haben. Weitere Informationen finden Sie unter the section called “Platzierungsgruppen auf AWS Outposts”.

Regeln und Einschränkungen

Für Spread Placement-Gruppen gelten die folgenden Regeln:

- Eine Rack-Spread-Placement-Gruppen unterstützt maximal sieben laufende Instances pro Availability Zone. In einer Region mit drei Availability Zones können Sie beispielsweise insgesamt 21 Instances in der Gruppe ausführen, mit sieben Instances in jeder Availability Zone. Wenn Sie versuchen, eine achte Instance innerhalb derselben Availability Zone und in derselben Spread Placement-Gruppe zu starten, wird die Instance nicht gestartet. Wenn Sie mehr als sieben Instances in einer Availability Zone benötigen, empfehlen wir Ihnen, mehrere Spread-Placement-Gruppen zu verwenden. Die Verwendung mehrerer Spread-Placement-Gruppen garantiert nicht die Verteilung der Instances zwischen den Gruppen, stellt aber die Verteilung für jede Gruppe sicher, um den Einfluss von bestimmten Fehlerklassen zu begrenzen.
- Spread Placement-Gruppen werden für Dedicated Instances nicht unterstützt.
- Spread-Placement-Gruppen auf Host-Ebene werden nur für Placement-Gruppe auf AWS Outposts unterstützt. Eine Spread-Placement-Gruppe auf Host-Ebene kann so viele Instances aufnehmen, wie Sie Hosts in Ihrer Outpost-Bereitstellung haben.
- In einer Region kann eine Spread-Placement-Gruppe auf Rack-Ebene maximal sieben laufende Instances pro Availability Zone pro Gruppe haben. Mit AWS Outposts kann eine Spread-Placement-Gruppen auf Rack-Ebene so viele Instances aufnehmen, wie Sie Racks in Ihrer Outpost-Bereitstellung haben.
- Kapazitätsreservierungen reservieren keine Kapazität in einer Spread-Placement-Gruppe.

Eine Platzierungsgruppe für Ihre EC2-Instances erstellen

Sie können eine Platzierungsgruppe verwenden, um die Platzierung von Instances im Verhältnis zueinander zu steuern. Nachdem Sie eine Platzierungsgruppe erstellt haben, können Sie Instances in der Platzierungsgruppe starten.

Einschränkung

Sie können in jeder Region maximal 500 Platzierungsgruppen pro Konto erstellen.

Console

Erstellen einer Platzierungsgruppe

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Placement Groups (Placement-Gruppen).
3. Wählen Sie Platzierungsgruppe erstellen.
4. Geben Sie einen Namen für die Gruppe an.

5. Wählen Sie die Platzierungsstrategie für die Gruppe: Cluster, Spread oder Partition.

   Wenn Sie Spread wählen, müssen Sie die Spread-Ebene wählen: Rack oder Host.

   Wenn Sie Partition wählen, müssen Sie die Anzahl der Partitionen für die Gruppe eingeben.
6. (Optional) Um ein Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen aus und geben Sie den Schlüssel und den Wert für das Tag ein.
7. Wählen Sie Create group (Gruppe erstellen) aus.

AWS CLI

Verwenden Sie den Befehl create-placement-group.

Eine Cluster-Placement-Gruppe erstellen

Das folgende Beispiel erstellt eine Platzierungsgruppe, welche die `cluster`-Platzierungsstrategie verwendet, und wendet ein Tag mit dem Schlüssel von `purpose` und dem Wert von `production` an.

```
aws ec2 create-placement-group \
    --group-name my-cluster \
    --strategy cluster \
    --tag-specifications 'ResourceType=placement-
group,Tags={Key=purpose,Value=production}'
```

So erstellen Sie eine Partition-Placement-Gruppe

Im folgenden Beispiel wird eine Platzierungsgruppe erstellt, welche die `partition`-Platzierungsstrategie verwendet und die fünf Partitionen mit dem `--partition-count`-Parameter angibt.

```
aws ec2 create-placement-group \
    --group-name HDFS-Group-A \
    --strategy partition \
    --partition-count 5
```

PowerShell

Verwenden Sie das cmdlet New-EC2PlacementGroup.

Eine Cluster-Placement-Gruppe erstellen

Im folgenden Beispiel wird eine Cluster-Placement-Gruppe erstellt.

```
New-EC2PlacementGroup `
    -GroupName my-placement-group `
    -Strategy cluster
```

So erstellen Sie eine Partition-Placement-Gruppe

Im folgenden Beispiel wird eine Partition-Placement-Gruppe erstellt.

```
New-EC2PlacementGroup `
    -GroupName my-placement-group `
    -Strategy partition `
    -PartitionCount 5
```

Platzierung für eine EC2-Instance ändern

Sie können die Platzierungsgruppe für eine Instance wie folgt ändern:

- Eine Instance in eine Platzierungsgruppe verschieben
- Verschieben einer Instance von einer Platzierungsgruppe in eine andere
- Entfernen einer Instance aus einer Platzierungsgruppe

Anforderung

Bevor Sie die Platzierungsgruppe für eine Instance ändern können, muss sich die Instance im Zustand `stopped` befinden.

Console

Die Instance-Platzierung ändern

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.

4. Wählen Sie Actions (Aktionen), Instance Settings (Instance-Einstellungen) und Modify Instance Placement (Instance-Platzierung ändern).
5. Führen Sie für die Platzierungsgruppe einen der folgenden Schritte aus:
   - Um die Instance zu einer Platzierungsgruppe hinzuzufügen, wählen Sie die Platzierungsgruppe aus.
   - Um die Instance von einer Platzierungsgruppe zu einer anderen zu verschieben wählen Sie die Platzierungsgruppe aus.
   - Um die Instance aus der Platzierungsgruppe zu entfernen, wählen Sie Keine aus.
6. Wählen Sie Speichern.

AWS CLI

So verschieben Sie eine Instance in eine Platzierungsgruppe

Verwenden Sie den Befehl modify-instance-placement.

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name MySpreadGroup
```

So entfernen Sie eine Instance aus einer Platzierungsgruppe

Verwenden Sie den Befehl modify-instance-placement. Wenn Sie eine leere Zeichenfolge als Namen für eine Platzierungsgruppe angeben, wird die Instance aus ihrer aktuellen Platzierungsgruppe entfernt.

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name ""
```

PowerShell

So verschieben Sie eine Instance in eine Platzierungsgruppe

Verwenden Sie das cmdlet Edit-EC2InstancePlacement mit dem Namen der Platzierungsgruppe.

```
Edit-EC2InstancePlacement `
    -InstanceId i-0123a456700123456 `
```

```
    -GroupName MySpreadGroup
```

So entfernen Sie eine Instance aus einer Platzierungsgruppe

Verwenden Sie das cmdlet Edit-EC2InstancePlacement mit einer leeren Zeichenfolge für den Namen der Platzierungsgruppe.

```
Edit-EC2InstancePlacement `
    -InstanceId i-0123a456700123456 `
    -GroupName ""
```

Erstellen einer Platzierungsgruppe

Wenn Sie eine Platzierungsgruppe ersetzen müssen oder nicht mehr benötigen, können Sie sie löschen. Bevor Sie eine Platzierungsgruppe löschen können, darf sie keine Instances enthalten. Sie können die Instances beenden, sie in eine andere Platzierungsgruppe verschieben oder sie aus der Platzierungsgruppe entfernen.

Console

So löschen Sie eine Platzierungsgruppe

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Placement Groups (Placement-Gruppen).
3. Wählen Sie die Platzierungsgruppe aus und wählen Sie Aktionen, Löschen.
4. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **Delete** ein und wählen Sie dann Löschen aus.

AWS CLI

So löschen Sie eine Platzierungsgruppe

Verwenden Sie den Befehl delete-placement-group.

```
aws ec2 delete-placement-group --group-name my-cluster
```

PowerShell

So löschen Sie eine Platzierungsgruppe

Verwenden Sie das cmdlet Remove-EC2PlacementGroup.

```
Remove-EC2PlacementGroup -GroupName my-cluster
```

Freigegebene Platzierungsgruppen

Durch die Freigabe von Platzierungsgruppen können Sie die Platzierung voneinander abhängiger Instances beeinflussen, die separaten AWS-Konten gehören. Ein Besitzer kann eine Platzierungsgruppe über mehrere AWS-Konten oder innerhalb seiner Organisation freigeben. Ein Teilnehmer kann Instances in einer Platzierungsgruppe starten, die mit seinem -Konto geteilt wird.

Ein Besitzer einer Placement-Gruppe kann eine Placement-Gruppe für folgendes freigeben:

- Spezifische AWS-Konten innerhalb oder außerhalb seiner Organisation
- eine Organisationseinheit innerhalb seiner -Organisation
- seine gesamte -Organisation

Sie können VPC-Peering verwenden, um Instances zu verbinden, die separaten AWS-Konten gehören, und die vollen Latenzvorteile nutzen, die von gemeinsam genutzten Cluster-Placement-Gruppen geboten werden.

Inhalt

- Regeln und Einschränkungen
- Erforderliche Berechtigungen
- Freigeben in mehreren Availability Zones
- Freigeben von Platzierungsgruppen
- Freigabe der Platzierungsgruppe aufheben

Regeln und Einschränkungen

Die folgenden Regeln und Einschränkungen gelten, wenn Sie eine Placement-Gruppe freigeben oder wenn eine Placement-Gruppe mit Ihnen geteilt wird.

- Um eine Placement-Gruppe freigeben zu können, müssen Sie diese in Ihrem AWS-Konto besitzen. Sie können keine Platzierungsgruppe freigeben, die für Sie freigegeben wurde.

- Wenn Sie eine Partition- oder eine Spread-Placement-Gruppe freigeben, ändern sich die Placement-Gruppenlimits nicht. Eine freigegebene Partition-Placement-Gruppe unterstützt maximal sieben Partitionen pro Availability Zone, und eine freigegebene verteilte Spread-Placement-Gruppe unterstützt maximal sieben laufende Instances pro Availability Zone.
- Um eine Platzierungsgruppe für Ihre Organisation oder eine Organisationseinheit in Ihrer Organisation freigeben zu können, müssen Sie die Freigabe mit AWS Organizations aktivieren. Weitere Informationen finden Sie unter Freigeben Ihrer AWS-Ressourcen.
- Wenn Sie die AWS-Managementkonsole zum Starten einer Instance verwenden, können Sie alle Platzierungsgruppen auswählen, die für Sie freigegeben wurden. Wenn Sie die AWS CLI zum Starten einer Instance verwenden, müssen Sie eine gemeinsam genutzte Platzierungsgruppe anhand der ID und nicht anhand des Namens angeben. Sie können den Namen der Platzierungsgruppe nur verwenden, wenn Sie der Besitzer der freigegebenen Platzierungsgruppe sind.
- Sie sind dafür verantwortlich, die Ihnen gehörenden Instances in einer freigegebenen Placement-Gruppe zu verwalten.
- Sie können Instances und Kapazitätsreservierungen, die einer gemeinsam genutzten Platzierungsgruppe zugeordnet sind, Ihnen aber nicht gehören, nicht anzeigen oder ändern.
- Der Amazon-Ressourcenname (ARN) einer Platzierungsgruppe enthält die ID des Kontos, dem die Platzierungsgruppe gehört. Sie können den Konto-ID-Teil eines Platzierungsgruppen-ARN verwenden, um den Besitzer einer Platzierungsgruppe zu identifizieren, die mit Ihnen geteilt wird.

Erforderliche Berechtigungen

Um eine Platzierungsgruppe freigeben zu können, müssen Benutzer über Berechtigungen für die folgenden Aktionen verfügen:

- `ec2:PutResourcePolicy`
- `ec2:DeleteResourcePolicy`

Freigeben in mehreren Availability Zones

Um sicherzustellen, dass Ressourcen auf die Availability Zones einer Region verteilt sind, ordnen wir Availability Zones einzeln Namen für jedes Konto zu. Dies könnte zu in mehreren Konten unterschiedlich benannten Availability Zones führen. So befindet sich die Availability Zone `us-east-1a` für Ihr AWS-Konto möglicherweise nicht im selben Ort wie `us-east-1a` für ein anderes AWS-Konto.

Um den Ort Ihrer Dedicated Hosts relativ zu Ihren Konten zu bestimmen, müssen Sie die Availability-Zone-ID (AZ-ID) verwenden. Die AZ-ID ist eine eindeutige, konsistente Kennung für eine Availability Zone innerhalb aller AWS-Konten. Beispielsweise ist `use1-az1` eine Availability-Zone-ID für die `us-east-1`-Region und ist derselbe Speicherort in jedem AWS-Konto. Weitere Informationen finden Sie unter AZ-IDs.

Freigeben von Platzierungsgruppen

Um eine Placement-Gruppe freigeben zu können, müssen Sie diese einer Ressourcenfreigabe hinzufügen. Eine Ressourcenfreigabe ist eine AWS RAM-Ressource, mit der Sie Ihre Ressourcen in mehreren AWS-Konten gemeinsam nutzen können. Eine Ressourcenfreigabe gibt die freizugebenden Ressourcen und die Konsumenten an, für die sie freigegeben werden.

Wenn Sie Teil einer Organisation in AWS Organizations sind und die Freigabe innerhalb Ihrer Organisation aktiviert ist, wird Nutzern in Ihrer Organisation Zugriff auf die freigegebene Placement-Gruppe gewährt.

Wenn die Placement-Gruppe mit einem AWS-Konto außerhalb Ihrer Organisation geteilt wird, erhält der AWS-Kontoinhaber eine Einladung, der Ressourcennutzung beizutreten. Sie können auf die freigegebene Placement-Gruppe zugreifen, nachdem sie die Einladung angenommen haben.

Sie können eine Platzierungsgruppe mit mehreren AWS-Konten teilen, indem SieAWS Resource Access Manager verwenden. Weitere Informationen finden Sie unter Erstellen einer Ressourcenfreigabe im AWS RAM-Benutzerhandbuch.

Freigabe der Platzierungsgruppe aufheben

Der Placement-Gruppenbesitzer kann die Freigabe einer freigegebenen Placement-Gruppe jederzeit aufheben. Wenn Sie die Freigabe einer freigegebenen Platzierungsgruppen aufheben, werden die folgenden Änderungen wirksam:

- Die AWS-Konten, mit denen eine Platzierungsgruppe geteilt wurde, können keine Instances mehr starten oder Kapazitäten reservieren.
- Wenn Ihre Instances in einer gemeinsamen Platzierungsgruppe ausgeführt wurden, werden sie von der Platzierungsgruppe getrennt, laufen aber weiterhin normal in Ihrem AWS-Konto.
- Alle Kapazitätsreservierungen in einer gemeinsamen Platzierungsgruppe werden von der Platzierungsgruppe getrennt, stehen Ihnen aber weiterhin in Ihrem AWS-Konto zur Verfügung.

Weitere Informationen finden Sie unter Löschen einer Ressourcenfreigabe im AWS RAM-Benutzerhandbuch.

Platzierungsgruppen auf AWS Outposts

AWS Outposts ist ein vollständig verwalteter Service, der AWS-Infrastruktur, Services, APIs und Tools auf Kundenstandorte ausweitet. Durch die Bereitstellung des lokalen Zugriffs auf die von AWS verwaltete Infrastruktur ermöglicht AWS Outposts Kunden, Anwendungen On-Premises mit denselben Programmierschnittstellen wie in AWS-Regionen zu erstellen und auszuführen, während lokale Datenverarbeitungs- und Speicherressourcen für geringere Latenz und lokale Datenverarbeitungsanforderungen verwendet werden.

Ein Outpost ist ein Pool von AWS-Rechen- und Speicherkapazitäten, die an einem Kundenstandort bereitgestellt werden. AWS betreibt, überwacht und verwaltet diese Kapazität als Teil einer AWS-Region.

Sie können Platzierungsgruppen auf Outposts erstellen, die Sie in Ihrem Konto angelegt haben. Auf diese Weise können Sie die Instances auf die zugrunde liegende Hardware auf einem Outpost an Ihrem Standort verteilen. Sie erstellen und verwenden Platzierungsgruppen auf Outposts auf die gleiche Weise wie Sie Platzierungsgruppen in regulären Availability Zones erstellen und verwenden. Wenn Sie eine Platzierungsgruppe mit einer Spread-Strategie auf einem Outpost erstellen, können Sie wählen, ob die Platzierungsgruppe Instances über Hosts oder Racks verteilt. Wenn Sie Instances auf Hosts verteilen, können Sie eine Spread-Strategie mit einem einzigen Rack-Outpost verwenden.

Überlegungen

- Ihre Spread-Placement-Gruppe auf Rack-Ebene kann so viele Instances aufnehmen, wie Sie Racks in Ihrer Outpost-Bereitstellung haben.
- Eine Spread-Placement-Gruppe auf Host-Ebene kann so viele Instances aufnehmen, wie Sie Hosts in Ihrer Outpost-Bereitstellung haben.

Voraussetzung

Sie müssen einen Outpost an Ihrem Standort installiert haben. Weitere Informationen finden Sie unter Outpost erstellen und die Kapazität dafür bestellen im AWS Outposts-Benutzerhandbuch.

So verwenden Sie eine Platzierungsgruppe für einen Outpost

1. Erstellen Sie ein Subnetz auf dem Outpost. Weitere Informationen finden Sie unter Erstellen eines Subnetzes im AWS Outposts-Benutzerhandbuch.
2. Erstellen Sie eine Platzierungsgruppe in der zugehörigen Region des Outposts. Wenn Sie eine Platzierungsgruppe mit einer Spread-Strategie erstellen, können Sie die Host- oder Rack-Spread-Ebene wählen, um zu bestimmen, wie die Gruppe Instances auf die zugrunde liegende Hardware Ihres Outposts verteilt. Weitere Informationen finden Sie unter the section called “Erstellen einer Placement-Gruppe”.
3. Launchen Sie eine Instance in die Platzierungsgruppe. Wählen Sie für Subnet (Subnetz) das Subnetz aus, das Sie in Schritt 1 erstellt haben, und für Placement group name (Name der Placement-Gruppe), wählen Sie die Platzierungsgruppe aus, die Sie in Schritt 2 erstellt haben. Weitere Informationen finden Sie unter Launch an Instance on your Outpost (Starten einer Instance auf Ihrem Outpost) im AWS Outposts-Benutzerhandbuch.

Netzwerk-MTU (Maximum Transmission Unit) für Ihre EC2-Instance

Die maximale Übertragungseinheit (MTU) einer Netzwerkverbindung ist die Größe (in Byte) des größten zulässigen Datenpakets, das über die Verbindung übergeben werden kann. Je größer die MTU einer Verbindung, desto mehr Daten können in einem einzelnen Paket übergeben werden. Ethernet-Rahmen bestehen aus dem Paket, also den eigentlichen Daten, die Sie senden, sowie aus den dazugehörigen Netzwerk-Overhead-Informationen.

Ethernet-Frames können in verschiedenen Formaten vorkommen, wobei das gängigste Format das standardmäßige Ethernet v2-Frameformat ist. Es unterstützt einen MTU-Wert von 1 500. Dies ist die größte unterstützte Ethernet-Paketgröße in den meisten Bereichen des Internets. Der maximal unterstützte MTU-Wert für eine Instance hängt von deren Instance-Typ ab.

Alle EC2-Instance-Typen unterstützen 1 500 MTU.

Inhalt

- Jumbo-Frames (9001 MTU)
- Path MTU Discovery
- Die MTU für Ihre Amazon EC2 Instances einstellen
- Fehlerbehebung

Jumbo-Frames (9001 MTU)

Für Jumbo-Frames können Sie die Nutzdatengröße pro Paket erhöhen und somit den Prozentsatz des Pakets erhöhen, bei dem es sich nicht um Paket-Overhead handelt. Mit Jumbo-Frames werden weniger Pakete benötigt, um die gleiche Menge an verwendbaren Daten zu übertragen. Für bestimmte Arten von Datenverkehr gelten jedoch die folgenden Höchstgrenzen für Nutzdaten:

MTU-Limit 1 500 Byte

- Datenverkehr über ein Internet-Gateway
- Datenverkehr über VPN-Verbindungen
- Datenverkehr zwischen AWS-Regionen, sofern kein Transit-Gateway verwendet wird

MTU-Limit 8 500 Byte

- Datenverkehr über eine regionsübergreifende VPC-Peering-Verbindung

Sind die Pakete größer als der MTU-Limit, werden sie fragmentiert oder sie werden verworfen, wenn im IP-Header das Flag `Don't Fragment` gesetzt ist.

Jumbo-Frames sollten für Internet-Datenverkehr bzw. für Datenverkehr, der eine VPC verlässt, nur mit Vorsicht verwendet werden. Pakete werden durch zwischengeschaltete Systeme fragmentiert, sodass dieser Datenverkehr verlangsamt wird. Um Jumbo-Frames innerhalb einer VPC zu verwenden und dabei den Datenverkehr, der aus der VPC gesendet werden soll, nicht zu verlangsamen, können Sie die MTU-Größe nach Route konfigurieren oder mehrere Elastic Network-Schnittstellen mit unterschiedlichen MTU-Größen und Routen verwenden.

Bei Instances, die sich gemeinsam innerhalb einer Cluster Placement-Gruppe befinden, helfen Jumbo-Frames dabei, den maximal möglichen Netzwerkdurchsatz zu ermöglichen, und werden für diese Zwecke empfohlen. Weitere Informationen finden Sie unter Platzierungsgruppen für Ihre Amazon-EC2-Instances.

Sie können für Datenverkehr zwischen Ihren VPCs und Ihren On-Premises-Netzwerken über Jumbo-Frames verwende Direct Connect. Weitere Informationen. u. a. zum Überprüfen der Jumbo-Frame-Funktionalität. finden Sie unter MTU für private virtuelle Schnittstellen oder virtuelle Transitschnittstellen im Direct Connect-Benutzerhandbuch.

Alle Instances der aktuellen Generation unterstützen Jumbo-Frames. Die folgenden Instance-Typen der vorherigen Generation unterstützen Jumbo-Frames: A1, C3, I2, M3 und R3.

Zugehörige Ressourcen

- Für NAT-Gateways siehe NAT-Gateway Grundlagen im Amazon VPC Benutzerhandbuch.
- Für Transit-Gateways, siehe Maximale Übertragungseinheit im Benutzerhandbuch für Amazon VPC Transit Gateways.
- Für lokale Zonen siehe Überlegungen im AWS Benutzerhandbuch für lokale Zonen.
- Weitere Informationen für AWS Wavelength finden Sie unter Maximale Übertragungseinheit im AWS Wavelength-Benutzerhandbuch.
- Informationen zu Outposts finden Sie im AWS Outposts-Benutzerhandbuch unter Anforderungen an die maximale Übertragungseinheit von Service Link.

Path MTU Discovery

Path MTU Discovery (PMTUD) wird verwendet, um den Pfad-MTU-Wert zwischen zwei Geräten zu ermitteln. Die Pfad-MTU ist die maximale Paketgröße, die auf dem Pfad zwischen dem sendenden Host und dem empfangenden Host unterstützt wird. Wenn es im Netzwerk zwischen zwei Hosts unterschiedliche MTU-Größen gibt, ermöglicht PMTUD dem empfangenden Host, mit einer ICMP-Nachricht für den ursprünglichen Host zu antworten. Diese ICMP-Nachricht weist den Ursprungshost an, die niedrigste MTU-Größe mit dem Netzwerkpfad zu verwenden und die Anforderung erneut zu senden. Ohne diese Verhandlung können Paketverluste auftreten, da die Anforderung für den empfangenden Host zu groß ist, um sie akzeptieren zu können.

Wenn ein Host ein Paket sendet, das größer als die MTU des empfangenden Hosts ist bzw. das größer als die MTU eines Geräts auf dem Pfad ist, löscht der empfangende Host bzw. das Gerät bei IPv4 das Paket und gibt dann die folgende ICMP-Meldung zurück: `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (Typ 3, Code 4). Dies weist den übertragenden Host an, die Nutzlast in mehrere kleinere Pakete aufzuteilen und diese dann erneut zu übertragen.

Das IPv6-Protokoll unterstützt keine Fragmentierung im Netzwerk. Wenn ein Host ein Paket sendet, das größer als die MTU des empfangenden Hosts ist bzw. das größer als die MTU eines Geräts auf dem Pfad ist, löscht der empfangende Host bzw. das Gerät das Paket und gibt dann die folgende ICMP-Meldung zurück: `ICMPv6 Packet Too Big (PTB)` (Typ 2). Dies weist den übertragenden Host an, die Nutzlast in mehrere kleinere Pakete aufzuteilen und diese dann erneut zu übertragen.

Verbindungen, die über Komponenten wie NAT-Gateways und Load Balancer hergestellt werden, werden automatisch verfolgt. Das bedeutet, dass die Verfolgung von Sicherheitsgruppen für

ausgehende Verbindungsversuche automatisch aktiviert wird. Wenn Verbindungen automatisch verfolgt werden oder die Sicherheitsgruppenregeln eingehenden ICMP-Datenverkehr zulassen, können Sie PMTUD-Antworten erhalten.

Hinweis: Der ICMP-Datenverkehr kann auch dann blockiert werden, wenn der Datenverkehr auf Ebene der Sicherheitsgruppe zulässig ist, z. B. wenn ein Eintrag in der Liste der Netzwerkzugriffskontrolle den ICMP-Verkehr zum Subnetz verhindert.

> **Important**
>
> Path MTU Discovery garantiert nicht, dass Jumbo-Frames nicht von einigen Routern verworfen werden. Ein Internet-Gateway in Ihrer VPC leitet nur Pakete mit bis zu 1 500 Byte weiter. Für Internet-Datenverkehr empfehlen sich Pakete mit einem MTU-Wert von 1 500.

Informationen zu MTU-Regeln für NAT-Gateways finden Sie unter Maximum Transmission Unit (MTU) im Amazon-VPC-Benutzerhandbuch. Informationen zu MTU-Regeln für Transit-Gateways finden Sie unter Maximum Transmission Unit (MTU) im AWS-Transit-Gateway-Benutzerhandbuch.

Die MTU für Ihre Amazon EC2 Instances einstellen

Die maximale Übertragungseinheit (MTU) einer Netzwerkverbindung ist die Größe (in Byte) des größten zulässigen Datenpakets, das über die Verbindung übergeben werden kann. Alle Amazon-EC2-Instances unterstützen Standard-Frames (1 500 MTU) und alle Instance-Typen der aktuellen Generation unterstützen Jumbo-Frames (9 001 MTU).

Sie können die MTU für Ihre Amazon-EC2-Instances und die Pfad-MTU zwischen Ihrer Instance und einem anderen Host anzeigen und Ihre Instances so konfigurieren, dass sie entweder Standard- oder Jumbo-Frames verwenden.

Aufgaben

- Überprüfen des Pfad-MTU-Werts zwischen zwei Hosts
- Überprüfen Sie die MTU für Ihre Instance
- Die MTU für Ihre Instance einstellen

Überprüfen des Pfad-MTU-Werts zwischen zwei Hosts

Verwenden Sie den folgenden Befehl, um die Pfad-MTU zwischen Ihrer EC2 Instance und einem anderen Host zu überprüfen. Sie können einen DNS-Namen oder eine IP-Adresse als Ziel angeben. Wenn es sich bei dem Ziel um eine andere EC2 Instance handelt, vergewissern Sie sich, dass ihre Sicherheitsgruppe eingehenden UDP-Datenverkehr erlaubt.

Welches Verfahren Sie verwenden, hängt vom Betriebssystem der Instance ab.

Linux-Instances

Führen Sie den tracepath-Befehl auf Ihrer Instance aus, um die Pfad-MTU zwischen Ihrer EC2 Instance und dem angegebenen Ziel zu überprüfen. Dieser Befehl ist Teil des `iputils`-Pakets, das standardmäßig in vielen Linux-Distributionen verfügbar ist.

In diesem Beispiel wird die Pfad-MTU zwischen einer EC2-Instance und `amazon.com` überprüft.

```
[ec2-user ~]$ tracepath amazon.com
```

In dieser Beispielausgabe ist die Pfad-MTU 1 500.

```
 1?: [LOCALHOST]     pmtu 9001
 1:  ip-172-31-16-1.us-west-1.compute.internal (172.31.16.1)   0.187ms pmtu 1500
 1:  no reply
 2:  no reply
 3:  no reply
 4:  100.64.16.241 (100.64.16.241)                              0.574ms
 5:  72.21.222.221 (72.21.222.221)                             84.447ms asymm 21
 6:  205.251.229.97 (205.251.229.97)                           79.970ms asymm 19
 7:  72.21.222.194 (72.21.222.194)                             96.546ms asymm 16
 8:  72.21.222.239 (72.21.222.239)                             79.244ms asymm 15
 9:  205.251.225.73 (205.251.225.73)                           91.867ms asymm 16
...
31:  no reply
     Too many hops: pmtu 1500
     Resume: pmtu 1500
```

Windows-Instances

Überprüfen Sie der Pfad-MTU mit mturoute

1. Laden Sie mturoute.exe von https://elifulkerson.com/projects/mturoute.php auf Ihre EC2-Instance herunter.
2. Öffnen Sie ein Eingabeaufforderungsfenster und wechseln Sie zu dem Verzeichnis, in das Sie heruntergeladen habe mturoute.exe.
3. Verwenden Sie den folgenden Befehl, um die Pfad-MTU zwischen Ihrer EC2 Instance und einem anderen Host zu überprüfen. In diesem Beispiel wird die Pfad-MTU zwischen einer EC2-Instance und `www.elifulkerson.com` überprüft.

   ```
   .\mturoute.exe www.elifulkerson.com
   ```

   In dieser Beispielausgabe ist die Pfad-MTU 1 500.

   ```
   * ICMP Fragmentation is not permitted. *
   * Speed optimization is enabled. *
   * Maximum payload is 10000 bytes. *
   + ICMP payload of 1472 bytes succeeded.
   - ICMP payload of 1473 bytes is too big.
   Path MTU: 1500 bytes.
   ```

Überprüfen Sie die MTU für Ihre Instance

Sie können die MTU für Ihre Instance überprüfen. Einige Instances sind so konfiguriert, dass sie Jumbo-Frames nutzen, während andere für die Nutzung von Standard-Framegrößen konfiguriert sind.

Welches Verfahren Sie verwenden, hängt vom Betriebssystem der Instance ab.

Linux-Instances

So überprüfen Sie die MTU-Einstellung auf einer Linux-Instance

Führen Sie den folgenden ip-Befehl auf Ihrer EC2-Instance aus. Wenn die primäre Netzwerkschnittstelle nicht `eth0` ist, ersetzen Sie `eth0` durch Ihre Netzwerkschnittstelle.

```
[ec2-user ~]$ ip link show eth0
```

In dieser Beispielausgabe gibt *mtu 9001* die Verwendung von Jumbo-Frames auf dieser Instance an.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP mode
 DEFAULT group default qlen 1000
    link/ether 02:90:c0:b7:9e:d1 brd ff:ff:ff:ff:ff:ff
```

Windows-Instances

Die Vorgehensweise, die Sie verwenden, ist vom Treiber auf Ihrer Instance abhängig.

ENA driver

Version 2.1.0 und höher

Verwenden Sie den folgenden Get-NetAdapterAdvancedProperty-Befehl auf Ihrer EC2-Instance, um den MTU-Wert abzurufen. Verwenden Sie den Platzhalter (Sternchen), um alle Ethernet-Namen abzurufen. Überprüfen Sie die Ausgabe für den Schnittstellennamen `*JumboPacket`. Der Wert 9015 bedeutet, dass Jumbo-Frames aktiviert sind. Jumbo-Frames sind standardmäßig deaktiviert.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet*"
```

Version 1.5 und früher

Verwenden Sie den folgenden Get-NetAdapterAdvancedProperty-Befehl auf Ihrer EC2-Instance, um den MTU-Wert abzurufen. Überprüfen Sie die Ausgabe für den Schnittstellennamen `MTU`. Ein Wert von 9001 zeigt an, dass Jumbo-Frames aktiviert sind. Jumbo-Frames sind standardmäßig deaktiviert.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

Intel SRIOV 82599 driver

Verwenden Sie den folgenden Get-NetAdapterAdvancedProperty-Befehl auf Ihrer EC2-Instance, um den MTU-Wert abzurufen. Überprüfen Sie den Eintrag für die Schnittstelle mit dem Namen `*JumboPacket`. Ein Wert von 9014 zeigt an, dass Jumbo-Frames aktiviert sind. (Beachten Sie, dass in der MTU-Größe der Header und die Nutzlast enthalten sind.) Jumbo-Frames sind standardmäßig deaktiviert.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

AWS PV driver

Um den MTU-Wert zu ermitteln, verwenden Sie den folgenden Befehl auf Ihrer EC2-Instance. Der Name der Schnittstelle kann hiervon abweichen. Suchen Sie in der Ausgabe nach einem Eintrag mit dem Namen „Ethernet“, „Ethernet 2“ oder „Local Area Connection“. Sie benötigen den Namen der Schnittstelle, um Jumbo-Frames zu aktivieren bzw. zu deaktivieren. Ein Wert von 9001 zeigt an, dass Jumbo-Frames aktiviert sind.

```
netsh interface ipv4 show subinterface
```

Die MTU für Ihre Instance einstellen

Sie möchte vielleicht Jumbo-Frames für Netzwerk-Datenverkehr innerhalb Ihrer VPC und Standard-Frames für Internet-Datenverkehr nutzen. Ganz gleich, welcher Anwendungsfall auf Sie zutrifft: Wir empfehlen Ihnen, sicherzustellen, dass Ihre Instance wie erwartet funktioniert.

Welches Verfahren Sie verwenden, hängt vom Betriebssystem der Instance ab.

Linux-Instances

So legen Sie den MTU-Wert auf einer Linux-Instance fest

1. Führen Sie den folgenden ip-Befehl in Ihrer Instance aus. Er setzt den gewünschten MTU-Wert auf 1 500, aber Sie können stattdessen auch 9 001 verwenden. Wenn die primäre Netzwerkschnittstelle nicht `eth0` ist, ersetzen Sie `eth0` durch die tatsächliche Netzwerkschnittstelle.

   ```
   [ec2-user ~]$ sudo ip link set dev eth0 mtu 1500
   ```

2. (Optional) Um die MTU-Netzwerkeinstellung nach einem Neustart beizubehalten, müssen Sie die folgenden Konfigurationsdateien je nach verwendetem Betriebssystem ändern.

   - Amazon Linux 2023 – Ändern Sie den `[Link]`-Abschnitt der Konfigurationsdatei. Die Standardkonfigurationsdatei ist `/usr/lib/systemd/network/80-ec2.network`. Sie können aber auch jede benutzerdefinierte Konfigurationsdatei aktualisieren, die in /run/systemd/network/ erstellt wurde, wobei der Dateiname *priority*-*interface*.network lautet.

Weitere Informationen finden Sie unter Netzwerkservice im Benutzerhandbuch für Amazon Linux.

```
MTUBytes=1500
```

- Amazon Linux 2 – Fügen Sie der Datei `/etc/sysconfig/network-scripts/ifcfg-eth0` die folgende Zeile hinzu:

```
MTU=1500
```

Fügen Sie der Datei `/etc/dhcp/dhclient.conf` die folgende Zeile hinzu:

```
request subnet-mask, broadcast-address, time-offset, routers, domain-name,
 domain-search, domain-name-servers, host-name, nis-domain, nis-servers, ntp-
servers;
```

- Andere Linux-Distributionen – Sehen Sie in der entsprechenden Dokumentation nach.

3. (Optional) Starten Sie Ihre Instance neu und vergewissern Sie sich, dass die MTU-Einstellung korrekt ist.

Windows-Instances

Die Vorgehensweise, die Sie verwenden, ist vom Treiber auf Ihrer Instance abhängig.

ENA driver

Sie können die MTU mit dem Geräte-Manager oder dem Set-NetAdapterAdvancedProperty-Befehl in Ihrer Instance ändern.

Version 2.1.0 und höher

Verwenden Sie den folgenden Befehl, um Jumbo-Frames zu aktivieren.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9015
```

Um Jumbo-Frames zu deaktivieren, verwenden Sie den folgenden Befehl.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

Version 1.5 und früher

Verwenden Sie den folgenden Befehl, um Jumbo-Frames zu aktivieren.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 9001
```

Um Jumbo-Frames zu deaktivieren, verwenden Sie den folgenden Befehl.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 1500
```

Intel SRIOV 82599 driver

Sie können die MTU mit dem Geräte-Manager oder dem Set-NetAdapterAdvancedProperty-Befehl in Ihrer Instance ändern.

Verwenden Sie den folgenden Befehl, um Jumbo-Frames zu aktivieren.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9014
```

Um Jumbo-Frames zu deaktivieren, verwenden Sie den folgenden Befehl.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

AWS PV driver

Sie können die MTU mit dem netsh-Befehl auf Ihrer Instance ändern. Sie können die MTU-Einstellung nicht mit dem Geräte-Manager ändern.

Verwenden Sie den folgenden Befehl, um Jumbo-Frames zu aktivieren.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=9001
```

Um Jumbo-Frames zu deaktivieren, verwenden Sie den folgenden Befehl.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=1500
```

Fehlerbehebung

Sollten beim Verwenden von Jumbo-Frames Verbindungsprobleme zwischen der EC2-Instance und einem Amazon-Redshift-Cluster auftreten, finden Sie Informationen unter Abfragen scheinen hängen zu bleiben und erreichen manchmal den Cluster nicht im Verwaltungshandbuch für Amazon Redshift.

Virtual Private Clouds für Ihre EC2-Instances

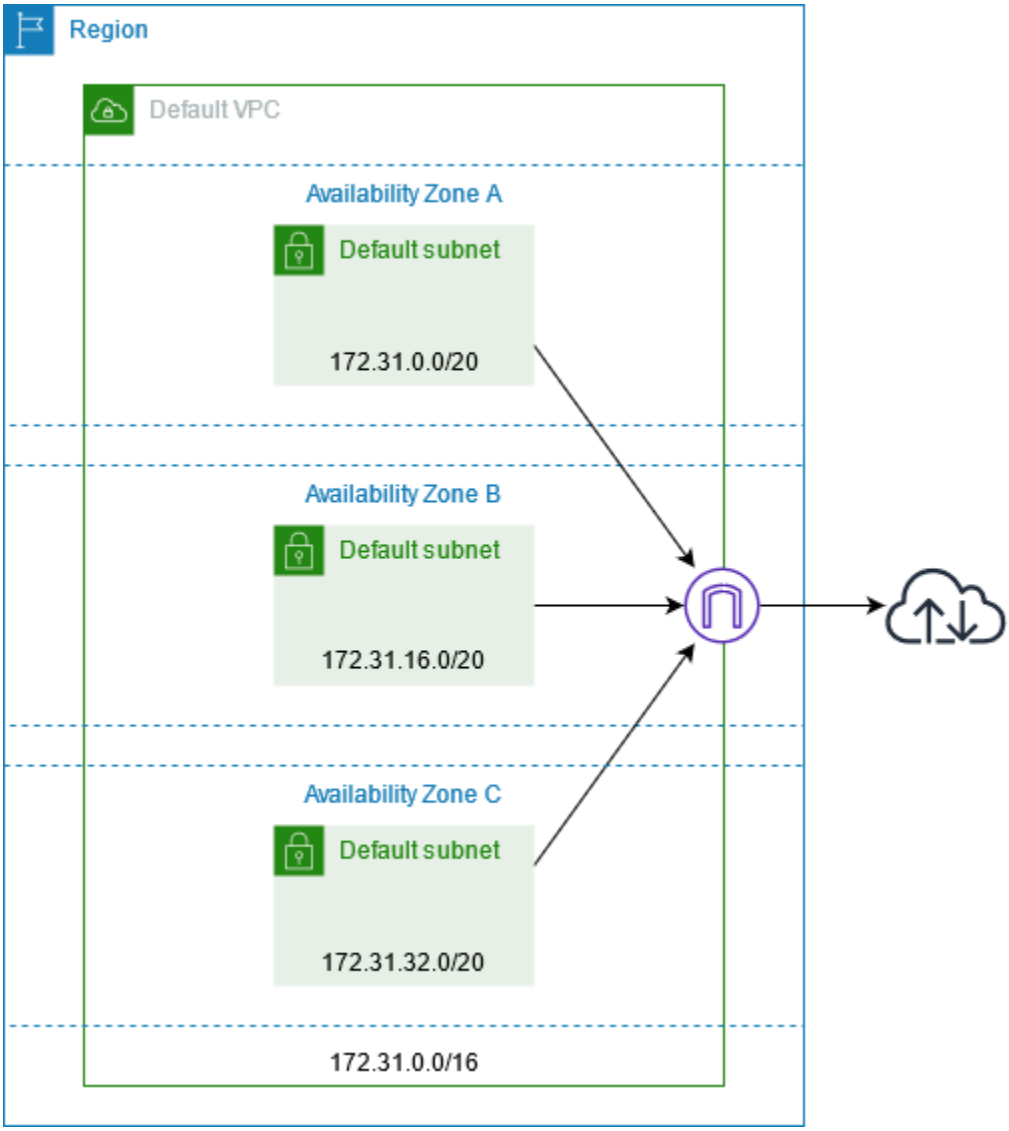
Mit Amazon Virtual Private Cloud (Amazon VPC) können Sie ein virtuelles Netzwerk in Ihrem eigenen logisch isolierten Bereich innerhalb der AWS Cloud einrichten, der als Virtual Private Cloud bzw. VPC bezeichnet wird. Sie können Ihre AWS-Ressourcen, z. B. Amazon-EC2-Instances, in den Subnetzen Ihrer VPC starten. Ihre VPC ist einem herkömmlichen Netzwerk sehr ähnlich, das Sie möglicherweise in Ihrem eigenen Rechenzentrum betreiben, bietet jedoch die Vorteile, die mit der Nutzung der skalierbaren Infrastruktur von einhergehen AWS. Sie können Ihre VPC konfigurieren. Dazu ist es möglich, den IP-Adressbereich auszuwählen, Subnetze zu erstellen sowie Routing-Tabellen, Netzwerk-Gateways und Sicherheitseinstellungen zu konfigurieren. Sie können Instances in Ihrer VPC mit dem Internet oder Ihrem eigenen Rechenzentrum verbinden.

Inhalt

- Ihre Standard-VPCs
- Nicht standardmäßige VPCs
- Internetzugang
- Gemeinsame Subnetze
- Nur IPv6-Subnetze

Ihre Standard-VPCs

Wenn Sie Ihr AWS-Konto erstellen, erstellen wir in jeder Region eine Standard-VPC. Eine Standard-VPC ist eine VPC, die bereits vorkonfiguriert und betriebsbereit ist. In jeder Standard-VPC gibt es beispielsweise ein Standardsubnetz für jede Availability Zone, ein an die VPC angeschlossenes Internet-Gateway und eine Route in der Haupt-Routing-Tabelle, die den gesamten Datenverkehr (0.0.0.0/0) an das Internet-Gateway sendet. Sie können die Konfiguration Ihrer Standard-VPCs nach Bedarf ändern. Sie können beispielsweise Subnetze und Routing-Tabellen hinzufügen.



Nicht standardmäßige VPCs

Anstatt eine Standard-VPC für Ihre Ressourcen zu verwenden, können Sie Ihre eigene VPC erstellen, wie unter Erstellen einer VPC im Amazon VPC-Benutzerhandbuch beschrieben wird.

Im Folgenden sind einige Dinge zu beachten, wenn Sie eine VPC für Ihre EC2-Instances erstellen.

- Behalten Sie für den IPv4-CIDR-Block entweder den Standardvorschlag bei oder geben Sie den für Ihre Anwendung oder Ihr Netzwerk erforderlichen CIDR-Block ein.
- Erstellen Sie Subnetze in mehreren Availability Zones, um eine hohe Verfügbarkeit zu erzielen.
- Wenn Ihre Instances über das Internet zugänglich sein müssen, führen Sie einen der folgenden Schritte aus:

- Wenn sich Ihre Instances in einem öffentlichen Subnetz befinden können, fügen Sie öffentliche Subnetze hinzu. Lassen Sie beide DNS-Optionen aktiviert. Optional können Sie jetzt oder später private Subnetze hinzufügen.
- Wenn sich Ihre Instances in einem privaten Subnetz befinden müssen, fügen Sie nur private Subnetze hinzu. Sie können ein NAT-Gateway hinzufügen, um den Instances in den privaten Subnetzen Internetzugang zu ermöglichen. Wenn Ihre Instances ein erhebliches Volumen an Datenverkehr über Availability Zones hinweg senden oder empfangen, erstellen Sie ein NAT-Gateway in jeder Availability Zone. Andernfalls können Sie ein NAT-Gateway in nur einer der Availability Zones erstellen und Instances starten, die zonenübergreifenden Datenverkehr in derselben Availability Zone wie das NAT-Gateway senden oder empfangen.

Internetzugang

Instances, die in ein Standardsubnetz in einer Standard-VPC gestartet werden, haben Zugriff auf das Internet, da die VPC dafür konfiguriert ist, öffentliche IP-Adressen und DNS-Host-Namen zuzuweisen, und die Haupt-Routing-Tabelle mit einer Route zu einem an die VPC angefügten Internet-Gateway konfiguriert ist.

Sie könnenfür die Subnetze, die Sie in Ihren Nicht-Standard-VPCs erstellen, einen der folgenden Schritte ausführen, um sicherzustellen, dass in diesen Subnetzen gestartete Instances Zugriff auf das Internet haben:

- Konfigurieren Sie ein Internet-Gateway. Weitere Informationen finden Sie unter Verbinden mit dem Internet über ein Internet-Gateway im Amazon-VPC-Benutzerhandbuch.
- Konfigurieren Sie ein öffentliches NAT-Gateway. Weitere Informationen finden Sie unter Zugriff auf das Internet aus einem privaten Subnetz im Benutzerhandbuch für Amazon VPC.

Gemeinsame Subnetze

Beachten Sie beim Starten von EC2-Instances in gemeinsam genutzten VPC-Subnetzen Folgendes:

- Teilnehmer können Instances in einem freigegebenen Subnetz ausführen, indem sie die ID des freigegebenen Subnetzes angeben. Die Teilnehmer müssen alle von ihnen angegebenen Netzwerkschnittstellen besitzen.

- Teilnehmer können Instances, die sie in einem freigegebenen Subnetz erstellt haben, starten, anhalten, beenden und beschreiben. Teilnehmer können Instances, die vom VPC-Eigentümer in einem freigegebenen Subnetz erstellt wurden, nicht starten, anhalten, beenden oder beschreiben.
- VPC-Eigentümer können Instances, die von Teilnehmern in einem freigegebenen Subnetz erstellt wurden, nicht starten, anhalten, beenden oder beschreiben.
- Die Teilnehmer können sich über den EC2-Instance-Verbindungs-Endpunkt mit einer Instance in einem freigegebenen Subnetz verbinden. Der Teilnehmer muss den EC2-Instance-Verbindungs-Endpunkt im freigegebenen Subnetz erstellen. Teilnehmer können keinen EC2-Instance-Verbindungs-Endpoint verwenden, den der VPC-Eigentümer im freigegebenen Subnetz erstellt hat.

Weitere Informationen zu freigegebenen Amazon-EC2-Ressourcen finden Sie hier:

- the section called “Gemeinsame Nutzung von AMI mit einer Organisation oder OU verwalten”
- the section called “Freigegebene Kapazitätsreservierungen”
- the section called “Freigegebene Platzierungsgruppen”
- Kontoübergreifendes Amazon EC2 Dedicated Host-Sharing

Weitere Informationen zu freigegebenen Subnetzen finden Sie unter Freigeben Ihrer VPC für andere Konten im Amazon-VPC-Benutzerhandbuch.

Nur IPv6-Subnetze

Eine EC2-Instance, die in einem reinen IPv6-Subnetz gestartet wird, erhält eine IPv6-Adresse, aber keine IPv4-Adresse. Alle Instances, die in einem reinen IPv6-Subnetz gestartet werden, müssen Nitro-basierte Instances sein.

Sicherheit bei Amazon EC2

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einem Rechenzentrum und einer Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der übergreifenden Verantwortlichkeit beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Amazon gelten EC2, finden Sie unter AWS Services im Bereich nach Compliance-Programm AWS .
- Sicherheit in der Cloud – Ihre Verantwortlichkeit umfasst die folgenden Bereiche.
  - Steuern des Netzwerkzugriffs auf Ihre Instances, z. B. durch die Konfiguration Ihrer VPC und Ihrer Sicherheitsgruppen. Weitere Informationen finden Sie unter Steuern des Netzwerkverkehrs.
  - Verwaltung der Anmeldedaten, die für die Verbindung mit Ihren Instances verwendet werden.
  - Verwaltung des Gastbetriebssystems und der Software, die für das Gastbetriebssystem bereitgestellt werden, einschließlich Updates und Sicherheitspatches. Weitere Informationen finden Sie unter Verwaltung von Updates für EC2 Amazon-Instances.
  - Konfigurieren der IAM-Rollen, die an die Instance angehängt sind, und die mit diesen Rollen verknüpften Berechtigungen. Weitere Informationen finden Sie unter IAM-Rollen für Amazon EC2.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung von Amazon anwenden können EC2. Es zeigt Ihnen, wie Sie Amazon konfigurieren EC2 , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre EC2 Amazon-Ressourcen zu überwachen und zu sichern.

Inhalt

- Datenschutz bei Amazon EC2
- Infrastruktursicherheit bei Amazon EC2

- Resilienz bei Amazon EC2
- Konformitätsvalidierung für Amazon EC2
- Identitäts- und Zugriffsmanagement für Amazon EC2
- Verwaltung von Updates für EC2 Amazon-Instances
- Bewährte Methoden für die Sicherheit in Windows-Instances
- EC2 Amazon-Schlüsselpaare und EC2 Amazon-Instances
- EC2 Amazon-Sicherheitsgruppen für Ihre EC2 Instances
- NitroTPM für Amazon-Instances EC2
- Bescheinigung von EC2 Amazon-Instanzen
- Credential Guard für Windows-Instances
- Greifen EC2 Sie über einen VPC-Endpunkt mit Schnittstelle auf Amazon zu

Datenschutz bei Amazon EC2

Das AWS Modell der gilt für den Datenschutz in Amazon Elastic Compute Cloud. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.

- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Amazon EC2 oder anderen zusammenarbeiten und die Konsole AWS CLI, API oder AWS-Services verwenden AWS SDKs. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Inhalt

- Datensicherheit bei Amazon EBS
- Verschlüsselung im Ruhezustand
- Verschlüsselung während der Übertragung

Datensicherheit bei Amazon EBS

Amazon-EBS-Volumes werden Ihnen als unformatierte Blockgeräte präsentiert. Diese logischen Geräte werden in der EBS-Infrastruktur erstellt und der Amazon-EBS-Service stellt sicher, dass die Geräte vor jeder (Wieder-)Verwendung durch einen Kunden logisch leer sind (d. h. die Rohblöcke werden auf Null gesetzt oder enthalten kryptografische pseudozufällige Daten).

Wenn Prozeduren erfordern, dass alle Daten mit einer bestimmten Methode gelöscht werden, entweder nach oder vor der Verwendung (oder beidem), wie z. B. in DoD 5220.22-M (National Industrial Security Program Operating Manual) oder NIST 800-88 (Guidelines for Media Sanitization), ist das in Amazon EBS entsprechend möglich. Diese Aktivität auf Blockebene wird auf die zugrunde liegenden Speichermedien im Amazon EBS-Service übertragen.

Verschlüsselung im Ruhezustand

EBS-Datenträger

Die Amazon EBS-Verschlüsselung ist eine Verschlüsselungslösung für Ihre EBS-Volumes und -Snapshots. Es benutzt AWS KMS keys. Weitere Informationen finden Sie unter Amazon-EBS-Verschlüsselung im Amazon-EBS-Benutzerhandbuch.

[Windows-Instances] Sie können auch Microsoft EFS- und NTFS-Berechtigungen für die Verschlüsselung auf Ordner- und Dateiebene verwenden.

Instance-Speicher-Volumes

Die Daten auf NVMe Instance-Speicher-Volumes werden mit einer XTS-AES-256-Verschlüsselung verschlüsselt, die auf einem Hardwaremodul auf der Instance implementiert ist. Die Schlüssel, die zur Verschlüsselung von Daten verwendet werden, die auf lokal angeschlossene NVMe Speichergeräte geschrieben werden, werden pro Kunde und pro Volume vergeben. Die Schlüssel werden vom Hardwaremodul generiert, das für AWS -Personal unzugänglich ist, und befinden sich nur in diesem. Die Verschlüsselungsschlüssel werden vernichtet, wenn die Instance angehalten oder beendet wird, und können nicht wiederhergestellt werden. Sie können diese Verschlüsselung nicht deaktivieren und keine eigenen Verschlüsselungsschlüssel bereitstellen.

Die Daten auf HDD-Instance-Speichervolumes auf H1-, D3- und D3en-Instances werden mit XTS-AES-256 und Einmalschlüsseln verschlüsselt.

Wenn Sie eine Instance anhalten, in den Ruhezustand versetzen oder beenden, wird jeder Speicherblock im Instance-Speicher-Volume zurückgesetzt. Deshalb ist der Zugriff auf Ihre Daten nicht über den Instance-Speicher einer anderen Instance möglich.

Arbeitsspeicher

Die Speicherverschlüsselung ist auf den folgenden Instances aktiviert:

- Instances mit AWS Graviton2-Prozessoren oder neueren Graviton-Prozessoren unterstützen die AWS Always-On-Speicherverschlüsselung. Die Verschlüsselungsschlüssel werden sicher im Hostsystem generiert, verlassen das Hostsystem nicht und werden zerstört, wenn der Host neu gestartet oder heruntergefahren wird. Weitere Informationen finden Sie unter AWS -Graviton-Processors.
- Instances mit skalierbaren Intel-Xeon-Prozessoren der 3. Generation (Ice Lake), z. B. M6i-Instances, und skalierbaren Intel-Xeon-Prozessoren der 4. Generation (Sapphire Rapids), z. B.

M7i-Instances. Diese Prozessoren unterstützen eine immer aktive Speicherverschlüsselung mit Intel Total Memory Encryption (TME).

- Instances mit AMD-EPYC-Prozessoren der 3. Generation (Milan), z. B. M6a-Instances, und AMD-EPYC-Prozessoren der 4. Generation (Genoa), z. B. M7a-Instances. Diese Prozessoren unterstützen eine immer aktive Speicherverschlüsselung mit AMD Secure Memory Encryption (SME).
- AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) wird für einige AMD-basierte Instance-Typen unterstützt. Weitere Informationen finden Sie unter EC2-Instance-Typen suchen, die AMD SEV-SNP unterstützen.

Verschlüsselung während der Übertragung

Verschlüsselung auf physischer Ebene

Alle Daten, die über das AWS globale Netzwerk zwischen AWS Regionen fließen, werden auf der physischen Ebene automatisch verschlüsselt, bevor sie gesicherte Einrichtungen verlassen. AWS Der gesamte Datenverkehr zwischen beiden AZs ist verschlüsselt. Zusätzliche Verschlüsselungsebenen, einschließlich der in diesem Abschnitt aufgeführten, bieten möglicherweise zusätzlichen Schutz.

Verschlüsselung bereitgestellt durch Amazon-VPC-Peering und regionsübergreifendem Peering in Transit Gateway

Der gesamte regionsübergreifende Datenverkehr, der Amazon-VPC- und Transit-Gateway-Peering verwendet, wird automatisch massenverschlüsselt, wenn er eine Region verlässt. Auf der physischen Ebene wird automatisch eine zusätzliche Verschlüsselungsebene für den gesamten Datenverkehr bereitgestellt, bevor er AWS gesicherte Einrichtungen verlässt, wie bereits in diesem Abschnitt erwähnt.

Verschlüsselung zwischen den Instances

AWS bietet sichere und private Konnektivität zwischen EC2 Instanzen aller Typen. Darüber hinaus verwenden einige Instance-Typen die Offload-Funktionen der zugrunde liegenden Nitro-System-Hardware, um den Datenverkehr während der Übertragung zwischen Instances automatisch zu verschlüsseln. Diese Verschlüsselung verwendet AEAD-Algorithmen (Authenticated Encryption with Associated Data) mit 256-Bit-Verschlüsselung. Es gibt keine Auswirkungen auf die Netzwerkleistung. Um diese zusätzliche Verschlüsselung des Datenverkehrs während der Übertragung zwischen Instances zu unterstützen, müssen die folgenden Anforderungen erfüllt sein:

- Die Instances verwenden die folgenden Instance-Typen:
  - Allzweck: M5dn, M5n, M5zn, M6a, M6i, M6id, M6idn, M6in, M7a, M7g, M7gd, M7i, M7i-flex, M8a, M8g, M8gd, M8i, M8i-flex, Mac-m4, Mac-m4pro
  - Für die Datenverarbeitung optimiert: C5n, C6a, C6Gn, C6i, C6id, C6in, C7a, C7g, C7GD, C7Gn, C7i, C7i-Flex, C8a, C8g, C8GB, C8GD, C8Gn, C8Gn, C8i, C8i-Flex
  - Speicheroptimiert: R5dn, R5n, R6a, R6i, R6id, R6idn, R6in, R7a, R7g, R7g, R7gd, R7i, R7iz, R8a, R8g, R8GB, R8gd, R8Gn, R8i, R8i-Flex, U-3tb1, U-6tb1, U-9tb1, U-9tb1, U-9tb1, U-9tb1, U-9tb1, U-9tb1, U-9tb1, U-9tb1, U-9tb1, U-9tb1, U-9tb1, U-9tb1, U-9tb1, U-9tb1, U-9tb1, U-9tb1, U-9tb1, U-9tb1, U-9 12 TB1, U-18 TB1, U-24 TB1, U7i-6 TB, U7i-8 TB, U7i-12 TB, U7in-16 TB, U7in-24 TB, U7in-32 TB, U7inH-32 TB, X2IDN, X2iEDN, X2IEZN, X8G, X8AEDZ
  - Speicheroptimiert: D3, D3en, I3en, I4g, I4i, I7i, I7ie, I8g, I8ge, Im4gn, Is4gen
  - Beschleunigtes Rechnen: DL1 DL2q,, F2, G4ad, G4dn, G5, G6, G6e, G6f, Gr6, Gr6f, Inf1, Inf2, P3dn, P4d, P4de, P5, P5e, P5en, P6-B200, P6-B300, GB2 P6e-0, Trn1, Trn1n, Trn2, TRN2u, VT1
  - Datenverarbeitung in Hochleistung: Hpc6a, Hpc6id, Hpc7a, Hpc7g
- Die Instances befinden sich in derselben Region.
- Die Instances befinden sich in derselben VPC oder per Peering VPCs, und der Datenverkehr wird nicht über ein virtuelles Netzwerkgerät oder einen virtuellen Netzwerkdienst wie einen Load Balancer oder ein Transit-Gateway geleitet.

Auf der physischen Ebene wird automatisch eine zusätzliche Verschlüsselungsebene für den gesamten Datenverkehr bereitgestellt, bevor er AWS gesicherte Einrichtungen verlässt, wie bereits in diesem Abschnitt erwähnt.

So zeigen Sie die Instance-Typen an, die den Datenverkehr während des Transitverkehrs zwischen Instances mithilfe von AWS CLI verschlüsseln

Verwenden Sie den folgenden describe-instance-types-Befehl.

```
aws ec2 describe-instance-types \
    --filters Name=network-info.encryption-in-transit-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

Verschlüsselung von und zu AWS Outposts

Ein Outpost stellt spezielle Netzwerkverbindungen her, die als Dienstlinks zu seiner AWS Heimatregion bezeichnet werden, und optional private Konnektivität zu einem von Ihnen angegebenen VPC-Subnetz. Der gesamte Datenverkehr über diese Verbindung ist vollständig verschlüsselt. Weitere Informationen finden Sie unter Konnektivität über Service-Links und Verschlüsselung während der Übertragung im AWS Outposts Benutzerhandbuch.

Verschlüsselung des Fernzugriffs

Die SSH- und RDP-Protokolle bieten sichere Kommunikationskanäle für den Fernzugriff auf Ihre Instances, sei es direkt oder über EC2 Instance Connect. Der Fernzugriff auf Ihre Instances mithilfe von AWS Systems Manager Session Manager oder Run Command wird mit TLS 1.2 verschlüsselt, und Anfragen zum Herstellen einer Verbindung werden mit Sigv4 signiert und von authentifiziert und autorisiert. AWS Identity and Access Management

Es liegt in Ihrer Verantwortung, ein Verschlüsselungsprotokoll wie Transport Layer Security (TLS) zu verwenden, um sensible Daten bei der Übertragung zwischen Clients und Ihren EC2 Amazon-Instances zu verschlüsseln.

(Windows-Instances) Stellen Sie sicher, dass Sie nur verschlüsselte Verbindungen zwischen EC2 Instances und den AWS API-Endpunkten oder anderen sensiblen Remote-Netzwerkdiensten zulassen. Sie können dies über eine ausgehende Sicherheitsgruppe oder Windows-Firewall-Regeln erzwingen.

Infrastruktursicherheit bei Amazon EC2

Als verwalteter Service ist Amazon Elastic Compute Cloud durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um EC2 über das Netzwerk auf Amazon zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Weitere Informationen finden Sie unter Infrastructure Protection in the Security Pillar — AWS Well-Architected Framework.

Netzwerkisolierung

Eine Virtual Private Cloud (VPC) ist ein virtuelles Netzwerk in Ihrem eigenen logisch isolierten Bereich in der AWS Cloud. Verwenden Sie VPCs es separat, um die Infrastruktur nach Arbeitslast oder organisatorischer Einheit zu isolieren.

Ein Subnetz ist ein Bereich von IP-Adressen in einer VPC. Wenn Sie eine Instance starten, starten Sie sie in einem Subnetz in Ihrer VPC. Verwenden Sie Subnetze, um Ihre Anwendungsschichten (z. B. Web, Anwendung und Datenbank) innerhalb einer einzelnen VPC zu isolieren. Verwenden Sie für Ihre Instances private Subnetze, wenn Sie nicht direkt aus dem Internet erreichbar sein sollen.

Um die EC2 Amazon-API von Ihrer VPC aus mit privaten IP-Adressen aufzurufen, verwenden Sie AWS PrivateLink. Weitere Informationen finden Sie unter Greifen EC2 Sie über einen VPC-Endpunkt mit Schnittstelle auf Amazon zu.

Isolierung auf physischen Hosts

Verschiedene EC2 Instances auf demselben physischen Host sind voneinander isoliert, als ob sie sich auf separaten physischen Hosts befinden würden. Der Hypervisor isoliert CPU und Speicher, und den Instances werden virtualisierte Festplatten anstelle des Zugriffs auf die Datenträger bereitgestellt.

Wenn Sie eine Instance stoppen oder beenden, wird der ihr zugewiesene Speicher vom Hypervisor gesäubert (mit Null überschrieben), bevor er einer neuen Instance zugewiesen wird. Jeder Speicherblock wird zurückgesetzt. Dadurch wird sichergestellt, dass Ihre Daten nicht unbeabsichtigt einer anderen Instance zugänglich gemacht werden.

Netzwerk-MAC-Adressen werden Instanzen von der AWS Netzwerkinfrastruktur dynamisch zugewiesen. IP-Adressen werden Instanzen entweder dynamisch von der AWS Netzwerkinfrastruktur zugewiesen oder von einem EC2 Administrator über authentifizierte API-Anfragen zugewiesen. Das AWS Netzwerk ermöglicht es Instanzen, Datenverkehr nur von der MAC- und den ihnen zugewiesenen IP-Adressen zu senden. Andernfalls wird der Datenverkehr unterbrochen.

Standardmäßig kann eine Instance keinen Datenverkehr empfangen, der nicht speziell an sie gerichtet ist. Wenn Sie Network Address Translation (NAT), Routing oder Firewall-Services auf Ihrer Instance ausführen müssen, können Sie die source/destination Überprüfung der Netzwerkschnittstelle deaktivieren.

Steuern des Netzwerkverkehrs

Ziehen Sie die folgenden Optionen zur Steuerung des Netzwerkverkehrs zu Ihren EC2 Instances in Betracht:

- Beschränken Sie den Zugriff auf Ihre Instances über Sicherheitsgruppen. Konfigurieren Sie Regeln, die den minimal erforderlichen Netzwerkverkehr zulassen. Sie können beispielsweise den Datenverkehr nur aus den Adressbereichen Ihres Unternehmensnetzwerks oder nur für bestimmte Protokolle, wie HTTPS, zulassen. Lassen Sie für Windows-Instances Windows-Verwaltungsverkehr und minimale ausgehende Verbindungen zu.
- Nutzen Sie Sicherheitsgruppen als primären Mechanismus zur Steuerung des Netzwerkzugriffs auf EC2 Amazon-Instances. Verwenden Sie das Netzwerk bei Bedarf ACLs sparsam, um eine zustandslose, grobkörnige Netzwerksteuerung zu gewährleisten. Sicherheitsgruppen sind vielseitiger als Netzwerke, ACLs da sie statusbehaftete Pakete filtern und Regeln erstellen können, die auf andere Sicherheitsgruppen verweisen. Das Netzwerk ACLs kann jedoch als sekundäre Kontrolle wirksam sein, wenn es darum geht, eine bestimmte Teilmenge des Datenverkehrs zu blockieren oder hochrangige Schutzmechanismen für Subnetze bereitzustellen. Da Netzwerke ACLs für ein ganzes Subnetz gelten, können sie auch so verwendet werden, als ob defense-in-depth eine Instance versehentlich ohne die richtige Sicherheitsgruppe gestartet wird.
- [Windows-Instances] Verwalten Sie die Windows-Firewall-Einstellungen mithilfe von Gruppenrichtlinienobjekten (GPO) zentral, um die Netzwerksteuerelemente weiter zu verbessern. Kunden verwenden die Windows-Firewall häufig, um den Netzwerkverkehr besser zu erkennen und Sicherheitsgruppenfilter zu ergänzen, indem sie erweiterte Regeln erstellen, um den Zugriff auf bestimmte Anwendungen auf das Netzwerk zu blockieren oder den Datenverkehr von einer Teilmenge der IP-Adressen zu filtern. Beispielsweise kann die Windows-Firewall den Zugriff auf die IP-Adresse des EC2 Metadatendienstes auf bestimmte Benutzer oder Anwendungen beschränken. Alternativ kann ein öffentlicher Service Sicherheitsgruppen verwenden, um den Datenverkehr auf bestimmte Ports zu beschränken, und die Windows-Firewall, um eine Liste explizit blockierter IP-Adressen zu führen.
- Verwenden Sie für Ihre Instances private Subnetze, wenn Sie nicht direkt aus dem Internet erreichbar sein sollen. Verwenden Sie einen Bastions-Host oder ein NAT-Gateway für den Internetzugriff von einer Instance in einem privaten Subnetz.
- [Windows-Instanzen] Verwenden Sie sichere Verwaltungsprotokolle wie RDP-Kapselung über. SSL/TLS. The Remote Desktop Gateway Quick Start provides best practices for deploying remote desktop gateway, including configuring RDP to use SSL/TLS

- [Windows-Instanzen] Verwenden Sie Active Directory oder Directory Service , um den interaktiven Benutzer- und Gruppenzugriff auf Windows-Instanzen streng und zentral zu steuern und zu überwachen und lokale Benutzerberechtigungen zu vermeiden. Vermeiden Sie auch die Verwendung von Domain-Administratoren und erstellen Sie stattdessen detailliertere, anwendungsspezifische rollenbasierte Konten. Just Enough Administration (JEA) ermöglicht die Verwaltung von Änderungen an Windows-Instances ohne interaktiven oder Administratorzugriff. Darüber hinaus ermöglicht JEA Unternehmen, den administrativen Zugriff auf die Teilmenge der PowerShell Windows-Befehle zu sperren, die für die Instanzverwaltung erforderlich sind. Weitere Informationen finden Sie im Abschnitt „Verwaltung des Zugriffs auf Amazon auf Betriebssystemebene EC2“ im Whitepaper AWS Security Best Practices.
- [Windows-Instances] Systemadministratoren sollten Windows-Konten mit eingeschränktem Zugriff für tägliche Aktivitäten verwenden und den Zugriff nur erhöhen, wenn dies erforderlich ist, um bestimmte Konfigurationsänderungen durchzuführen. Greifen Sie darüber hinaus nur auf Windows-Instances direkt zu, wenn dies unbedingt erforderlich ist. Nutzen Sie stattdessen zentrale Konfigurationsmanagementsysteme wie EC2 Run Command, Systems Center Configuration Manager (SCCM), Windows PowerShell DSC oder Amazon EC2 Systems Manager (SSM), um Änderungen an Windows-Server zu übertragen.
- Konfigurieren Sie Amazon VPC-Subnetz-Routingtabellen mit den minimal erforderlichen Netzwerkrouten. Platzieren Sie beispielsweise nur EC2 Amazon-Instances, die direkten Internetzugang benötigen, in Subnetzen mit Routen zu einem Internet-Gateway und platzieren Sie nur EC2 Amazon-Instances, die direkten Zugriff auf interne Netzwerke benötigen, in Subnetzen mit Routen zu einem virtuellen privaten Gateway.
- Erwägen Sie die Verwendung zusätzlicher Sicherheitsgruppen oder Netzwerkschnittstellen, um den Datenverkehr der EC2 Amazon-Instance-Verwaltung getrennt vom regulären Anwendungsdatenverkehr zu kontrollieren und zu prüfen. Dieser Ansatz ermöglicht es Kunden, spezielle IAM-Richtlinien für die Änderungssteuerung zu implementieren, wodurch Änderungen an Sicherheitsgruppenregeln oder automatisierten Regelverifizierungsskripts leichter geprüft werden können. Mehrere Netzwerk-Schnittstellen bieten außerdem zusätzliche Optionen zur Steuerung des Netzwerkdatenverkehrs, einschließlich der Möglichkeit, Host-basierte Routing-Richtlinien zu erstellen oder verschiedene VPC-Subnetz-Routing-Regeln basierend auf einer einem Subnetz zugewiesenen Netzwerkschnittstelle zu nutzen.
- Verwenden Sie AWS Virtual Private Network oder Direct Connect , um private Verbindungen von Ihren Remote-Netzwerken zu Ihren herzustellen VPCs. Weitere Informationen finden Sie unter Network-to-Amazon VPC-Konnektivitätsoptionen.

- Verwenden Sie VPC Flow-Protokolle, um den Datenverkehr zu überwachen, der Ihre Instances erreicht.
- Verwenden Sie den GuardDuty Malware-Schutz, um verdächtiges Verhalten zu identifizieren, das auf bösartige Software auf Ihren Instances hindeutet, die Ihre Arbeitslast gefährden, Ressourcen für böswillige Zwecke wiederverwenden und sich unbefugten Zugriff auf Ihre Daten verschaffen könnte.
- Verwenden Sie GuardDuty Runtime Monitoring, um potenzielle Bedrohungen für Ihre Instanzen zu identifizieren und darauf zu reagieren. Weitere Informationen finden Sie unter So funktioniert Runtime Monitoring mit EC2 Amazon-Instances.
- Verwenden Sie AWS Security Hub CSPM, Reachability Analyzer oder Network Access Analyzer, um zu überprüfen, ob Ihre Instances unbeabsichtigt auf das Netzwerk zugreifen können.
- Verwenden Sie EC2 Instance Connect, um mithilfe von Secure Shell (SSH) eine Verbindung zu Ihren Instances herzustellen, ohne SSH-Schlüssel teilen und verwalten zu müssen.
- Verwenden Sie AWS Systems Manager Session Manager, um entfernt auf Ihre Instances zuzugreifen, anstatt eingehende SSH-Ports zu öffnen und SSH-Schlüssel RDP-Ports zu verwalten.
- Verwenden Sie AWS Systems Manager Run Command, um allgemeine administrative Aufgaben zu automatisieren, anstatt eine Verbindung zu Ihren Instances herzustellen.
- [Windows-Instanzen] Viele der Windows-Betriebssystemrollen und Microsoft-Geschäftsanwendungen bieten auch erweiterte Funktionen wie Einschränkungen des IP-Adressbereichs in IIS, TCP/IP Filterrichtlinien in Microsoft SQL Server und Verbindungsfilterrichtlinien in Microsoft Exchange. Netzwerkeinschränkungsfunktionalität innerhalb der Anwendungsebene kann zusätzliche Verteidigungsebenen für kritische Geschäftsanwendungsserver bereitstellen.

Amazon VPC unterstützt zusätzliche Netzwerksicherheitskontrollen wie Gateways, Proxyserver und Netzwerküberwachungsoptionen. Weitere Informationen finden Sie unter Kontrollieren des Datenverkehrs im Benutzerhandbuch von Amazon VPC.

Resilienz bei Amazon EC2

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch

Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Falls Sie Ihre Daten oder Anwendungen über größere geografische Distanzen hinweg replizieren müssen, verwenden Sie AWS -Local Zones. Eine AWS lokale Zone ist eine Erweiterung einer AWS Region in geografischer Nähe zu Ihren Benutzern. Local Zones haben ihre eigenen Verbindungen mit dem Internet und unterstützen Direct Connect. Wie alle AWS Regionen sind AWS Local Zones vollständig von anderen AWS Zonen isoliert.

Wenn Sie Ihre Daten oder Anwendungen in einer AWS lokalen Zone replizieren müssen, AWS empfiehlt es sich, eine der folgenden Zonen als Failover-Zone zu verwenden:

- Eine andere Local Zone
- Eine Availability Zone in der Region, bei der es sich nicht um die übergeordnete Zone handelt. Sie können den describe-availability-zonesBefehl verwenden, um die übergeordnete Zone anzuzeigen.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur EC2 bietet Amazon die folgenden Funktionen zur Unterstützung Ihrer Datenstabilität:

- AMIs Regionsübergreifendes Kopieren
- Kopieren von EBS-Snapshots über Regionen hinweg
- Automatisierung mit EBS-Unterstützung AMIs mithilfe von Amazon Data Lifecycle Manager
- Automatisierung von EBS-Snapshots mit Amazon Data Lifecycle Manager
- Aufrechterhaltung des Zustands und der Verfügbarkeit Ihrer Flotte mithilfe von Amazon EC2 Auto Scaling
- Verteilung des eingehenden Datenverkehrs auf mehrere Instances in einer einzigen Availability Zone oder mehreren Availability Zones mithilfe von ELB

Konformitätsvalidierung für Amazon EC2

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services

unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. Weitere Informationen zu Ihrer Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services finden Sie in der AWS Sicherheitsdokumentation.

Identitäts- und Zugriffsmanagement für Amazon EC2

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um EC2 Amazon-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Ihre Sicherheitsdaten identifizieren Sie gegenüber Diensten in AWS und gewähren Ihnen Zugriff auf AWS Ressourcen, wie z. B. Ihre EC2 Amazon-Ressourcen. Sie können Funktionen von Amazon EC2 und IAM verwenden, um anderen Benutzern, Diensten und Anwendungen die Nutzung Ihrer EC2 Amazon-Ressourcen zu ermöglichen, ohne Ihre Sicherheitsinformationen weiterzugeben. Sie können IAM verwenden, um zu kontrollieren, wie andere Benutzer Ressourcen in Ihren nutzen AWS-Konto, und Sie können Sicherheitsgruppen verwenden, um den Zugriff auf Ihre EC2 Amazon-Instances zu kontrollieren. Sie können wählen, ob Sie die vollständige oder eingeschränkte Nutzung Ihrer EC2 Amazon-Ressourcen zulassen möchten.

Wenn Sie ein Entwickler sind, können Sie IAM-Rollen verwenden, um die Sicherheitsanmeldedaten zu verwalten, die für die Anwendungen erforderlich sind, die Sie auf Ihren EC2 Instances ausführen. Nachdem Sie Ihrer Instance eine IAM-Rolle zugewiesen haben, können Ihre Anwendungen, die auf der Instance ausgeführt werden, die Anmeldeinformationen vom Instance Metadata Service (IMDS) abrufen.

Bewährte Methoden für den Schutz Ihrer AWS Ressourcen mithilfe von IAM finden Sie unter Bewährte Sicherheitsmethoden in IAM im IAM-Benutzerhandbuch.

Inhalt

- Identitätsbasierte Richtlinien für Amazon EC2
- Beispielrichtlinien zur Steuerung des Zugriffs auf die EC2 Amazon-API
- Beispielrichtlinien zur Steuerung des Zugriffs auf die EC2 Amazon-Konsole
- AWS verwaltete Richtlinien für Amazon EC2
- IAM-Rollen für Amazon EC2

Identitätsbasierte Richtlinien für Amazon EC2

Standardmäßig sind Benutzer nicht berechtigt, EC2 Amazon-Ressourcen zu erstellen oder zu ändern oder Aufgaben mithilfe der EC2 Amazon-API, der EC2 Amazon-Konsole oder der CLI auszuführen. Damit Benutzer Ressourcen erstellen oder ändern und Aufgaben ausführen können, müssen Sie IAM-Richtlinien erstellen, die Benutzern die Berechtigung zur Verwendung der spezifischen Ressourcen und API-Aktionen gewähren, die sie benötigen. Anschließend fügen Sie diese Richtlinien den Benutzern, Gruppen oder IAM-Rollen an, die diese Berechtigungen benötigen.

Wenn Sie eine Richtlinie einem Benutzer, einer Benutzergruppe oder einer Rolle zuweisen, kann diese dem Benutzer die Berechtigung zur Durchführung der angegebenen Aufgaben auf den angegebenen Ressourcen gewähren oder verweigern. Weitere allgemeine Informationen zu IAM-Richtlinien finden Sie unter Berechtigungen und Richtlinien in IAM im IAM-Benutzerhandbuch. Weitere Informationen zum Verwalten und Erstellen von IAM-Richtlinien finden Sie unter Verwalten von IAM-Richtlinien.

Eine IAM-Richtlinie muss Berechtigungen zur Nutzung einer oder mehrerer EC2 Amazon-Aktionen gewähren oder verweigern. Zudem muss die Richtlinie die Ressourcen benennen, die für diese Aktion verwendet werden dürfen. Dabei kann es sich um alle Ressourcen oder ggf. auch um bestimmte Ressourcen handeln. Eine Richtlinie kann auch Bedingungen enthalten, die für eine Ressource gelten.

Zunächst können Sie überprüfen, ob die AWS verwalteten Richtlinien für Amazon Ihren EC2 Anforderungen entsprechen. Sie können aber Ihre eigenen benutzerdefinierten Richtlinien erstellen. Weitere Informationen finden Sie unter the section called “AWS verwaltete Richtlinien”.

Inhalt

- Richtliniensyntax
- Aktionen für Amazon EC2
- Unterstützte Berechtigungen auf Ressourcenebene für Amazon-API-Aktionen EC2

- Amazon-Ressourcennamen (ARNs) für Amazon EC2
- Zustandsschlüssel für Amazon EC2
- Den Zugriff mithilfe des attributbasierten Zugriffs steuern
- Gewähren von Berechtigungen für Benutzer, Gruppen und Rollen
- Prüfen, ob Benutzer über die erforderlichen Berechtigungen verfügen

Richtliniensyntax

Eine IAM-Richtlinie ist ein JSON-Dokument, das eine oder mehrere Anweisungen enthält. Jede Anweisung ist folgendermaßen strukturiert.

```
{
  "Statement":[{
    "Effect":"effect",
    "Action":"action",
    "Resource":"arn",
    "Condition":{
      "condition":{
        "key":"value"
        }
      }
    }
  ]
}
```

Eine Anweisung kann aus verschiedenen Elementen bestehen:

- Effect: Der effect-Wert kann `Allow` oder `Deny` lauten. -Benutzer verfügen standardmäßig nicht über die Berechtigung zur Verwendung von Ressourcen und API-Aktionen. Daher werden alle Anfragen abgelehnt. Dieser Standardwert kann durch eine explizite Zugriffserlaubnis überschrieben werden. Eine explizite Zugriffsverweigerung überschreibt jedwede Zugriffserlaubnis.
- Action: Mit action wird die API-Aktion spezifiziert, für die Sie Berechtigungen erteilen oder verweigern. Weitere Informationen zur Spezifizierung von action finden Sie unter Aktionen für Amazon EC2.
- Resource: Die von einer Aktion betroffene Ressource. Bei einigen EC2 Amazon-API-Aktionen können Sie bestimmte Ressourcen in Ihre Richtlinie aufnehmen, die durch die Aktion erstellt oder geändert werden können. Sie legen eine Ressource unter Verwendung eines Amazon-Ressourcennamens (ARN) oder eines Platzhalters (*) fest, um anzugeben, dass die Anweisung

für alle Ressourcen gilt. Weitere Informationen finden Sie unter Unterstützte Berechtigungen auf Ressourcenebene für Amazon-API-Aktionen EC2 .

- Condition: Bedingungen sind optional. Mit ihrer Hilfe können Sie bestimmen, wann Ihre Richtlinie wirksam ist. Weitere Informationen zur Angabe von Bedingungen für Amazon EC2 finden Sie unterZustandsschlüssel für Amazon EC2.

Weitere Informationen zu Richtlinienanforderungen finden Sie in der IAM-JSON-Richtlinienreferenz im IAM-Benutzerhandbuch. Beispiele für IAM-Richtlinienerklärungen für Amazon finden Sie EC2 unterBeispielrichtlinien zur Steuerung des Zugriffs auf die EC2 Amazon-API.

Aktionen für Amazon EC2

In einer IAM-Richtlinienanweisung können Sie jede API-Aktion von jedem Service, der IAM unterstützt, angeben. Verwenden Sie für Amazon EC2 das folgende Präfix mit dem Namen der API-Aktion:`ec2:`. Zum Beispiel `ec2:RunInstances` und `ec2:CreateImage`.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie folgendermaßen mit Kommas:

```
"Action": ["ec2:action1", "ec2:action2"]
```

Sie können auch mehrere Aktionen mittels Platzhaltern angeben. Beispielsweise können Sie alle Aktionen festlegen, deren Name mit dem Wort "Describe" beginnt:

```
"Action": "ec2:Describe*"
```

> **Note**
>
> Derzeit unterstützen die Amazon EC2 Describe* API-Aktionen keine Berechtigungen auf Ressourcenebene. Weitere Informationen zu Berechtigungen auf Ressourcenebene für Amazon finden Sie EC2 unter. Identitätsbasierte Richtlinien für Amazon EC2

Um alle EC2 Amazon-API-Aktionen anzugeben, verwenden Sie den Platzhalter * wie folgt:

```
"Action": "ec2:*"
```

Eine Liste der EC2 Amazon-Aktionen finden Sie unter Von Amazon definierte Aktionen EC2 in der Service Authorization Reference.

Unterstützte Berechtigungen auf Ressourcenebene für Amazon-API-Aktionen EC2

Berechtigungen auf Ressourcenebene bedeutet, dass Sie angeben können, für welche Ressourcen die Benutzer Aktionen ausführen dürfen. Amazon EC2 bietet teilweise Unterstützung für Berechtigungen auf Ressourcenebene. Das bedeutet, dass Sie für bestimmte EC2 Amazon-Aktionen steuern können, wann Benutzer diese Aktionen verwenden dürfen, basierend auf Bedingungen, die erfüllt sein müssen, oder auf bestimmten Ressourcen, die Benutzer verwenden dürfen. Zum Beispiel können Sie Benutzern die Berechtigungen erteilen, Instances zu starten, aber nur für einen bestimmten Typ und nur mithilfe eines bestimmten AMI.

Um eine Ressource in einer IAM-Richtlinienanweisung anzugeben, verwenden Sie deren Amazon-Ressourcennamen (ARN). Mehr Informationen zur Angabe des ARN-Werts erhalten Sie unter Amazon-Ressourcennamen (ARNs) für Amazon EC2. Wenn eine API-Aktion einzelne Personen nicht unterstützt ARNs, müssen Sie einen Platzhalter (*) verwenden, um anzugeben, dass alle Ressourcen von der Aktion betroffen sein können.

Tabellen, die angeben, welche EC2 Amazon-API-Aktionen Berechtigungen auf Ressourcenebene unterstützen, ARNs sowie die Bedingungsschlüssel, die Sie in einer Richtlinie verwenden können, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon. EC2

Denken Sie daran, dass Sie in den IAM-Richtlinien, die Sie für Amazon-API-Aktionen verwenden, tagbasierte Berechtigungen auf Ressourcenebene anwenden können. EC2 Dies ermöglicht Ihnen eine bessere Kontrolle darüber, welche Ressourcen ein Benutzer erstellen, ändern oder verwenden kann. Weitere Informationen finden Sie unter Erteilen Sie die Erlaubnis, EC2 Amazon-Ressourcen während der Erstellung zu taggen.

Amazon-Ressourcennamen (ARNs) für Amazon EC2

Jede IAM-Richtlinienerklärung gilt für die Ressourcen, die Sie mithilfe ihrer ARNs angeben.

Ein ARN weist die folgende generelle Syntax auf:

```
arn:aws:[service]:[region]:[account-id]:resourceType/resourcePath
```

Service nicht zulässig

Der Service (z. B. `ec2`)

Region

Die Region für die Ressource (z. B. `us-east-1`)

account-id

Die AWS Konto-ID ohne Bindestriche (z. B.). `123456789012`

RessourcenTyp

Der Typ der Ressource (z. B. `instance`)

resourcePath

Ein Pfad zur Identifizierung der Ressource. Sie können in den Pfaden das Platzhalterzeichen Sternchen (*) verwenden.

Verwenden Sie beispielsweise den ARN wie folgt, um eine bestimmte Instance (`i-1234567890abcdef0`) in der Anweisung anzugeben.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

Sie können auch alle Instances angeben, die zu einem bestimmten Konto gehören, indem Sie das Platzhalterzeichen (*) folgendermaßen hinzufügen.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

Sie können auch alle EC2 Amazon-Ressourcen angeben, die zu einem bestimmten Konto gehören, indem Sie den Platzhalter * wie folgt verwenden.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:*"
```

Um alle Ressourcen anzugeben oder falls eine bestimmte API-Aktion dies nicht unterstützt ARNs, verwenden Sie den Platzhalter * im `Resource` Element wie folgt.

```
"Resource": "*"
```

Viele EC2 Amazon-API-Aktionen beinhalten mehrere Ressourcen. Beispielsweise fügt `AttachVolume` ein Amazon-EBS-Volume an eine Instance an, sodass ein Benutzer über

Berechtigungen zum Verwenden des Volumes und der Instance verfügen muss. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie sie wie folgt ARNs durch Kommas.

```
"Resource": ["arn1", "arn2"]
```

Eine Liste von ARNs vier EC2 Amazon-Ressourcen finden Sie unter Von Amazon definierte Ressourcentypen EC2.

Zustandsschlüssel für Amazon EC2

In einer Richtlinienanweisung können Sie optional Bedingungen angeben, mit denen gesteuert wird, wann die Richtlinie in Kraft tritt. Jede Bedingung enthält ein oder mehrere Schlüssel-Wert-Paare. Bei Bedingungsschlüsseln muss die Groß- und Kleinschreibung nicht beachtet werden. Wir haben AWS globale Bedingungsschlüssel sowie zusätzliche dienstspezifische Bedingungsschlüssel definiert.

Eine Liste der servicespezifischen Bedingungsschlüssel für Amazon EC2 finden Sie unter Bedingungsschlüssel für Amazon EC2. Amazon implementiert EC2 auch die AWS globalen Bedingungsschlüssel. Für weitere Informationen vgl. In allen Anforderungen verfügbare Informationen im IAM-Benutzerhandbuch.

Alle EC2 Amazon-Aktionen unterstützen die Tasten `aws:RequestedRegion` und `ec2:Region` Condition. Weitere Informationen finden Sie unter Beispiel: Beschränken des Zugriffs auf eine bestimmte Region.

Verwenden Sie die `Condition`-Anweisung, um einen Bedingungsschlüssel in Ihrer IAM-Richtlinie zu verwenden. Die folgende Richtlinie gewährt Benutzern beispielsweise die Berechtigung, eingehende und ausgehende Regeln für jede Sicherheitsgruppe hinzuzufügen und zu entfernen. Der `ec2:Vpc`-Bedingungsschlüssel wird verwendet, um anzugeben, dass diese Aktionen nur für Sicherheitsgruppen in einer bestimmten VPC ausgeführt werden können.

JSON

```
{
"Version":"2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action": [
       "ec2:AuthorizeSecurityGroupIngress",
       "ec2:AuthorizeSecurityGroupEgress",
       "ec2:RevokeSecurityGroupIngress",
```

```
        "ec2:RevokeSecurityGroupEgress"],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:security-group/*",
       "Condition": {
         "StringEquals": {
           "ec2:Vpc": "arn:aws:ec2:us-east-1:111122223333:vpc/
vpc-11223344556677889"
         }
       }
     }
   ]
}
```

Wenn Sie mehrere Bedingungen oder mehrere Schlüssel in einer einzelnen Bedingung angeben, werden diese mit einer logischen UND-Operation ausgewertet. Wenn Sie eine einzelne Bedingung mit mehreren Werten für einen Schlüssel angeben, wird die Bedingung mit einer logischen ODER-Operation ausgewertet. Damit die Berechtigungen erteilt werden, müssen alle Bedingungen erfüllt sein.

Bei der Angabe von Bedingungen können Sie auch Platzhalter verwenden. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags (Markierungen) im IAM-Benutzerhandbuch.

> **Important**
>
> Einige API-Aktionen verwenden mehrere Ressourcen. Viele Bedingungsschlüssel sind jedoch ressourcenspezifisch. Wenn Sie eine Richtlinie mit einem Bedingungsschlüssel schreiben, legen Sie über das `Resource`-Element der Anweisung fest, für welche Ressource der Bedingungsschlüssel gültig ist. Andernfalls verhindert die Richtlinie möglicherweise, dass Benutzer die Aktion überhaupt ausführen, da die Bedingungsprüfung für die Ressourcen fehlschlägt, auf die der Bedingungsschlüssel nicht zutrifft. Wenn Sie keine Ressource angeben möchten oder über das `Action`-Element Ihrer Richtlinie mehrere API-Aktionen hinzugefügt haben, müssen Sie mit dem `...IfExists`-Bedingungstyp sicherstellen, dass der Bedingungsschlüssel für die Ressourcen, die ihn nicht verwenden, ignoriert wird. Weitere Informationen finden Sie unter... IfExists Bedingungen im IAM-Benutzerhandbuch.

Bedingungsschlüssel

- ec2:Attribute-Bedingungsschlüssel

- ec2:ResourceID-Bedingungsschlüssel
- ec2:SourceInstanceARN-Bedingungsschlüssel

ec2:Attribute-Bedingungsschlüssel

Der `ec2:Attribute`-Bedingungsschlüssel kann für Bedingungen verwendet werden, die den Zugriff nach einem Attribut einer Ressource filtern.

Dieser Bedingungsschlüssel unterstützt nur Eigenschaften eines primitiven Datentyps (wie Zeichenketten oder Ganzzahlen) oder komplexe AttributeValueObjekte, die nur eine Value-Eigenschaft enthalten (wie die Beschreibung oder ImdsSupportObjekte der ModifyImageAttributeAPI-Aktion). Der Bedingungsschlüssel kann nicht für komplexe Objekte verwendet werden, die mehrere Eigenschaften enthalten, wie z. B. das LaunchPermissionObjekt von ModifyImageAttribute.

Die folgende Richtlinie verwendet beispielsweise den `ec2:Attribute/Description` Bedingungsschlüssel, um den Zugriff nach dem komplexen Description-Objekt der ModifyImageAttributeAPI-Aktion zu filtern. Der Bedingungsschlüssel lässt nur Anforderungen zu, die die Beschreibung eines Images entweder in `Production` oder `Development` ändern.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute/Description": [
            "Production",
            "Development"
          ]
        }
      }
    }
  ]
}
```

Die folgende Beispielrichtlinie verwendet den `ec2:Attribute` Bedingungsschlüssel, um den Zugriff nach der primitiven Attributeigenschaft der ModifyImageAttributeAPI-Aktion zu filtern. Der Bedingungsschlüssel lehnt alle Anforderungen ab, die versuchen, die Beschreibung eines Images zu ändern.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute": "Description"
        }
      }
    }
  ]
}
```

ec2:ResourceID-Bedingungsschlüssel

Wenn Sie die folgenden `ec2:`*`Resource`*`ID`-Bedingungsschlüssel mit den angegebenen API-Aktionen verwenden, wird der Bedingungsschlüsselwert verwendet, um die resultierende Ressource anzugeben, die von der API-Aktion erstellt wird. `ec2:`*`Resource`*`ID`-Bedingungsschlüssel können nicht zum Angeben einer Quellressource verwendet werden, die in der API-Anfrage angegeben ist. Wenn Sie einen der folgenden `ec2:`*`Resource`*`ID`-Bedingungsschlüssel mit einer angegebenen API verwenden, müssen Sie immer den Platzhalter (*) angeben. Wenn Sie einen anderen Wert angeben, wird die Bedingung zur Laufzeit immer in * aufgelöst. Um beispielsweise den `ec2:ImageId` Bedingungsschlüssel mit der CopyImageAPI zu verwenden, müssen Sie den Bedingungsschlüssel wie folgt angeben:

JSON

```
{
```

```
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:ImageID": "*"
        }
      }
    }
  ]
}
```

Es wird empfohlen, die Verwendung von diesen Bedingungsschlüsseln bei diesen API-Aktionen zu vermeiden:

- `ec2:DhcpOptionsID` – `CreateDhcpOptions`
- `ec2:ImageID` – `CopyImage`, `CreateImage`, `ImportImage` und `RegisterImage`
- `ec2:InstanceID` – `RunInstances` und `ImportInstance`
- `ec2:InternetGatewayID` – `CreateInternetGateway`
- `ec2:NetworkAclID` – `CreateNetworkAcl`
- `ec2:NetworkInterfaceID` – `CreateNetworkInterface`
- `ec2:PlacementGroupName` – `CreatePlacementGroup`
- `ec2:RouteTableID` – `CreateRouteTable`
- `ec2:SecurityGroupID` – `CreateSecurityGroup`
- `ec2:SnapshotID` – `CopySnapshot`, `CreateSnapshot`, `CreateSnapshots` und `ImportSnapshots`
- `ec2:SubnetID` – `CreateSubnet`
- `ec2:VolumeID` – `CreateVolume` und `ImportVolume`
- `ec2:VpcID` – `CreateVpc`
- `ec2:VpcPeeringConnectionID` – `CreateVpcPeeringConnection`

Um den Zugriff nach einer bestimmten Ressource zu filtern IDs, empfehlen wir, das `Resource` Richtlinienelement wie folgt zu verwenden.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-01234567890abcdef"
    }
  ]
}
```

ec2:SourceInstanceARN-Bedingungsschlüssel

Verwenden Sie `ec2:SourceInstanceARN`, um den ARN der Instance anzugeben, von der aus eine Anfrage getätigt wird. Dies ist ein AWS globaler Bedingungsschlüssel, was bedeutet, dass Sie ihn mit anderen Diensten als Amazon verwenden können EC2. Eine Beispielrichtlinie finden Sie in Beispiel: Erlauben Sie einer bestimmten Instanz, Ressourcen in anderen AWS Diensten anzuzeigen.

Den Zugriff mithilfe des attributbasierten Zugriffs steuern

Wenn Sie eine IAM-Richtlinie erstellen, die Benutzern die Erlaubnis zur Nutzung von EC2 Ressourcen erteilt, können Sie Tag-Informationen in das `Condition` Element der Richtlinie aufnehmen, um den Zugriff anhand von Tags zu steuern. Dies wird als attributbasierte Zugriffskontrolle (ABAC) bezeichnet. ABAC bietet eine besser Kontrolle darüber, welche Ressourcen ein Benutzer ändern, verwenden oder löschen kann. Weitere Informationen finden Sie unter Was ist ABAC für AWS?

Beispielsweise können Sie eine Richtlinie erstellen, die es Benutzern ermöglicht, eine Instance zu beenden, aber die Aktion verweigert, wenn die Instance über den `environment=production`-Tag (Markierungen) verfügt. Dazu verwenden Sie den `aws:ResourceTag`-Bedingungsschlüssel, um den Zugriff auf die Ressource basierend auf den der Ressource zugewiesenen Tags (Markierung) zu erlauben oder zu verweigern.

```
"StringEquals": { "aws:ResourceTag/environment": "production" }
```

Informationen darüber, ob eine EC2 Amazon-API-Aktion die Zugriffskontrolle mithilfe des `aws:ResourceTag` Bedingungsschlüssels unterstützt, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2. Beachten Sie, dass die `Describe`-Aktionen keine Berechtigungen auf Ressourcenebene unterstützen, sodass sie in einer separaten Anweisung ohne Bedingungen angegeben werden müssen.

Beispiele für IAM-Richtlinien finden Sie unter Beispielrichtlinien zur Steuerung des Zugriffs auf die EC2 Amazon-API.

Wenn Sie Benutzern den Zugriff zu Ressourcen auf der Grundlage von Tags (Markierungen) gewähren oder verweigern, müssen Sie daran denken, Benutzern explizit das Hinzufügen und Entfernen dieser Tags (Markierungen) von den jeweiligen Ressourcen unmöglich zu machen. Andernfalls können Benutzer möglicherweise Ihre Einschränkungen umgehen und sich Zugriff auf eine Ressource verschaffen, indem sie ihre Tags (Markierungen) modifizieren.

Gewähren von Berechtigungen für Benutzer, Gruppen und Rollen

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Prüfen, ob Benutzer über die erforderlichen Berechtigungen verfügen

Nach der Erstellung einer IAM-Richtlinie sollten Sie zunächst überprüfen, ob damit den Benutzern die benötigten Berechtigungen zur Verwendung bestimmter API-Aktionen und Ressourcen erteilt werden. Anschließend können Sie die Richtlinie anwenden.

Erstellen Sie zunächst einen Benutzer zu Testzwecken und fügen Sie dann die von Ihnen erstellte IAM-Richtlinie dem Testbenutzer an. Anschließend initiieren Sie mit dem Testbenutzer eine Anforderung.

Wenn die EC2 Amazon-Aktion, die Sie testen, eine Ressource erstellt oder ändert, sollten Sie die Anfrage mit dem `DryRun` Parameter stellen (oder den AWS CLI Befehl mit der `--dry-run` Option ausführen). In diesem Fall schließt der Aufruf zwar die Autorisierungsprüfung, aber nicht die Operation ab. Beispielsweise können Sie prüfen, ob ein Benutzer eine bestimmte Instance beenden kann, ohne sie tatsächlich abzuschließen. Sofern der Testbenutzer über die erforderlichen Berechtigungen verfügt, gibt die Anforderung `DryRunOperation` zurück. Andernfalls wird `UnauthorizedOperation` zurückgegeben.

Falls die Richtlinie dem Benutzer nicht die erwarteten Berechtigungen erteilt oder zu viele Berechtigungen gewährt, können Sie die Richtlinie entsprechend anpassen und erneut testen, bis Sie die gewünschten Ergebnisse erhalten.

> **Important**
>
> Es kann einige Minuten dauern, bis Richtlinienänderungen wirksam werden. Daher wird empfohlen, fünf Minuten verstreichen zu lassen, bevor Sie die aktualisierte Richtlinie testen.

Bei einer fehlgeschlagenen Autorisierungsprüfung gibt die Anforderung eine codierte Nachricht mit Diagnoseinformationen zurück. Sie können die Nachricht mit der Aktion `DecodeAuthorizationMessage` decodieren. Weitere Informationen finden Sie DecodeAuthorizationMessagein der AWS Security Token Service API-Referenz und decode-authorization-message.

Beispielrichtlinien zur Steuerung des Zugriffs auf die EC2 Amazon-API

Sie können IAM-Richtlinien verwenden, um Benutzern die für die Arbeit mit Amazon EC2 erforderlichen Berechtigungen zu gewähren. step-by-stepAnweisungen finden Sie im IAM-Benutzerhandbuch unter Erstellen von IAM-Richtlinien.

Die folgenden Beispiele zeigen Richtlinienerklärungen, mit denen Sie Benutzern Berechtigungen zur Nutzung von Amazon gewähren können EC2. Diese Richtlinien sind für Anfragen konzipiert, die mit dem AWS CLI oder einem AWS SDK gestellt werden. Ersetzen Sie in den folgenden Beispielen jedes Beispiel *`user input placeholder`* durch Ihre eigenen Informationen.

Beispiele

- Beispiel: schreibgeschützter Zugriff
- Beispiel: Beschränken des Zugriffs auf eine bestimmte Region
- Arbeiten mit Instances
- Instanzen starten (RunInstances)
- Arbeiten mit Spot-Instances
- Beispiel: Arbeiten mit Reserved Instances
- Beispiel: Markieren von Ressourcen
- Beispiel: Arbeiten mit IAM-Rollen
- Beispiel: Arbeiten mit Routing-Tabellen
- Beispiel: Erlauben Sie einer bestimmten Instanz, Ressourcen in anderen AWS Diensten anzuzeigen
- Beispiel: Arbeiten mit Startvorlagen
- Arbeiten mit Instance-Metadaten
- Arbeiten Sie mit Amazon-EBS-Volumes und Snapshots

Richtlinien für die Arbeit in der EC2 Amazon-Konsole finden Sie beispielsweise unterBeispielrichtlinien zur Steuerung des Zugriffs auf die EC2 Amazon-Konsole.

Beispiel: schreibgeschützter Zugriff

Die folgende Richtlinie gewährt Benutzern die Erlaubnis, alle EC2 Amazon-API-Aktionen zu verwenden, deren Namen mit beginnen`Describe`. Das `Resource`-Element verwendet einen Platzhalter, wodurch Benutzer alle Ressourcen mit diesen API-Aktionen angeben können. Das Sternchen (*) als Platzhalter ist auch dann erforderlich, wenn die API-Aktion keine Berechtigungen auf Ressourcenebene unterstützt. Weitere Informationen darüber, welche EC2 Amazon-API-Aktionen ARNs Sie verwenden können, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2.

Die Benutzer haben keine Berechtigung zum Ausführen von Aktionen auf den Ressourcen (es sei denn, eine andere Anweisung erteilt ihnen diese Erlaubnis), da ihnen die Berechtigung für die Verwendung von API-Aktionen standardmäßig verweigert wird.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    }
   ]
}
```

Beispiel: Beschränken des Zugriffs auf eine bestimmte Region

Die folgende Richtlinie verweigert Benutzern die Erlaubnis, alle EC2 Amazon-API-Aktionen zu verwenden, es sei denn, die Region ist Europa (Frankfurt). Es verwendet den globalen Bedingungsschlüssel`aws:RequestedRegion`, der von allen EC2 Amazon-API-Aktionen unterstützt wird.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "eu-central-1"
        }
      }
    }
```

```
  ]
}
```

Alternativ können Sie den Bedingungsschlüssel verwenden`ec2:Region`, der für Amazon spezifisch ist EC2 und von allen EC2 Amazon-API-Aktionen unterstützt wird.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ec2:Region": "eu-central-1"
        }
      }
    }
  ]
}
```

Arbeiten mit Instances

Beispiele

- Beispiel: Beschreiben, Initiieren, Stoppen, Starten und Beenden aller Instances
- Beispiel: Beschreiben aller Instances sowie Stoppen, Starten und Beenden nur bestimmter Instances

Beispiel: Beschreiben, Initiieren, Stoppen, Starten und Beenden aller Instances

Mit der folgenden Richtlinie wird Benutzern Berechtigungen erteilt, die im Element `Action` angegebenen API-Aktionen zu verwenden. Das `Resource`-Element verwendet den Platzhalter "*", wodurch Benutzer alle Ressourcen mit diesen API-Aktionen angeben können. Das Sternchen (*) als Platzhalter ist auch dann erforderlich, wenn die API-Aktion keine Berechtigungen auf

Ressourcenebene unterstützt. Weitere Informationen darüber, welche EC2 Amazon-API-Aktionen ARNs Sie verwenden können, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2.

Die Benutzer haben keine Berechtigung zur Verwendung von anderen API-Aktionen (es sei denn, eine andere Anweisung erteilt ihnen die entsprechende Erlaubnis), da den Benutzern die Berechtigung für die Verwendung von API-Aktionen standardmäßig verweigert wird.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": "*"
    }
   ]
}
```

Beispiel: Beschreiben aller Instances sowie Stoppen, Starten und Beenden nur bestimmter Instances

Die folgende Richtlinie erlaubt den Benutzern, alle Instances zu beschreiben, nur die Instances i-1234567890abcdef0 und i-0598c7d356eba48d7 zu starten und anzuhalten sowie ausschließlich Instances in der Region `us-east-1` mit dem Ressourcen-Tag „`purpose=test`“ zu beenden.

In der ersten Anweisung legt ein *-Platzhalter im `Resource`-Element fest, dass die Benutzer alle Ressourcen für die Aktion angeben können. In diesem Beispiel können sie alle Instances auflisten. Das Sternchen (*) als Platzhalter ist auch dann erforderlich, wenn die API-Aktion keine

Berechtigungen auf Ressourcenebene unterstützt (in diesem Fall `ec2:DescribeInstances`). Weitere Informationen darüber, welche EC2 Amazon-API-Aktionen ARNs Sie verwenden können, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2.

Die zweite Anweisung erteilt Berechtigungen auf Ressourcenebene für die Aktionen `StopInstances` und `StartInstances`. Die spezifischen Instanzen werden durch ihre Eigenschaften ARNs im `Resource` Element gekennzeichnet.

Die dritte Anweisung ermöglicht es Benutzern, alle Instances in der `us-east-1` Region zu beenden, die zu dem angegebenen AWS Konto gehören, aber nur dort, wo die Instanz das Tag hat`"purpose=test"`. Das `Condition`-Element bestimmt, wann die Richtlinienanweisung wirksam ist.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
   {
   "Effect": "Allow",
      "Action": "ec2:DescribeInstances",
      "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/i-1234567890abcdef0",
        "arn:aws:ec2:us-east-1:111122223333:instance/i-0598c7d356eba48d7"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "ec2:TerminateInstances",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
      "Condition": {
         "StringEquals": {
            "aws:ResourceTag/purpose": "test"
         }
```

```
        }
    }

    ]
}
```

Instanzen starten (RunInstances)

Die RunInstancesAPI-Aktion startet eine oder mehrere On-Demand-Instances oder eine oder mehrere Spot-Instances. `RunInstances`benötigt ein AMI und erstellt eine Instanz. Benutzer können in der Anforderung ein Schlüsselpaar und eine Sicherheitsgruppe angeben. Der Start in einer VPC erfordert ein Subnetz und generiert eine Netzwerkschnittstelle. Beim Starten von einem Amazon EBS-Backed AMI wird ein Volume erstellt. Daher muss der Benutzer über Berechtigungen zur Nutzung dieser EC2 Amazon-Ressourcen verfügen. Sie können eine Richtlinienanweisung erstellen, damit die Benutzer einen optionalen Parameter für `RunInstances` angeben müssen oder die Werte einschränken, die den Benutzern für einen Parameter gestattet sind.

Weitere Informationen zu den Berechtigungen auf Ressourcenebene, die zum Starten einer Instance erforderlich sind, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon. EC2

Standardmäßig verfügen Benutzer nicht über Berechtigungen, die resultierenden Instances zu beschreiben, zu starten, anzuhalten oder zu beenden. Eine Möglichkeit, den Benutzern die Berechtigung zum Verwalten der resultierenden Instances zu erteilen, besteht darin, ein spezielles Tags (Markierung) für jede Instance und eine Anweisung zu erstellen, welche dazu dient, die Instances mit diesem Tag (Markierung) zu verwalten. Weitere Informationen finden Sie unter Arbeiten mit Instances.

Ressourcen

- AMIs
- Instance-Typen
- Subnets
- EBS-Datenträger
- Tags (Markierungen)
- Tags (Markierungen) in einer Startvorlage
- Elastisch GPUs
- Startvorlagen

AMIs

Die folgende Richtlinie ermöglicht es Benutzern, Instances nur mit den angegebenen AMIs, `ami-9e1670f7` und zu starten. `ami-45cf5c3c` Die Benutzer können eine Instance nicht mit anderen starten AMIs (es sei denn, eine andere Anweisung erteilt den Benutzern die Erlaubnis dazu).

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:us-east-1::image/ami-9e1670f7",
        "arn:aws:ec2:us-east-1::image/ami-45cf5c3c",
        "arn:aws:ec2:us-east-1:111122223333:instance/*",
        "arn:aws:ec2:us-east-1:111122223333:volume/*",
        "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
        "arn:aws:ec2:us-east-1:111122223333:security-group/*",
        "arn:aws:ec2:us-east-1:111122223333:subnet/*",
        "arn:aws:ec2:us-east-1:111122223333:network-interface/*"
      ]
    }
   ]
}
```

Alternativ ermöglicht die folgende Richtlinie Benutzern, Instances von allen Anbietern von AMIs Amazon oder bestimmten vertrauenswürdigen und verifizierten Partnern aus zu starten. Das `Condition`-Element in der ersten Anweisung überprüft, ob `ec2:Owner` `amazon` ist. Die Benutzer können eine Instance nicht mit anderen starten AMIs (es sei denn, eine andere Erklärung erteilt den Benutzern die Erlaubnis dazu).

JSON

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

```
            {
         "Effect": "Allow",
         "Action": "ec2:RunInstances",
         "Resource": [
            "arn:aws:ec2:us-east-1::image/ami-*"
         ],
         "Condition": {
            "StringEquals": {
               "ec2:Owner": "amazon"
            }
         }
      },
      {
         "Effect": "Allow",
         "Action": "ec2:RunInstances",
         "Resource": [
            "arn:aws:ec2:us-east-1:111122223333:instance/*",
            "arn:aws:ec2:us-east-1:111122223333:subnet/*",
            "arn:aws:ec2:us-east-1:111122223333:volume/*",
            "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
            "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
            "arn:aws:ec2:us-east-1:111122223333:security-group/*"
            ]
         }
      ]
}
```

Instance-Typen

Die folgende Richtlinie gestattet es Benutzern, Instances nur mit dem `t2.micro`- oder `t2.small`-Instance-Typ zu starten, wodurch die Kosten kontrolliert werden können. Die Benutzer können keine größeren Instances starten, da das `Condition`-Element der ersten Anweisung überprüft, ob `ec2:InstanceType` entweder `t2.micro` oder `t2.small` ist.

JSON

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

```
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1:111122223333:instance/*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1::image/ami-*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:volume/*",
         "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
         "arn:aws:ec2:us-east-1:111122223333:security-group/*"
         ]
      }
   ]
}
```

Sie können alternativ eine Richtlinie erstellen, die Benutzern Berechtigungen zum Starten aller Instances, mit Ausnahme der Instance-Typen `t2.micro` und `t2.small`, verweigert.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
        {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1:111122223333:instance/*"
      ],
      "Condition": {
         "StringNotEquals": {
```

```
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1::image/ami-*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:instance/*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:volume/*",
         "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
         "arn:aws:ec2:us-east-1:111122223333:security-group/*"
         ]
      }
   ]
}
```

Subnets

Die folgende Richtlinie erlaubt den Benutzern, Instances ausschließlich im angegebenen Subnetz, `subnet-12345678`, zu starten. Die Gruppe kann keine Instances in einem anderen Subnetz starten (es sei denn, eine andere Anweisung gewährt den Benutzern die entsprechende Berechtigung).

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:subnet/subnet-12345678",
        "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
        "arn:aws:ec2:us-east-1:111122223333:instance/*",
        "arn:aws:ec2:us-east-1:111122223333:volume/*",
        "arn:aws:ec2:us-east-1::image/ami-*",
        "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
```

```
        "arn:aws:ec2:us-east-1:111122223333:security-group/*"
      ]
    }
  ]
}
```

Alternativ können Sie eine Richtlinie erstellen, die Benutzern Berechtigungen zum Starten einer Instance in jedem anderen Subnetz verweigert. Zu diesem Zweck verweigert die Anweisung die Berechtigung zum Erstellen einer Netzwerkschnittstelle, außer wenn das `subnet-12345678`-Subnetz festgelegt wird. Diese Verweigerung setzt alle anderen Richtlinien außer Kraft, die erstellt werden, um zu gestatten, Instances in anderen Subnetzen zu starten.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
         {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*"
      ],
      "Condition": {
         "ArnNotEquals": {
            "ec2:Subnet": "arn:aws:ec2:us-east-1:111122223333:subnet/
subnet-12345678"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:us-east-1::image/ami-*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:instance/*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:volume/*",
         "arn:aws:ec2:us-east-1:111122223333:key-pair/*",
         "arn:aws:ec2:us-east-1:111122223333:security-group/*"
```

```
        ]
      }
   ]
}
```

EBS-Datenträger

Die Richtlinie unten ermöglicht es den Benutzern, Instances nur zu starten, wenn die EBS-Volumes für die Instance verschlüsselt sind. Der Benutzer muss eine Instance von einem AMI starten, das mit verschlüsselten Snapshots erstellt wurde, um sicherzustellen, dass das Stamm-Volume verschlüsselt wird. Jedes weitere Volume, das der Instance während des Starts vom Benutzer angefügt wird, muss auch verschlüsselt sein.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
                {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Bool": {
                    "ec2:Encrypted": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
```

```
        }
    ]
}
```

Tags (Markierungen)

Markieren von Instances bei der Erstellung

Die folgende Richtlinie gestattet es den Benutzern, Instances zu starten und sie während ihrer Erstellung zu markieren. Bei Aktionen zur Ressourcenerstellung, die Tags anwenden, müssen Benutzer über Berechtigungen für die Aktion `CreateTags` verfügen. Die zweite Anweisung enthält den `ec2:CreateAction`-Bedingungsschlüssel, sodass die Benutzer Tags nur im Kontext von `RunInstances` und nur für Instances erstellen können. Die Benutzer können keine vorhandenen Ressourcen mit Tags versehen und Volumes nicht mit der `RunInstances`-Anforderung markieren.

Weitere Informationen finden Sie unter Erteilen Sie die Erlaubnis, EC2 Amazon-Ressourcen während der Erstellung zu taggen.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
```

```
    }
  ]
}
```

Markieren von Instances und Volumes bei der Erstellung mit bestimmten Tags

Die folgende Richtlinie umfasst den `aws:RequestTag`-Bedingungsschlüssel. Die Benutzer müssen daher alle Instances und Volumes, die durch `RunInstances` erstellt werden, mit den Tags `environment=production` und `purpose=webserver` versehen. Werden nicht genau diese Tags (Markierungen) übergeben oder überhaupt keine Tags (Markierungen) angegeben, schlägt die Anforderung fehl.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:us-east-1::image/*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
         "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:us-east-1:111122223333:security-group/*",
         "arn:aws:ec2:us-east-1:111122223333:key-pair/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
          "arn:aws:ec2:us-east-1:111122223333:volume/*",
          "arn:aws:ec2:us-east-1:111122223333:instance/*"
      ],
      "Condition": {
         "StringEquals": {
```

```
            "aws:RequestTag/environment": "production" ,
            "aws:RequestTag/purpose": "webserver"
         }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
         "StringEquals": {
            "ec2:CreateAction" : "RunInstances"
         }
       }
    }
  ]
}
```

Markieren von instances und Volumes bei der Erstellung mit mindestens einem bestimmten Tag

Die Richtlinie unten verwendet den `ForAnyValue`-Modifikator für die `aws:TagKeys`-Bedingung, um festzulegen, dass mindestens ein Tag (Markierung) in der Anforderung angegeben werden muss und der `environment`- oder `webserver`-Schlüssel enthalten sein muss. Das Tag (Markierung) muss sowohl auf Instances als auch auf Volumes angewendet werden. In der Anforderung können beliebige Tags (Markierungen)-Werte angegeben werden.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:us-east-1::image/*",
         "arn:aws:ec2:us-east-1:111122223333:subnet/*",
```

```
            "arn:aws:ec2:us-east-1:111122223333:network-interface/*",
            "arn:aws:ec2:us-east-1:111122223333:security-group/*",
            "arn:aws:ec2:us-east-1:111122223333:key-pair/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:RunInstances"
        ],
        "Resource": [
            "arn:aws:ec2:us-east-1:111122223333:volume/*",
            "arn:aws:ec2:us-east-1:111122223333:instance/*"
        ],
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": ["environment","webserver"]
            }
         }
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags"
        ],
        "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
        "Condition": {
            "StringEquals": {
                "ec2:CreateAction" : "RunInstances"
            }
         }
    }
  ]
}
```

Wenn Instances bei der Erstellung markiert werden, müssen sie mit einem bestimmten Tag markiert sein

In der folgenden Richtlinie ist es nicht notwendig, dass die Benutzer in der Anforderung Tags (Markierungen) angeben, aber wenn sie dies tun, muss es das Tag (Markierungen) `purpose=test` sein. Andere Tags (Markierungen) sind nicht zulässig. Die Benutzer können in der `RunInstances`-Anforderung die Tags auf jede Ressource anwenden, die mit Tags versehen werden kann.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/purpose": "test",
             "ec2:CreateAction" : "RunInstances"
          },
          "ForAllValues:StringEquals": {
              "aws:TagKeys": "purpose"
          }
       }
    }
  ]
}
```

Um jeden Benutzer zu verbieten, der Tag auf create for aufgerufen hat RunInstances

JSON

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

```
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Erlaube nur bestimmte Tags für spot-instances-request. Hier kommt die überraschende Inkonsistenz Nr. 2 ins Spiel. Unter normalen Umständen führt das Angeben von keinen Tags (Markierungen) zu „Unauthenticated (Nicht authentifiziert)“. Im Fall von wird diese Richtlinie nicht ausgewertet spot-instances-request, wenn keine spot-instances-request Tags vorhanden sind, sodass eine Spot-on-Run-Anfrage ohne Tags erfolgreich ist.

Tags (Markierungen) in einer Startvorlage

Im folgenden Beispiel können Benutzer Instances starten, jedoch nur über eine bestimmte Startvorlage (`lt-09477bcd97b0d310e`). Durch den Bedingungsschlüssel `ec2:IsLaunchTemplateResource` werden Benutzer daran gehindert, in der Startvorlage angegebene Ressourcen außer Kraft zu setzen. Der zweite Teil der Anweisung erlaubt Benutzern das Markieren von Instances bei der Erstellung – dieser Teil der Anweisung wird benötigt, wenn in der Startvorlage Tags (Markierungen) für die Instance angegeben werden.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/lt-09477bcd97b0d310e"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Elastisch GPUs

In der folgenden Richtlinie können Benutzer eine Instance starten und eine elastische GPU zum Anfügen an die Instance angeben. Benutzer können Instances in jeder Region starten, das Anfügen einer elastischen GPU ist beim Start jedoch nur in der Region `us-east-2` möglich.

Der `ec2:ElasticGpuType`-Bedingungsschlüssel stellt sicher, dass Instances entweder den Elastic `eg1.medium`- oder `eg1.large`-GPU-Typ verwenden.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
             {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:111122223333:elastic-gpu/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-2",
                    "ec2:ElasticGpuType": [
                        "eg1.medium",
                        "eg1.large"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:111122223333:network-interface/*",
                "arn:aws:ec2:*:111122223333:instance/*",
                "arn:aws:ec2:*:111122223333:subnet/*",
                "arn:aws:ec2:*:111122223333:volume/*",
                "arn:aws:ec2:*:111122223333:key-pair/*",
                "arn:aws:ec2:*:111122223333:security-group/*"
            ]
        }
    ]
}
```

Startvorlagen

Im folgenden Beispiel können Benutzer Instances starten, jedoch nur über eine bestimmte Startvorlage (`lt-09477bcd97b0d310e`). Benutzer können die Parameter in der Startvorlage außer Kraft setzen, indem sie die Parameter in der Aktion `RunInstances` angeben.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
         {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/lt-09477bcd97b0d310e"
          }
       }
    }
  ]
}
```

In diesem Beispiel können Benutzer Instances nur starten, wenn sie eine Startvorlage verwenden. Die Richtlinie verwendet den `ec2:IsLaunchTemplateResource` Bedingungsschlüssel, um zu verhindern, dass Benutzer bereits ARNs in der Startvorlage vorhandene Werte überschreiben.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
         {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
```

```
            "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/*"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

Die folgende Beispielsrichtlinie erlaubt einem Benutzer, Instances zu starten, jedoch nur über eine Startvorlage. Benutzer können in der Anforderung keine Subnetz- und Netzwerkschnittstellen-Parameter außer Kraft setzen. Diese Parameter können nur in der Startvorlage angegeben werden. Im ersten Teil der Anweisung wird das NotResourceElement verwendet, um alle anderen Ressourcen außer Subnetzen und Netzwerkschnittstellen zuzulassen. Der zweite Teil der Anweisung erlaubt die Subnetz- und Netzwerkschnittstellen-Ressourcen, jedoch nur, wenn sie ihren Ursprung in der Startvorlage haben.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": ["arn:aws:ec2:us-east-1:111122223333:subnet/*",
                      "arn:aws:ec2:us-east-1:111122223333:network-interface/*" ],
      "Condition": {
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/*"
          }
       }
    },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": ["arn:aws:ec2:us-east-1:111122223333:subnet/*",
```

```
                  "arn:aws:ec2:us-east-1:111122223333:network-interface/*" ],
      "Condition": {
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/*"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

Das folgende Beispiel erlaubt Benutzern, Instances zu starten, jedoch nur über eine Startvorlage und wenn die Startvorlage den Tag (Markierungen) `Purpose=Webservers` aufweist. Benutzer können mit der Aktion `RunInstances` keine Parameter der Startvorlage außer Kraft setzen.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
      "Condition": {
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:us-east-1:111122223333:launch-
template/*"
          },
         "Bool": {
            "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
```

```
      "Condition": {
       "StringEquals": {
           "aws:ResourceTag/Purpose": "Webservers"
        }
       }
     }
  ]
}
```

Arbeiten mit Spot-Instances

Sie können die RunInstances Aktion verwenden, um Spot-Instance-Anfragen zu erstellen und die Spot-Instance-Anfragen bei der Erstellung zu taggen. Die Ressource, für die Sie angeben müssen, RunInstances ist`spot-instances-request`.

Die `spot-instances-request`-Ressource wird in der IAM-Richtlinie wie folgt ausgewertet:

- Wenn Sie eine Spot-Instance-Anfrage bei der Erstellung EC2 nicht taggen, bewertet Amazon die `spot-instances-request` Ressource in der RunInstances Abrechnung nicht.
- Wenn Sie eine Spot-Instance-Anfrage bei der Erstellung taggen, EC2 bewertet Amazon die `spot-instances-request` Ressource in der RunInstances Abrechnung.

Daher gelten für die `spot-instances-request`-Ressource die folgenden Regeln für die IAM-Richtlinie:

- Wenn Sie RunInstances eine Spot-Instance-Anfrage erstellen und nicht beabsichtigen, die Spot-Instance-Anfrage bei der Erstellung zu taggen, müssen Sie die `spot-instances-request` Ressource nicht explizit zulassen. Der Aufruf ist erfolgreich.
- Wenn Sie RunInstances eine Spot-Instance-Anfrage erstellen und beabsichtigen, die Spot-Instance-Anfrage bei der Erstellung zu taggen, müssen Sie die `spot-instances-request` Ressource in die RunInstances Allow-Anweisung aufnehmen, andernfalls schlägt der Aufruf fehl.
- Wenn Sie RunInstances eine Spot-Instance-Anfrage erstellen und beabsichtigen, die Spot-Instance-Anfrage bei der Erstellung zu taggen, müssen Sie die `spot-instances-request` Ressource oder den * Platzhalter in der Allow-Anweisung CreateTags angeben, andernfalls schlägt der Aufruf fehl.

Sie können Spot-Instances mit RunInstances oder RequestSpotInstances anfordern. Die folgenden Beispiel-IAM-Richtlinien gelten nur, wenn Spot-Instances über RunInstances angefordert werden.

Beispiel: Spot-Instances anfordern mit RunInstances

Die folgende Richtlinie ermöglicht es Benutzern, Spot-Instances mithilfe der RunInstances Aktion anzufordern. Die `spot-instances-request` Ressource, die von erstellt wurde RunInstances, fordert Spot-Instances an.

> **Note**
>
> Um Spot-Instance-Anfragen RunInstances zu erstellen, können Sie sie `spot-instances-request` aus der `Resource` Liste streichen, wenn Sie nicht beabsichtigen, die Spot-Instance-Anfragen bei der Erstellung zu taggen. Dies liegt daran, dass Amazon die `spot-instances-request` Ressource in der RunInstances Anweisung EC2 nicht bewertet, wenn die Spot-Instance-Anfrage bei create nicht markiert ist.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        }
    ]
```

```
}
```

⚠ Warning

NICHT UNTERSTÜTZT — Beispiel: Benutzern die Erlaubnis verweigern, Spot-Instances anzufordern mit RunInstances
Die folgende Richtlinie wird für die `spot-instances-request`-Ressource nicht unterstützt. Die folgende Richtlinie soll Benutzern die Berechtigung zum Starten von On-Demand-Instances erteilen, ihnen jedoch die Berechtigung zum Anfordern von Spot-Instances verweigern. Die `spot-instances-request` Ressource, die von erstellt wurde RunInstances, ist die Ressource, die Spot-Instances anfordert. Die zweite Anweisung soll die RunInstances Aktion für die `spot-instances-request` Ressource verweigern. Diese Bedingung wird jedoch nicht unterstützt, da Amazon die `spot-instances-request` Ressource in der RunInstances Anweisung EC2 nicht bewertet, wenn die Spot-Instance-Anfrage bei create nicht markiert ist.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequestsNOTSUPPORTEDDONOTUSE",
```

```
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
        }
    ]
}
```

Beispiel: Markieren von Spot-Instance-Anforderungen beim Erstellen

Die folgende Richtlinie ermöglicht es Benutzern, alle Ressourcen zu markieren, die während des Instance-Starts erstellt werden. Die erste Anweisung ermöglicht RunInstances das Erstellen der aufgelisteten Ressourcen. Die `spot-instances-request` Ressource, die von erstellt wurde RunInstances, ist die Ressource, die Spot-Instances anfordert. Die zweite Anweisung stellt einen *-Platzhalter bereit, mit dem alle Ressourcen markiert werden können, wenn sie beim Start der Instance erstellt werden.

> **Note**
>
> Wenn Sie eine Spot-Instance-Anfrage bei der Erstellung taggen, EC2 bewertet Amazon die `spot-instances-request` Ressource in der RunInstances Abrechnung. Daher müssen Sie die `spot-instances-request` Ressource für die RunInstances Aktion ausdrücklich zulassen, andernfalls schlägt der Aufruf fehl.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
```

```
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Beispiel: Markieren beim Erstellen von Spot-Instance-Anforderungen verweigern

Die folgende Richtlinie verweigert Benutzern die Berechtigung zum Markieren der Ressourcen, die während des Instance-Starts erstellt werden.

Die erste Anweisung ermöglicht RunInstances das Erstellen der aufgelisteten Ressourcen. Die `spot-instances-request` Ressource, die von erstellt wurde RunInstances, ist die Ressource, die Spot-Instances anfordert. Die zweite Anweisung stellt einen *-Platzhalter bereit, um alle Ressourcen zu verweigern, die markiert werden, wenn sie beim Start der Instance erstellt werden. Wenn `spot-instances-request` oder eine andere Ressource bei create markiert ist, schlägt der RunInstances Aufruf fehl.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
```

```
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenyTagResources",
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Warning

NICHT UNTERSTÜTZT – Beispiel: Erstellen einer Spot-Instance-Anforderung nur zulassen, wenn ihr ein bestimmtes Tag (Markierung) zugewiesen wird

Die folgende Richtlinie wird für die `spot-instances-request`-Ressource nicht unterstützt. Die folgende Richtlinie soll nur dann RunInstances die Erlaubnis zum Erstellen einer Spot-Instance-Anfrage gewähren, wenn die Anfrage mit einem bestimmten Tag gekennzeichnet ist. Die erste Anweisung ermöglicht es RunInstances , die aufgelisteten Ressourcen zu erstellen. Die zweite Anweisung soll Benutzern nur dann die Berechtigung erteilen, eine Spot-Instance-Anforderung zu erstellen, wenn die Anforderung den Tag (Markierung) `environment=production` enthält. Wenn diese Bedingung auf andere Ressourcen angewendet wird, die von erstellt wurden RunInstances, führt die Angabe keiner Tags zu einem `Unauthenticated` Fehler. Wenn jedoch keine Tags für die Spot-Instance-Anfrage angegeben sind, bewertet Amazon die `spot-instances-request` Ressource in der RunInstances Abrechnung EC2 nicht, was dazu führt, dass Spot-Instance-Anfragen ohne Tags von RunInstances erstellt werden.

Beachten Sie, dass die Angabe eines anderen Tags als zu einem `Unauthenticated` Fehler `environment=production` führt, denn wenn ein Benutzer eine Spot-Instance-Anfrage taggt, EC2 bewertet Amazon die `spot-instances-request` Ressource in der RunInstances Anweisung.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid":
 "RequestSpotInstancesOnlyIfTagIsEnvironmentProductionNOTSUPPORTEDDONOTUSE",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/
*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }

    ]
```

```
}
```

Beispiel: Erstellen einer Spot-Instance-Anforderung verweigern, wenn ihr ein bestimmtes Tag (Markierung) zugewiesen ist

Die folgende Richtlinie verweigert RunInstances die Erlaubnis, eine Spot-Instance-Anfrage zu erstellen, wenn die Anfrage mit gekennzeichnet ist. `environment=production`

Die erste Anweisung ermöglicht RunInstances das Erstellen der aufgelisteten Ressourcen.

Die zweite Anweisung verweigert Benutzern die Berechtigung, eine Spot-Instance-Anforderung zu erstellen, wenn die Anforderung den Tag (Markierung) `environment=production` enthält. Die Angabe von `environment=production` als Tag führt zu einem `Unauthenticated`-Fehler. Wenn Sie andere oder keine Tags (Markierungen) angeben, wird eine Spot-Instance-Anforderung erstellt.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequests",
            "Effect": "Deny",
```

```
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Beispiel: Arbeiten mit Reserved Instances

Mit der folgenden Richtlinie wird Benutzern die Berechtigung zum Ansehen, Ändern und Kaufen von Reserved Instances in Ihrem Konto gewährt.

Für einzelne Reserved Instances können keine Berechtigungen auf Ressourcenebene erteilt werden. Diese Richtlinie bedeutet, dass die Benutzer Zugriff auf alle Reserved Instances im Konto haben.

Der Platzhalter * im Element `Resource` legt fest, dass Benutzer alle Ressourcen für die Aktion angeben können. In diesem Beispiel können sie alle Reserved Instances im Konto auflisten und bearbeiten. Sie haben auch die Möglichkeit, die Kontoanmeldeinformationen zu verwenden, um Reserved Instances zu kaufen. Das Sternchen (*) als Platzhalter ist auch dann erforderlich, wenn die API-Aktion keine Berechtigungen auf Ressourcenebene unterstützt.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
```

```
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeReservedInstancesOfferings"
      ],
      "Resource": "*"
    }
   ]
}
```

Benutzern wird die Berechtigung zum Ansehen und Ändern der Reserved Instances in Ihrem Konto erteilt, aber nicht zum Kauf von neuen Reserved Instances.

JSON

```
{
  "Version":"2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource": "*"
    }
  ]
}
```

Beispiel: Markieren von Ressourcen

Die folgende Richtlinie erlaubt Benutzern nur die Verwendung der `CreateTags`-Aktion, um einer Instance Tags hinzuzufügen, wenn das Tag den `environment`-Schlüssel und den `production`-Wert enthält. Es sind keine anderen Tags erlaubt und der Benutzer kann keine anderen Ressourcentypen markieren.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        }
    ]
}
```

Die Richtlinie unten ermöglicht es den Benutzern, jede markierbare Ressource, die bereits ein Tag mit dem `owner`-Schlüssel und einen Benutzernamen als Wert aufweist, mit Tags zu versehen. Zudem müssen die Benutzer ein Tag (Markierung) mit dem `anycompany:environment-type`-Schlüssel und dem Wert `test` oder `prod` in der Anforderung festlegen. Die Benutzer können zusätzliche Tags (Markierungen) in der Anforderung angeben.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/anycompany:environment-type":
 ["test","prod"],
                    "aws:ResourceTag/owner": "${aws:username}"
                }
```

```
            }
        }
    ]
}
```

Sie können eine IAM-Richtlinie erstellen, die den Benutzern erlaubt, bestimmte Tags (Markierungen) für eine Ressource zu löschen. Die folgende Richtlinie gestattet es den Benutzern zum Beispiel, Tags für ein Volume zu löschen, sofern die Anforderung die Tag-Schlüssel `environment` oder `cost-center` enthält. Für den Tag (Markierung) kann ein beliebiger Wert angegeben werden, aber der Tag (Markierung)-Schlüssel muss einem der genannten Schlüssel entsprechen.

> **Note**
>
> Wenn Sie eine Ressource löschen, werden alle der Ressource zugeordneten Tags (Markierungen) ebenfalls gelöscht. Die Benutzer benötigen keine Berechtigungen für die Verwendung der Aktion `ec2:DeleteTags`, um eine Ressource zu löschen, die Tags aufweist. Sie müssen nur über Berechtigungen zum Ausführen der Löschaktion verfügen.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Allow",
      "Action": "ec2:DeleteTags",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:volume/*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment","cost-center"]
        }
      }
    }
  ]
}
```

Diese Richtlinie erlaubt den Benutzern, auf beliebigen Ressourcen nur den `environment=prod`-Tag zu löschen. Dies gilt zudem nur, wenn die Ressource bereits den `owner`-Schlüssel-Tag und einen Benutzernamen als Wert aufweist. Benutzer können keine anderen Tags für eine Ressource löschen.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
      {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/environment": "prod",
          "aws:ResourceTag/owner": "${aws:username}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment"]
        }
      }
    }
  ]
}
```

Beispiel: Arbeiten mit IAM-Rollen

Die folgende Richtlinie erlaubt Benutzern das Anfügen, Ersetzen und Trennen einer IAM-Rolle für Instances, die über den `department=test`-Tag (Markierung) verfügt. Das Ersetzen oder Trennen einer IAM-Rolle erfordert eine Zuordnungs-ID. Die Richtlinie erteilt den Benutzern daher außerdem die Berechtigung, die `ec2:DescribeIamInstanceProfileAssociations`-Aktion zu verwenden.

Die Benutzer müssen über die Berechtigung für die `iam:PassRole`-Aktion verfügen, um die Rollen an die Instance zu übergeben.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department":"test"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeIamInstanceProfileAssociations",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::111122223333:role/DevTeam*"
    }
  ]
}
```

Die folgende Richtlinie erlaubt Benutzern das Anfügen oder Ersetzen einer IAM-Rolle für eine beliebige Instance. Es können nur IAM-Rollen angefügt oder ersetzt werden, deren Namen mit `TestRole-` beginnen. Stellen Sie bei der `iam:PassRole`-Aktion sicher, dass Sie den Namen der IAM-Rolle und nicht den des Instance-Profils angeben, falls sich diese Namen unterscheiden. Weitere Informationen finden Sie unter Instance-Profile.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateIamInstanceProfile",
                "ec2:ReplaceIamInstanceProfileAssociation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeIamInstanceProfileAssociations",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/TestRole-*"
        }
    ]
}
```

Beispiel: Arbeiten mit Routing-Tabellen

Die folgende Richtlinie ermöglicht Benutzern das Hinzufügen, Entfernen und Ersetzen von Routings für Routing-Tabellen, die nur mit VPC `vpc-ec43eb89` verbunden sind. Zur Angabe einer VPC für den Bedingungsschlüssel `ec2:Vpc` müssen Sie den vollständigen ARN der VPC angeben.

JSON

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

```
                "ec2:DeleteRoute",
                "ec2:CreateRoute",
                "ec2:ReplaceRoute"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1:111122223333:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Vpc": "arn:aws:ec2:us-east-1:111122223333:vpc/vpc-
ec43eb89"
                }
            }
        }
    ]
}
```

Beispiel: Erlauben Sie einer bestimmten Instanz, Ressourcen in anderen AWS Diensten anzuzeigen

Nachfolgend finden Sie ein Beispiel für eine Richtlinie, die Sie einer IAM-Rolle anhängen können. Die Richtlinie ermöglicht es einer Instanz, Ressourcen in verschiedenen AWS Diensten anzuzeigen. Sie geben mit dem Bedingungsschlüssel `ec2:SourceInstanceARN` an, dass es sich bei der Instance, von der die Anforderung ausging, um die Instance `i-093452212644b0dd6` handeln muss. Wenn die gleiche IAM-Rolle mit einer anderen Instance verbunden ist, kann die andere Instance keine dieser Aktionen ausführen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVolumes",
                "s3:ListAllMyBuckets",
                "dynamodb:ListTables",
                "rds:DescribeDBInstances"
            ],
```

```
            "Resource": [
                "*"
            ],
            "Condition": {
                "ArnEquals": {
                    "ec2:SourceInstanceARN": "arn:aws:ec2:us-
east-1:111122223333:instance/i-0934522126 44b0dd6"
                }
            }
        }
    ]
}
```

Beispiel: Arbeiten mit Startvorlagen

Die folgende Richtlinie erlaubt Benutzern, eine Startvorlagenversion zu erstellen und eine Startvorlage zu bearbeiten, jedoch nur für eine bestimmte Startvorlage (`lt-09477bcd97b0d3abc`). Benutzer können nicht mit anderen Startvorlagen arbeiten.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
   {
      "Action": [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/
lt-09477bcd97b0d3abc"
    }
  ]
}
```

Die folgende Richtlinie erlaubt Benutzern, eine Startvorlage und Startvorlagenversion zu löschen, vorausgesetzt, dass die Startvorlage den Tag (Markierungen) `Purpose=Testing` aufweist.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Action": [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:us-east-1:111122223333:launch-template/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Purpose": "Testing"
        }
      }
    }
  ]
}
```

Arbeiten mit Instance-Metadaten

Die folgenden Richtlinien stellen sicher, dass Benutzer Instanz-Metadaten nur mithilfe des Instanz-Metadatendienstes Version 2 (IMDSv2) abrufen können. Sie können die folgenden vier Richtlinien zu einer Richtlinie mit vier Anweisungen zusammenfassen. Wenn diese zu einer Richtlinie zusammengefasst werden, können Sie die Richtlinie als Service-Kontrollrichtlinie (SCP) verwenden. Sie kann gleichermaßen gut als Verweigerungsrichtlinie funktionieren, die Sie auf eine bestehende IAM-Richtlinie anwenden (zum Aufheben und Einschränken bestehender Berechtigungen) oder auch als SCP, die global auf ein Konto, eine OE oder eine gesamte Organisation angewendet wird.

> **Note**
>
> Die folgenden Richtlinien für RunInstances Metadatenoptionen müssen in Verbindung mit einer Richtlinie verwendet werden, die dem Prinzipal Berechtigungen zum Starten einer Instance erteilt RunInstances. Wenn der Prinzipal nicht auch über RunInstances Berechtigungen verfügt, kann er keine Instance starten. Weitere Informationen finden Sie in den Richtlinien unter Arbeiten mit Instances und Instanzen starten (RunInstances).

Important

Wenn Sie Amazon EC2 Auto Scaling Scaling-Gruppen verwenden und die Verwendung von IMDSv2 für alle neuen Instances vorschreiben müssen, müssen Ihre Amazon EC2 Auto Scaling Scaling-Gruppen Startvorlagen verwenden.
Wenn eine Amazon EC2 Auto Scaling Scaling-Gruppe eine Startvorlage verwendet, werden die `ec2:RunInstances` Berechtigungen des IAM-Prinzipals geprüft, wenn eine neue Amazon EC2 Auto Scaling Scaling-Gruppe erstellt wird. Sie werden auch überprüft, wenn eine bestehende Amazon EC2 Auto Scaling Scaling-Gruppe aktualisiert wird, um eine neue Startvorlage oder eine neue Version einer Startvorlage zu verwenden.
Einschränkungen bei der Verwendung von IMDSv1 On-IAM-Prinzipalen für `RunInstances` werden nur überprüft, wenn eine Amazon EC2 Auto Scaling Scaling-Gruppe, die eine Startvorlage verwendet, erstellt oder aktualisiert wird. Für eine Amazon EC2 Auto Scaling Scaling-Gruppe, die für die Verwendung der `Latest` `Default` Startvorlage konfiguriert ist, werden die Berechtigungen nicht geprüft, wenn eine neue Version der Startvorlage erstellt wird. Damit die Berechtigungen überprüft werden können, müssen Sie die Amazon EC2 Auto Scaling Scaling-Gruppe so konfigurieren, dass sie eine bestimmte Version der Startvorlage verwendet.

Um die Verwendung von IMDSv2 On-Instances zu erzwingen, die von Amazon EC2 Auto Scaling Scaling-Gruppen gestartet wurden, sind die folgenden zusätzlichen Schritte erforderlich:

1. Deaktivieren Sie die Verwendung von Startkonfigurationen für alle Konten in Ihrer Organisation, indem Sie entweder Service-Kontrollrichtlinien (SCPs) oder IAM-Berechtigungsgrenzen für neu erstellte Principals verwenden. Aktualisieren Sie für bestehende IAM-Prinzipale mit Amazon EC2 Auto Scaling Scaling-Gruppenberechtigungen die zugehörigen Richtlinien mit diesem Bedingungsschlüssel. Um die Verwendung von Startkonfigurationen zu deaktivieren, erstellen oder ändern Sie den entsprechenden SCP, die Berechtigungsgrenze oder die IAM-Richtlinie mit dem Bedingungsschlüssel `"autoscaling:LaunchConfigurationName"` mit dem als `null` angegebenen Wert.
2. Konfigurieren Sie für neue Startvorlagen die Instance-Metadatenoptionen in der Startvorlage. Erstellen Sie für vorhandene Startvorlagen eine neue Version der Startvorlage und konfigurieren Sie die Instance-Metadatenoptionen in der neuen Version.
3. In der Richtlinie, die einen jeden Prinzipal zur Verwendung einer Startvorlage berechtigt, beschränken Sie die Zuordnung von `$latest` und `$default` durch Angabe von

`"autoscaling:LaunchTemplateVersionSpecified": "true"`. Indem Sie die Verwendung auf eine bestimmte Version einer Startvorlage beschränken, können Sie sicherstellen, dass neue Instances mit der Version gestartet werden, in der die Instance-Metadatenoptionen konfiguriert sind. Weitere Informationen finden Sie LaunchTemplateSpecificationin der Amazon EC2 Auto Scaling API-Referenz, insbesondere unter dem `Version` Parameter.

4. Für eine Amazon EC2 Auto Scaling Scaling-Gruppe, die eine Startkonfiguration verwendet, ersetzen Sie die Startkonfiguration durch eine Startvorlage. Weitere Informationen finden Sie unter Migrieren Ihrer Amazon EC2 Auto Scaling Scaling-Gruppen zum Starten von Vorlagen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.
5. Stellen Sie für eine Amazon EC2 Auto Scaling Scaling-Gruppe, die eine Startvorlage verwendet, sicher, dass sie eine neue Startvorlage mit konfigurierten Instance-Metadatenoptionen oder eine neue Version der aktuellen Startvorlage mit konfigurierten Instance-Metadatenoptionen verwendet. Weitere Informationen finden Sie unter update-auto-scaling-group.

Beispiele

- Erzwingen der Verwendung von IMDSv2
- Abmeldung verweigern von IMDSv2
- Angeben des maximalen Hop-Limits
- Beschränken, wer die Instance-Metadatenoptionen ändern kann
- Erfordert das Abrufen von Rollenanmeldedaten IMDSv2

Erzwingen der Verwendung von IMDSv2

Die folgende Richtlinie legt fest, dass Sie die RunInstances API nur aufrufen können, wenn für die Instance auch die Verwendung von aktiviert wurde IMDSv2 (angegeben durch`"ec2:MetadataHttpTokens": "required"`). Wenn Sie nicht angeben, dass die Instanz dies erfordert IMDSv2, erhalten Sie beim Aufrufen der RunInstances API eine `UnauthorizedOperation` Fehlermeldung.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
              {
           "Sid": "RequireImdsV2",
           "Effect": "Deny",
           "Action": "ec2:RunInstances",
           "Resource": "arn:aws:ec2:*:*:instance/*",
           "Condition": {
               "StringNotEquals": {
                   "ec2:MetadataHttpTokens": "required"
               }
           }
       }
    ]
}
```

Abmeldung verweigern von IMDSv2

Die folgende Richtlinie legt fest, dass Sie die `ModifyInstanceMetadataOptions` API nicht aufrufen und gleichzeitig die Option IMDSv1 oder zulassen können IMDSv2. Wenn Sie die `ModifyInstanceMetadataOptions`-API aufrufen, muss das `HttpTokens`-Attribut auf `required` gesetzt sein.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Sid": "DenyIMDSv1HttpTokensModification",
        "Effect": "Deny",
        "Action": "ec2:ModifyInstanceMetadataOptions",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:Attribute/HttpTokens": "required"
            },
            "Null": {
                "ec2:Attribute/HttpTokens": false
            }
        }
    }]
```

```
}
```

Angeben des maximalen Hop-Limits

Die folgende Richtlinie legt fest, dass Sie die RunInstances API nur aufrufen können, wenn Sie auch ein Hop-Limit angeben, und das Hop-Limit darf nicht mehr als 3 betragen. Wenn Sie das nicht tun, erhalten Sie beim Aufrufen der RunInstances API eine `Unauthorized0peration` Fehlermeldung.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
                {
            "Sid": "MaxImdsHopLimit",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "NumericGreaterThan": {
                    "ec2:MetadataHttpPutResponseHopLimit": "3"
                }
            }
        }
    ]
}
```

Beschränken, wer die Instance-Metadatenoptionen ändern kann

Die folgende Richtlinie erlaubt es nur Benutzern mit der `ec2-imds-admins`-Rolle, Änderungen an den Optionen für die Instance-Metadaten vorzunehmen. Wenn ein anderer Principal als die `ec2-imds-admins` Rolle versucht, die ModifyInstanceMetadataOptions API aufzurufen, wird eine `Unauthorized0peration` Fehlermeldung angezeigt. Diese Anweisung könnte verwendet werden, um die Verwendung der ModifyInstanceMetadataOptions API zu kontrollieren. Derzeit gibt es keine detaillierten Zugriffskontrollen (Bedingungen) für die ModifyInstanceMetadataOptions API.

Erfordert das Abrufen von Rollenanmeldedaten IMDSv2

Die folgende Richtlinie legt fest, dass, wenn diese Richtlinie auf eine Rolle angewendet wird und die Rolle vom EC2 Dienst übernommen wird und die resultierenden Anmeldeinformationen zum Signieren einer Anfrage verwendet werden, die Anfrage mit den EC2 Rollenanmeldeinformationen signiert werden muss, von der abgerufen wurde IMDSv2. Andernfalls erhalten alle API-Aufrufe einen `Unauthorized0peration`-Fehler. Diese Anweisung/Richtlinie kann allgemein angewendet werden, denn wenn die Anfrage nicht mit EC2 Rollenanmeldedaten signiert ist, hat sie keine Wirkung.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
                {
            "Sid": "RequireAllEc2RolesToUseV2",
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "NumericLessThan": {
                    "ec2:RoleDelivery": "2.0"
                }
            }
        }
    ]
}
```

Arbeiten Sie mit Amazon-EBS-Volumes und Snapshots

Beispielrichtlinien für die Arbeit mit Amazon EBS-Volumes und -Snapshots finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon EBS.

Beispielrichtlinien zur Steuerung des Zugriffs auf die EC2 Amazon-Konsole

Sie können IAM-Richtlinien verwenden, um Benutzern die für die Arbeit mit Amazon EC2 erforderlichen Berechtigungen zu gewähren. step-by-stepAnweisungen finden Sie im IAM-Benutzerhandbuch unter Erstellen von IAM-Richtlinien.

Für die Konsole werden zusätzliche API-Aktionen für bestimmte Features verwendet, was bei diesen Richtlinien zu unerwarteten Ergebnissen führen kann. Wenn ein Benutzer zum Beispiel über die Berechtigung verfügt, nur die `DescribeVolumes`-API-Aktion zu verwenden, schlägt sein Versuch fehl, Volumes in der Konsole anzusehen. In diesem Abschnitt werden Richtlinien vorgestellt, mit denen Benutzer mit bestimmten Teilen der Konsole arbeiten können. Weitere Informationen zum Erstellen von Richtlinien für die EC2 Amazon-Konsole finden Sie im folgenden AWS Sicherheits-Blogbeitrag: Benutzern die Erlaubnis erteilen, in der EC2 Amazon-Konsole zu arbeiten.

Die folgenden Beispiele zeigen Richtlinienerklärungen, mit denen Sie Benutzern Berechtigungen zur Nutzung von Amazon gewähren können EC2. Ersetzen Sie jeden *`user input placeholder`* durch Ihre Informationen. Diese Richtlinien sind auf Anforderungen ausgelegt, die über die AWS-Managementkonsole erfolgen. Die EC2 Amazon-Konsole ruft möglicherweise mehrere API-Aktionen auf, um eine einzelne Ressource anzuzeigen, und es ist möglicherweise nicht offensichtlich, bis der Benutzer eine Aufgabe versucht und die Konsole einen Fehler anzeigt. Weitere Informationen finden Sie im folgenden AWS Sicherheits-Blogbeitrag: Benutzern die Erlaubnis erteilen, in der EC2 Amazon-Konsole zu arbeiten.

Beispiele

- Beispiel: schreibgeschützter Zugriff
- Beispiel: Verwenden Sie den EC2 Launch-Instance-Assistenten
- Beispiel: Arbeiten mit Sicherheitsgruppen
- Beispiel: Arbeiten mit Elastic-IP-Adressen
- Beispiel: Arbeiten mit Reserved Instances

Verwenden Sie einen Service wie AWS CloudTrail, um einfacher herauszufinden, welche API-Aktionen zum Ausführen von Aufgaben in der Konsole erforderlich sind. Wenn Ihre Richtlinie keine Berechtigung zum Erstellen oder Ändern einer bestimmten Ressource erteilt, zeigt die Konsole eine codierte Meldung mit Diagnoseinformationen an. Sie können die Nachricht mit der DecodeAuthorizationMessageAPI-Aktion für AWS STS oder mit dem decode-authorization-messageBefehl in der AWS CLI dekodieren.

Beispiel: schreibgeschützter Zugriff

Damit Benutzer alle Ressourcen in der EC2 Amazon-Konsole anzeigen können, können Sie dieselbe Richtlinie wie im folgenden Beispiel verwenden:Beispiel: schreibgeschützter Zugriff. Die Benutzer können keine Aktionen für diese Ressourcen ausführen und keine neuen Ressourcen erstellen, sofern ihnen keine andere Anweisung die Berechtigung dazu gewährt.

Instanzen und AMIs Snapshots anzeigen

Alternativ haben Sie die Möglichkeit, schreibgeschützten Zugriff auf eine Untermenge von Ressourcen bereitzustellen. Ersetzen Sie hierfür den *-Platzhalter in der `ec2:Describe`-API-Aktion mit konkreten `ec2:Describe`-Aktionen für jede Ressource. Die folgende Richtlinie ermöglicht es Benutzern AMIs, alle Instances und Snapshots in der EC2 Amazon-Konsole anzuzeigen. Die `ec2:DescribeTags` Aktion ermöglicht es Benutzern, öffentlich AMIs einzusehen. Die Konsole benötigt die Tagging-Informationen AMIs, um öffentlich angezeigt zu werden. Sie können diese Aktion jedoch entfernen, damit Benutzer nur private AMIs Inhalte anzeigen können.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeTags",
         "ec2:DescribeSnapshots"
      ],
      "Resource": "*"
   }
   ]
}
```

> **Note**
>
> Die EC2 `ec2:Describe*` Amazon-API-Aktionen unterstützen keine Berechtigungen auf Ressourcenebene, sodass Sie nicht kontrollieren können, welche einzelnen Ressourcen Benutzer in der Konsole anzeigen können. Aus diesem Grund ist in der obigen Anweisung der *-Platzhalter im `Resource`-Element erforderlich. Weitere Informationen darüber, welche EC2 Amazon-API-Aktionen ARNs Sie verwenden können, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2.

Instanzen und CloudWatch Metriken anzeigen

Die folgende Richtlinie ermöglicht es Benutzern, Instances in der EC2 Amazon-Konsole sowie CloudWatch Alarme und Metriken auf der Registerkarte Überwachung der Seite Instances einzusehen. Die EC2 Amazon-Konsole verwendet die CloudWatch API, um die Alarme und Messwerte anzuzeigen. Sie müssen den Benutzern daher die Erlaubnis erteilen`cloudwatch:DescribeAlarms`, die`cloudwatch:DescribeAlarmsForMetric`, `cloudwatch:ListMetrics``cloudwatch:GetMetricStatistics`, und `cloudwatch:GetMetricData` Aktionen zu verwenden.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeInstanceTypes",
         "cloudwatch:DescribeAlarms",
         "cloudwatch:DescribeAlarmsForMetric",
         "cloudwatch:ListMetrics",
         "cloudwatch:GetMetricStatistics",
         "cloudwatch:GetMetricData"
      ],
      "Resource": "*"
   }
   ]
}
```

Beispiel: Verwenden Sie den EC2 Launch-Instance-Assistenten

Der Amazon EC2 Launch Instance Wizard ist ein Bildschirm mit Optionen zum Konfigurieren und Starten einer Instance. Ihre Richtlinie muss die Berechtigung für die API-Aktionen enthalten, die den Benutzern ermöglichen, mit den Optionen des Assistenten zu arbeiten. Fehlt eine solche Berechtigung in der Richtlinie, werden einige Elemente im Assistenten nicht ordnungsgemäß geladen und die Benutzer können den Start nicht abschließen.

Grundlegender Zugriff auf den Launch Instance Wizard

Für einen erfolgreich abgeschlossenen Start müssen Sie den Benutzern die Berechtigung erteilen, die `ec2:RunInstances`-API-Aktion und mindestens die folgenden API-Aktionen zu verwenden:

- `ec2:DescribeImages`: Zum Ansehen und Auswählen eines AMI.
- `ec2:DescribeInstanceTypes`: Zum Anzeigen und Auswählen eines Instance-Typs.
- `ec2:DescribeVpcs`: Zum Anzeigen der verfügbaren Versionen von Ruby.
- `ec2:DescribeSubnets`: Zum Ansehen aller verfügbaren Subnetze für die ausgewählte VPC.
- `ec2:DescribeSecurityGroups` oder `ec2:CreateSecurityGroup`: Zum Anzeigen und Auswählen einer vorhandenen Sicherheitsgruppe oder zum Erstellen einer neuen Sicherheitsgruppe.
- `ec2:DescribeKeyPairs` oder `ec2:CreateKeyPair`: Um ein vorhandenes Schlüsselpaar auszuwählen oder ein neues Schlüsselpaar zu erstellen.
- `ec2:AuthorizeSecurityGroupIngress`: Zum Hinzufügen von Regeln für eingehenden Datenverkehr.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateSecurityGroup",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateKeyPair"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": "ec2:RunInstances",
            "Resource": "*"
        }
    ]
}
```

Sie können den Benutzern mehr Optionen zur Verfügung stellen, indem Sie der Richtlinie weitere API-Aktionen hinzufügen, zum Beispiel:

- `ec2:DescribeAvailabilityZones`: Zum Anzeigen und Auswählen einer spezifischen Availability Zone.
- `ec2:DescribeNetworkInterfaces`:Zum Ansehen und Auswählen von vorhandenen Netzwerkschnittstellen für das ausgewählte Subnetz.
- Zum Hinzufügen von Regeln für ausgehenden Datenverkehr zu VPC-Sicherheitsgruppen müssen die Benutzer für die `ec2:AuthorizeSecurityGroupEgress`-API-Aktion berechtigt sein. Zum Ändern oder Löschen von vorhandenen Regeln muss den Benutzern die Berechtigung erteilt werden, die relevante `ec2:RevokeSecurityGroup*`-API-Aktion zu verwenden.
- `ec2:CreateTags`: Zum Markieren der Ressourcen, die von `RunInstances` erstellt werden. Weitere Informationen finden Sie unter Erteilen Sie die Erlaubnis, EC2 Amazon-Ressourcen während der Erstellung zu taggen. Wenn die Benutzer keine Berechtigung zur Verwendung dieser Aktion haben und auf der Markierungsseite des Launch Instance Wizard versuchen, Tags anzuwenden, schlägt der Start fehl.

  > **Important**
  >
  > Das Angeben eines Namens beim Starten einer Instance erstellt ein Tag und erfordert die Aktion `ec2:CreateTags`. Seien Sie vorsichtig, wenn Sie Benutzern die Erlaubnis zur Verwendung der Aktion `ec2:CreateTags` erteilen, da dies Ihre Möglichkeit einschränkt, den `aws:ResourceTag`-Bedingungsschlüssel zu nutzen, um die Verwendung anderer Ressourcen einzuschränken. Wenn Sie Benutzern die Berechtigung zur Verwendung der Aktion `ec2:CreateTags` erteilen, können sie den Tag (Markierung) einer Ressource ändern, um diese Einschränkungen zu umgehen. Weitere Informationen finden Sie unter Den Zugriff mithilfe des attributbasierten Zugriffs steuern.

- Um Systems-Manager-Parameter bei der Auswahl eines AMIs zu verwenden, müssen Sie `ssm:DescribeParameters` und `ssm:GetParameters` zu Ihrer Richtlinie hinzufügen. `ssm:DescribeParameters` gewährt Ihren Benutzern die Berechtigung, Systems-Manager-

Parameter anzuzeigen und auszuwählen. `ssm:GetParameters` gewährt Ihren Benutzern die Berechtigung, die Werte der Systems-Manager-Parameter abzurufen. Sie können auch den Zugriff auf bestimmte Systems Manager-Parameter beschränken. Weitere Informationen finden Sie unter Zugriff auf bestimmte Systems Manager-Parameter weiter unten in diesem Abschnitt.

Derzeit unterstützen die EC2 `Describe*` Amazon-API-Aktionen keine Berechtigungen auf Ressourcenebene, sodass Sie nicht einschränken können, welche einzelnen Ressourcen Benutzer im Launch-Instance-Assistenten anzeigen können. Sie können allerdings Berechtigungen auf Ressourcenebene auf die `ec2:RunInstances`-API-Aktion anwenden, um die Ressourcen zu begrenzen, die die Benutzer beim Starten einer Instance nutzen dürfen. Der Start schlägt fehl, wenn die Benutzer Optionen auswählen, für deren Verwendung sie nicht autorisiert sind.

Zugriff auf einen bestimmten Instance-Typ, ein Subnetz und eine Region einschränken

Die folgende Richtlinie ermöglicht es Benutzern, `t2.micro` Instances zu starten, die AMIs Eigentum von Amazon sind, und zwar nur in einem bestimmten Subnetz (`subnet-1a2b3c4d`). Benutzer können Starts nur in der angegebenen Region durchführen. Wenn Benutzer im Launch Instance Wizard eine andere Region, einen anderen Instance-Typ, ein anderes AMI oder ein anderes Subnetz auswählen, schlägt der Start fehl.

In der ersten Anweisung wird den Benutzern die Berechtigung erteilt, die Optionen im Launch Instance Wizard anzuzeigen oder neue zu erstellen, wie im Beispiel oben gezeigt. Dank der zweiten Anweisung haben die Benutzer die Berechtigung, die zum Starten einer Instance in einer VPC erforderlichen Ressourcen – Netzwerkschnittstelle, Volume, Schlüsselpaar, Sicherheitsgruppe und Subnetz – für die `ec2:RunInstances`-Aktion zu verwenden. Weitere Informationen zur Verwendung der `ec2:RunInstances`-Aktion finden Sie unter Instanzen starten (RunInstances). Mit der dritten und vierten Anweisung wird den Benutzern die Berechtigung gewährt, die Instance- bzw. AMI-Ressourcen zu nutzen. Dabei muss allerdings die Instance eine `t2.micro`-Instance und Amazon oder bestimmte vertrauenswürdige und verifizierte Partner der Eigentümer des AMI sein.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
```

```
            "ec2:DescribeImages",
            "ec2:DescribeInstanceTypes",
            "ec2:DescribeKeyPairs",
            "ec2:CreateKeyPair",
            "ec2:DescribeVpcs",
            "ec2:DescribeSubnets", "ec2:DescribeSecurityGroups",
            "ec2:CreateSecurityGroup",
            "ec2:AuthorizeSecurityGroupIngress"
        ],
        "Resource": "*"
        },
        {
           "Effect": "Allow",
           "Action":"ec2:RunInstances",
           "Resource": [
              "arn:aws:ec2:us-east-2:111122223333:network-interface/*",
              "arn:aws:ec2:us-east-2:111122223333:volume/*",
              "arn:aws:ec2:us-east-2:111122223333:key-pair/*",
              "arn:aws:ec2:us-east-2:111122223333:security-group/*",
              "arn:aws:ec2:us-east-2:111122223333:subnet/subnet-1a2b3c4d"
           ]
        },
        {
           "Effect": "Allow",
           "Action": "ec2:RunInstances",
           "Resource": [
              "arn:aws:ec2:us-east-2:111122223333:instance/*"
           ],
           "Condition": {
              "StringEquals": {
                 "ec2:InstanceType": "t2.micro"
              }
           }
        },
        {
           "Effect": "Allow",
           "Action": "ec2:RunInstances",
           "Resource": [
                 "arn:aws:ec2:us-east-2::image/ami-*"
           ],
           "Condition": {
              "StringEquals": {
                 "ec2:Owner": "amazon"
              }
```

```
      }
   }
   ]
}
```

Zugriff auf bestimmte Systems Manager-Parameter einschränken

Die folgende Richtlinie gewährt Zugriff auf die Verwendung von Systems Manager-Parametern mit einem bestimmten Namen.

Die erste Anweisung gewährt Benutzern die Erlaubnis, Systems Manager-Parameter anzuzeigen, wenn sie im Launch Instance Wizard ein AMI auswählen. Die zweite Anweisung gibt Benutzern die Berechtigung, nur Parameter zu verwenden, die mit `prod-*` bezeichnet sind.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ssm:DescribeParameters"
      ],
      "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action": [
         "ssm:GetParameters"
      ],
     "Resource": "arn:aws:ssm:us-east-2:123456123456:parameter/prod-*"
   }
   ]
}
```

Beispiel: Arbeiten mit Sicherheitsgruppen

Anzeigen von Sicherheitsgruppen sowie Hinzufügen und Entfernen von Regeln

Die folgende Richtlinie gewährt Benutzern die Berechtigung, Sicherheitsgruppen in der EC2 Amazon-Konsole anzuzeigen, Regeln für eingehenden und ausgehenden Datenverkehr hinzuzufügen und zu entfernen sowie Regelbeschreibungen für bestehende Sicherheitsgruppen, die das Tag tragen, aufzulisten und zu ändern. `Department=Test`

In der ersten Anweisung erlaubt die `ec2:DescribeTags`-Aktion den Benutzern, Tags in der Konsole anzusehen. Damit wird es für die Benutzer einfacher, die Sicherheitsgruppen zu bestimmen, die sie bearbeiten dürfen.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeSecurityGroups",
         "ec2:DescribeSecurityGroupRules",
         "ec2:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:AuthorizeSecurityGroupIngress",
         "ec2:RevokeSecurityGroupIngress",
         "ec2:AuthorizeSecurityGroupEgress",
         "ec2:RevokeSecurityGroupEgress",
         "ec2:ModifySecurityGroupRules",
         "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
         "ec2:UpdateSecurityGroupRuleDescriptionsEgress"
      ],
      "Resource": [
         "arn:aws:ec2:us-east-2:111122223333:security-group/*"
      ],
      "Condition": {
         "StringEquals": {
            "aws:ResourceTag/Department": "Test"
         }
      }
   },
```

```
    {
       "Effect": "Allow",
       "Action": [
          "ec2:ModifySecurityGroupRules"
       ],
       "Resource": [
          "arn:aws:ec2:us-east-2:111122223333:security-group-rule/*"
       ]
    }
]}
```

Arbeiten mit dem Dialogfeld Create Security Group (Sicherheitsgruppe erstellen)

Sie können eine Richtlinie erstellen, die es Benutzern ermöglicht, mit dem Dialogfeld „Sicherheitsgruppe erstellen“ in der EC2 Amazon-Konsole zu arbeiten. Damit die Benutzer dieses Dialogfeld verwenden können, müssen sie mindestens über Berechtigungen für die folgenden API-Aktionen verfügen:

- `ec2:CreateSecurityGroup`: Zum Erstellen einer neuen Sicherheitsgruppe.
- `ec2:DescribeVpcs`: Um eine Liste der VPCs in der VPC-Liste vorhandenen Objekte anzuzeigen.

Mit diesen Berechtigungen können die Benutzer eine neue Sicherheitsgruppe erstellen, dieser aber keine Regeln hinzufügen. Für die Arbeit mit Regeln im Dialogfeld Create Security Group fügen Sie der Richtlinie die folgenden API-Aktionen hinzu:

- `ec2:AuthorizeSecurityGroupIngress`: Zum Hinzufügen von Regeln für eingehenden Datenverkehr.
- `ec2:AuthorizeSecurityGroupEgress`: Zum Hinzufügen von Regeln für ausgehenden Datenverkehr zu VPC-Sicherheitsgruppen.
- `ec2:RevokeSecurityGroupIngress`: Zum Ändern oder Löschen vorhandener eingehender Regeln. Diese Aktion ist hilfreich, damit die Benutzer in der Konsole das Feature Copy to new verwenden können. Mit diesem Feature wird das Dialogfeld Create Security Group geöffnet und mit den gleichen Regeln vorausgefüllt, die in der ausgewählten vorhandenen Sicherheitsgruppe enthalten sind.
- `ec2:RevokeSecurityGroupEgress`: Zum Ändern oder Löschen von Regeln für ausgehenden Datenverkehr für VPC-Sicherheitsgruppen. Dies ist nützlich, um Benutzern zu ermöglichen, die

ausgehende Standardregel zu ändern oder zu löschen, die jeden ausgehenden Datenverkehr erlaubt.

- `ec2:DeleteSecurityGroup`: Für den Fall, dass ungültige Regeln nicht gespeichert werden können. Die Konsole erstellt zuerst die Sicherheitsgruppe und fügt dann die angegebenen Regeln hinzu. Wenn die Regeln ungültig sind, schlägt die Aktion fehl und die Konsole versucht, die Sicherheitsgruppe zu löschen. Das Dialogfeld Create Security Group bleibt geöffnet, sodass die Benutzer die unwirksame Regel korrigieren und erneut versuchen können, die Sicherheitsgruppe zu erstellen. Die API-Aktion ist nicht erforderlich. Wenn aber ein Benutzer nicht über die Berechtigung zu ihrer Verwendung verfügt und versucht, eine Sicherheitsgruppe mit ungültigen Regeln zu erstellen, wird die Sicherheitsgruppe ohne jede Regel erstellt. Der Benutzer muss die Regeln danach hinzufügen.
- `ec2:UpdateSecurityGroupRuleDescriptionsIngress`: Zum Hinzufügen oder Aktualisieren von Beschreibungen von Sicherheitsgruppenregeln für eingehenden Datenverkehr.
- `ec2:UpdateSecurityGroupRuleDescriptionsEgress`: Zum Hinzufügen oder Aktualisieren von Beschreibungen von Sicherheitsgruppenregeln für ausgehenden Datenverkehr.
- `ec2:ModifySecurityGroupRules`: Zum Modifizieren von Sicherheitsgruppenregeln.
- `ec2:DescribeSecurityGroupRules`: Zum Auflisten von Sicherheitsgruppenregeln.

Die folgende Richtlinie erteilt Benutzern die Berechtigung, das Dialogfeld Create Security Group zu verwenden und für Sicherheitsgruppen, die mit einer bestimmten VPC (`vpc-1a2b3c4d`) verknüpft sind, Regeln für ein- und ausgehenden Datenverkehr zu erstellen. Benutzer können Sicherheitsgruppen für eine VPC erstellen, ihnen jedoch keine Regeln hinzufügen. Ebenso können die Benutzer vorhandenen Sicherheitsgruppen, die nicht mit der VPC verknüpft sind, keine Regeln hinzufüge `vpc-1a2b3c4d`. Den Benutzern wird außerdem die Berechtigung erteilt, alle Sicherheitsgruppen in der Konsole anzusehen. Damit wird es für die Benutzer einfacher, die Sicherheitsgruppen zu bestimmen, denen sie Regeln für eingehenden Datenverkehr hinzufügen können. Die Richtlinie gewährt den Benutzern zudem die Berechtigung zum Löschen von Sicherheitsgruppen, die mit der VPC `vpc-1a2b3c4d` verknüpft sind.

JSON

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

```
        "ec2:DescribeSecurityGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource": "arn:aws:ec2:us-east-2:111122223333:security-group/*",
      "Condition":{
         "ArnEquals": {
            "ec2:Vpc": "arn:aws:ec2:us-east-2:111122223333:vpc/vpc-1a2b3c4d"
         }
      }
    }
   ]
}
```

Beispiel: Arbeiten mit Elastic-IP-Adressen

Damit Benutzer Elastic IP-Adressen in der EC2 Amazon-Konsole anzeigen können, müssen Sie den Benutzern die Erlaubnis zur Verwendung der `ec2:DescribeAddresses` Aktion erteilen.

Sie können Benutzern die Arbeit mit Elastic IP-Adressen ermöglichen, indem Sie der Richtlinie folgende Aktionen hinzufügen.

- `ec2:AllocateAddress`: Zum Zuweisen einer Elastic IP-Adresse.
- `ec2:ReleaseAddress`: Zum Freigeben einer Elastic IP-Adresse.
- `ec2:AssociateAddress`: Zum Zuordnen einer Elastic IP-Adresse zu einer Instance oder Netzwerkschnittstelle.
- `ec2:DescribeNetworkInterfaces` und `ec2:DescribeInstances`: Zum Arbeiten mit der Seite Associate address. Auf der Seite werden die verfügbaren Instances oder Netzwerkschnittstellen angezeigt, denen Sie eine Elastic IP-Adresse zuordnen können.
- `ec2:DisassociateAddress`: Zum Aufheben der Zuordnung einer Elastic IP-Adresse zu einer Instance oder Netzwerkschnittstelle.

Die Richtlinie unten erlaubt den Benutzern, Elastic IP-Adressen anzusehen, zuzuordnen und mit Instances zu verknüpfen. Die Benutzer können die Elastic IP-Adressen nicht freigeben, nicht mit Netzwerkschnittstellen verknüpfen und keine Verknüpfungen aufheben.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAddresses",
                "ec2:AllocateAddress",
                "ec2:DescribeInstances",
                "ec2:AssociateAddress"
            ],
            "Resource": "*"
        }
    ]
}
```

Beispiel: Arbeiten mit Reserved Instances

Mit der folgenden Richtlinie können Benutzer Reserved Instances in Ihrem Konto anzeigen und ändern sowie neue Reserved Instances in der AWS-Managementkonsole erwerben.

Diese Richtlinie ermöglicht es Benutzern, alle Reserved Instances sowie On-Demand-Instances im Konto anzuzeigen. Für einzelne Reserved Instances können keine Berechtigungen auf Ressourcenebene erteilt werden.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeReservedInstances",
         "ec2:ModifyReservedInstances",
```

```
            "ec2:PurchaseReservedInstancesOffering",
            "ec2:DescribeInstances",
            "ec2:DescribeInstanceTypes",
            "ec2:DescribeAvailabilityZones",
            "ec2:DescribeReservedInstancesOfferings"
        ],
        "Resource": "*"
    }
    ]
}
```

Die `ec2:DescribeAvailabilityZones` Aktion ist erforderlich, um sicherzustellen, dass die EC2 Amazon-Konsole Informationen zu den Availability Zones anzeigen kann, in denen Sie Reserved Instances kaufen können. Die `ec2:DescribeInstances`-Aktion ist nicht erforderlich, sorgt aber dafür, dass der Benutzer die Instance im Konto sehen kann und Reservierungen kauft, die den richtigen Anforderungen entsprechen.

Wenn Sie den Benutzerzugriff begrenzen möchten, passen Sie die API-Aktionen an. Zum Beispiel hat der Benutzer nach dem Entfernen von `ec2:DescribeInstances` und `ec2:DescribeAvailabilityZones` schreibgeschützten Zugriff.

AWS verwaltete Richtlinien für Amazon EC2

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie unter AWS Verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

AWS verwaltete Richtlinie: AmazonEC2FullAccess

Sie können die `AmazonEC2FullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt Berechtigungen, die den vollen Zugriff auf Amazon ermöglichen EC2.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AmazonEC2FullAccess in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AmazonEC2ReadOnlyAccess

Sie können die `AmazonEC2ReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt Berechtigungen, die nur Lesezugriff auf Amazon ermöglichen. EC2

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AmazonEC2ReadOnlyAccess in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AmazonEC2ImageReferencesAccessPolicy

Sie können die `AmazonEC2ImageReferencesAccessPolicy`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt die für die Verwendung der EC2 DescribeImageReferences API erforderlichen Berechtigungen, einschließlich der Berechtigung zum Anzeigen von EC2 Instanzen, Startvorlagen, Systems Manager Manager-Parametern und Image Builder Builder-Rezepten.
Die Richtlinie unterstützt die `IncludeAllResourceTypes` Flagge und wird auch weiterhin funktionieren, wenn Unterstützung für neue Ressourcentypen AWS hinzugefügt wird, sodass future Richtlinienaktualisierungen nicht mehr erforderlich sind.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AmazonEC2ImageReferencesAccessPolicy in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSEC2CapacityReservationFleetRolePolicy

Diese Richtlinie ist an die serviceverknüpfte Rolle namens AWSServiceRoleForEC2CapacityReservationFleet angehängt, damit der Service in Ihrem Namen Kapazitätsreservierungen in einer Kapazitätsreservierungsflotte erstellen, ändern und stornieren

kann. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Kapazitätsreservierungsflotten.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSEC2CapacityReservationFleetRolePolicy in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSEC2FleetServiceRolePolicy

Diese Richtlinie ist der serviceverknüpften Rolle AWSServiceRoleForEC2Fleetzugeordnet, sodass EC2 Fleet Instances in Ihrem Namen anfordern, starten, beenden und taggen kann. Weitere Informationen finden Sie unter Servicebezogene Rolle für Fleet EC2 .

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSEC2FleetServiceRolePolicy in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSEC2SpotFleetServiceRolePolicy

Diese Richtlinie ist an die servicegebundene Rolle namens AWSServiceRoleForEC2SpotFleet angefügt, damit die Spot-Flotte in Ihrem Namen Instances starten und verwalten kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rolle für Spot-Flotte.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSEC2SpotFleetServiceRolePolicy in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSEC2SpotServiceRolePolicy

Diese Richtlinie ist der servicebasierten Rolle zugeordnet AWSServiceRoleForEC2Spot, sodass Amazon EC2 Spot-Instances in Ihrem Namen starten und verwalten kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rolle für Spot-Instance-Anforderungen.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSEC2SpotServiceRolePolicy in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSEC2VssSnapshotPolicy

Sie können diese verwaltete Richtlinie an die IAM-Instance-Profilrolle anhängen, die Sie für Ihre Amazon EC2 Windows-Instances verwenden. Die Richtlinie gewährt Amazon Berechtigungen, die es Amazon EC2 ermöglichen, VSS-Snapshots in Ihrem Namen zu erstellen und zu verwalten.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSEC2VssSnapshotPolicy in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: DeclarativePoliciesEC2Report

Diese Richtlinie ist der dienstbezogenen Rolle zugeordnet, die so benannt ist`AWSServiceRoleForDeclarativePoliciesEC2Report`, dass sie nur Lesezugriff gewährt, die für die Erstellung des Kontostatusberichts für deklarative Richtlinien APIs erforderlich ist.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter DeclarativePoliciesEC2Report in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: EC2FastLaunchFullAccess

Sie können die `EC2FastLaunchFullAccess`-Richtlinie Ihrem Instance-Profil oder einer anderen IAM-Rolle anfügen. Diese Richtlinie gewährt vollen Zugriff auf EC2 Schnellstartaktionen sowie gezielte Berechtigungen wie folgt.

Details zu Berechtigungen

- EC2 Schnellstart — Administratorzugriff wird gewährt, sodass die Rolle EC2 Fast Launch aktivieren oder deaktivieren und Fast Launch-Images beschreiben EC2 kann.
- Amazon EC2 — Zugriff wird für die Vorgänge Amazon EC2 RunInstancesCreateTags, Describe und Create and Modify Launch Template gewährt. Außerdem wird Zugriff gewährt, um Netzwerk- und Sicherheitsgruppenressourcen zu erstellen, Eingangsregeln zu autorisieren und Ressourcen zu löschen, die von EC2 Fast Launch erstellt wurden.
- IAM – Der Zugriff wird gewährt, um Instance-Profile abzurufen und zu verwenden, deren Name `ec2fastlaunch` enthält, zur Erstellung der EC2FastLaunchServiceRolePolicy-serviceverknüpften Rolle.
- CloudFormation— EC2 Fast Launch erhält Zugriff zur Beschreibung und Erstellung von Stacks sowie zum Löschen von CloudFormation Stacks, die von Fast Launch erstellt wurden.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter EC2FastLaunchFullAccess in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSEC2CapacityManagerServiceRolePolicy

Diese Richtlinie ist der benannten dienstbezogenen Rolle zugeordnet AWSServiceRoleForEC2CapacityManager, sodass EC2 Capacity Manager in Ihrem Namen Kapazitätsressourcen verwalten und in AWS Organizations integrieren kann. Weitere Informationen finden Sie unter Dienstbezogene Rollen für EC2 Capacity Manager.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter AWSEC2CapacityManagerServiceRolePolicy in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: EC2FastLaunchServiceRolePolicy

Diese Richtlinie ist der serviceverknüpften Rolle mit dem Namen AWSServiceRoleForEC2FastLaunchzugeordnet, sodass Amazon EC2 eine Reihe von vorab bereitgestellten Snapshots erstellen und verwalten kann, die den Zeitaufwand für das Starten von Instances über Ihr EC2 Fast Launch-fähiges AMI reduzieren. Weitere Informationen finden Sie unter the section called “Serviceverknüpfte Rolle”.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter EC2FastLaunchServiceRolePolicy in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: Ec2InstanceConnect

Sie können die `Ec2InstanceConnect`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt Kunden Berechtigungen, die es Kunden ermöglichen, EC2 Instance Connect aufzurufen, um kurzlebige Schlüssel für ihre EC2 Instances zu veröffentlichen und Connect über SSH oder die EC2 Instance Connect-CLI zu verbinden.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter Ec2InstanceConnect in der Referenz zu von AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: Ec2InstanceConnectEndpoint

Diese Richtlinie ist einer dienstbezogenen Rolle zugeordnet, die so benannt ist AWSServiceRoleForEC2InstanceConnect, dass EC2 Instance Connect Endpoint Aktionen in Ihrem Namen ausführen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rolle für EC2 Instance Connect Endpoint.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter Ec2InstanceConnectEndpoint in der Referenz zu von AWS verwalteten Richtlinien. Eine Beschreibung der Aktualisierungen dieser Richtlinie finden Sie unter EC2 Aktualisierungen der AWS verwalteten Richtlinien durch Amazon.

EC2 Aktualisierungen der AWS verwalteten Richtlinien durch Amazon

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Amazon an, EC2 seit dieser Service begonnen hat, diese Änderungen zu verfolgen.

Änderungen	Beschreibung	Date
AWSEC2CapacityManagerServiceRolePolicy – Neue Richtlinie	Amazon EC2 hat diese Richtlinie hinzugefügt, damit Sie Kapazitätsressourcen verwalten und sich in Ihrem Namen mit AWS Organizations integrieren können.	15. Oktober 2025
AmazonEC2ImageReferencesAccessPolicy – Neue Richtlinie	Amazon EC2 hat diese Richtlinie hinzugefügt, um die Erlaubnis zum Scannen aller von der EC2 DescribeImageReferences API unterstützten Ressourcentypen zu gewähren.	26. August 2025
Ec2InstanceConnectEndpoint— Aktualisierte Richtlinie	Um die Änderung vorhandener Instance Connect-Endpunkte zu unterstützen, hat Amazon diese Richtlinie EC2 aktualisiert, um Berechtigungen zum Zuweisen und Aufheben der Zuweisung von IPv6 Adressen und zum Ändern von Sicherheitsgruppen auf Netzwerkschnittstellen, die von EC2 Instance Connect Endpoint erstellt wurden, hinzugefügt. Amazon hat diese Richtlinie EC2 auch aktualisiert, um den `Null` Condition Operator durch den `StringLike` Condition Operator zu ersetzen.	31. Juli 2025

Änderungen	Beschreibung	Date
EC2FastLaunchServiceRolePolicy— Aktualisierte Richtlinie	Um zu verhindern, dass Ressourcen verwaist sind, hat Amazon diese Richtlinie EC2 aktualisiert und nun die Erlaubnis hinzugefügt, Volumes, Volumenattribute und Netzwerkschnittstellen zu beschreiben und Volumes und Netzwerkschnittstellen zu löschen, die von EC2 Fast Launch erstellt wurden.	17. Juli 2025
EC2FastLaunchFullAccess— Aktualisierte Richtlinie	Amazon hat diese Richtlinie EC2 aktualisiert und umfasst nun auch Vorgänge zum Erstellen und Ändern von Startvorlagen, zum Erstellen von Netzwerk- und Sicherheitsgruppenressourcen, zum Autorisieren von Eingangsregeln und zum Löschen von Ressourcen, die von EC2 Fast Launch erstellt wurden. Es kann außerdem Stapel beschreiben und erstellen sowie CloudFormation Stapel löschen, die EC2 von Fast Launch erstellt wurden.	14. Mai 2025

Änderungen	Beschreibung	Date
EC2FastLaunchServiceRolePolicy— Aktualisierte Richtlinie	Amazon hat diese Richtlinie EC2 aktualisiert, um Amazon EventBridge Access zur Erstellung und Verwaltung von Eventregeln für EC2 Fast Launch hinzuzufügen. Darüber hinaus kann EC2 Fast Launch jetzt CloudFormation Stacks beschreiben, eine Instance von einem zugehörigen AMI aus starten AWS License Manager, eine Liste der erstellten AWS KMS Grants abrufen, die zurückgezogen werden können, und Startvorlagen löschen, die es erstellt hat.	14. Mai 2025
AWSEC2CapacityReservationFleetRolePolicy— Aktualisierte Berechtigungen	Amazon `AWSEC2CapacityReservationFleetRolePolicy` hat die verwaltete Richtlinie EC2 aktualisiert, sodass der `ArnLike` Bedingungsoperator anstelle des `StringLike` Bedingungsoperators verwendet wird.	03. März 2025
AmazonEC2ReadOnlyAccess – hat neue Berechtigung	Amazon EC2 hat eine Berechtigung hinzugefügt, mit der Sie Sicherheitsgruppen mithilfe des `GetSecurityGroupsForVpc` Vorgangs abrufen können.	27. Dezember 2024

Änderungen	Beschreibung	Date
EC2FastLaunchFullAccess – Neue Richtlinie	Amazon EC2 hat diese Richtlinie hinzugefügt, um API-Aktionen im Zusammenhang mit der EC2 Schnellstartfunktion von einer Instance aus durchzuführen. Die Richtlinie kann an das Instance-Profil für eine Instance angehängt werden, die von einem EC2 Fast Launch-fähigen AMI aus gestartet wurde.	14. Mai 2024
AWSEC2VssSnapshotPolicy – Neue Richtlinie	Amazon EC2 hat die `AWSEC2VssSnapshotPolicy` Richtlinie hinzugefügt, die Berechtigungen zum Erstellen und Hinzufügen von Tags zu Amazon Machine Images (AMIs) und EBS-Snapshots enthält.	28. März 2024
Ec2InstanceConnectEndpoint – Neue Richtlinie	Amazon EC2 hat die `Ec2InstanceConnectEndpoint` Richtlinie hinzugefügt. Diese Richtlinie ist der AWSServiceRoleForEC2InstanceConnectservicever knüpften Rolle beigefügt, damit Amazon EC2 Aktionen in Ihrem Namen durchführen kann, wenn Sie einen EC2 Instance Connect-Endpunkt erstellen.	24. Januar 2023

Änderungen	Beschreibung	Date
EC2FastLaunchServiceRolePolicy – Neue Richtlinie	Amazon EC2 hat die EC2 Schnellstartfunktion hinzugefügt, damit Windows Instances schneller starten AMIs kann, indem eine Reihe von vorab bereitgestellten Snapshots erstellt wird.	26. November 2021
Amazon EC2 hat begonnen, Änderungen zu verfolgen	Amazon EC2 hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen	1. März 2021

IAM-Rollen für Amazon EC2

Anwendungen müssen ihre API-Anfragen mit AWS Anmeldeinformationen signieren. Wenn Sie ein Anwendungsentwickler sind, benötigen Sie daher eine Strategie für die Verwaltung der Anmeldeinformationen für Ihre Anwendungen, die auf EC2 Instances ausgeführt werden. Sie können zum Beispiel die AWS -Anmeldeinformationen sicher an die Instances verteilen, damit die Anwendungen auf diesen Instances sie zum Signieren von Anforderungen verwenden können, während Ihre Anmeldeinformationen vor anderen Benutzern geschützt bleiben. Es ist jedoch schwierig, Anmeldeinformationen sicher an jede Instance zu verteilen, insbesondere an diejenigen, die in Ihrem Namen AWS erstellt werden, wie Spot-Instances oder Instances in Amazon EC2 Auto Scaling Scaling-Gruppen. Sie müssen auch in der Lage sein, die Anmeldeinformationen für jede Instance zu aktualisieren, wenn Sie Ihre AWS Anmeldeinformationen wechseln.

Wir haben IAM-Rollen entworfen, damit Ihre Anwendungen die API-Anforderungen sicher von Ihren Instances senden können, ohne dass Sie die von den Anwendungen verwendeten Sicherheitsanmeldeinformationen verwalten müssen. Anstatt Ihre AWS Anmeldeinformationen zu erstellen und zu verteilen, können Sie die Berechtigung zum Stellen von API-Anfragen mithilfe von IAM-Rollen wie folgt delegieren:

1. Erstellen Sie eine IAM-Rolle.
2. Definieren Sie, welche Konten oder AWS Dienste die Rolle übernehmen können.

3. Definieren Sie, welche API-Aktionen und -Ressourcen die Anwendung nach Annahme der Rolle verwenden kann.
4. Geben Sie die Rolle beim Starten der Instance an oder verknüpfen Sie die Rolle mit einer vorhandenen Instance.
5. Lassen Sie die Anwendung einen Satz vorübergehende Anmeldeinformationen abrufen und verwenden.

Verwenden Sie IAM-Rollen zum Beispiel zum Erteilen von Berechtigungen für Anwendungen, die auf Instances ausgeführt werden, die einen Bucket in Amazon S3 verwenden müssen. Sie können Berechtigungen für IAM-Rollen angeben, indem Sie eine Richtlinie im JSON-Format erstellen. Diese Richtlinien sind denen ähnlich, die Sie für -Benutzer erstellen. Wenn Sie an einer Rolle etwas ändern, wird diese Änderung an alle Instances weitergegeben.

> **Note**
>
> Die Anmeldeinformationen für Amazon EC2 IAM-Rollen unterliegen nicht der in der Rolle konfigurierten maximalen Sitzungsdauer. Weitere Informationen finden Sie unter Methods to assume a role im IAM-Benutzerhandbuch.

Beim Erstellen von IAM-Rollen ordnen Sie IAM-Richtlinien mit geringsten Berechtigungen zu, die den Zugriff auf die spezifischen API-Aufrufe einschränken, die die Anwendung benötigt. Verwenden Sie für die Windows-to-Windows Kommunikation klar definierte und gut dokumentierte Windows-Gruppen und -Rollen, um den Zugriff auf Anwendungsebene zwischen Windows-Instances zu gewähren. Gruppen und Rollen ermöglichen es Kunden, Berechtigungen auf Anwendungs- und NTFS-Ordnerebene zu definieren, um den Zugriff auf anwendungsspezifische Anforderungen zu beschränken.

Sie können nur eine IAM-Rolle an eine Instance anhängen, aber Sie können die gleiche Rolle an viele Instances anhängen. Weitere Informationen zum Erstellen und Verwenden von IAM-Rollen finden Sie unter Rollen im IAM-Benutzerhandbuch.

Sie können Berechtigungen auf Ressourcenebene auf Ihre IAM-Richtlinien anwenden, um zu steuern, ob Benutzer einer Instance IAM-Rollen anfügen, diese ersetzen oder trennen können. Weitere Informationen finden Sie unter Unterstützte Berechtigungen auf Ressourcenebene für Amazon-API-Aktionen EC2 und in diesem Beispiel: Beispiel: Arbeiten mit IAM-Rollen.

Inhalt

- Instance-Profile
- Berechtigungen für Ihren Anwendungsfall
- Abrufen von Sicherheitsanmeldeinformationen aus Instance-Metadaten
- Gewähren von Berechtigungen zum Anhängen einer IAM-Rolle an eine Instance
- Anfügen einer IAM-Rolle an eine Instance
- Instanzidentitätsrollen für EC2 Amazon-Instances

Instance-Profile

Amazon EC2 verwendet ein Instance-Profil als Container für eine IAM-Rolle. Wenn Sie eine IAM-Rolle mithilfe der IAM-Konsole erstellen, erzeugt die Konsole automatisch ein Instance-Profil und gibt ihm denselben Namen wie der entsprechenden Rolle. Wenn Sie die EC2 Amazon-Konsole verwenden, um eine Instance mit einer IAM-Rolle zu starten oder einer Instance eine IAM-Rolle zuzuweisen, wählen Sie die Rolle anhand einer Liste von Instance-Profilnamen aus.

Wenn Sie die AWS CLI API oder ein AWS SDK verwenden, um eine Rolle zu erstellen, erstellen Sie die Rolle und das Instance-Profil als separate Aktionen mit möglicherweise unterschiedlichen Namen. Wenn Sie dann die AWS CLI API oder ein AWS SDK verwenden, um eine Instance mit einer IAM-Rolle zu starten oder einer Instance eine IAM-Rolle zuzuweisen, geben Sie den Namen des Instanzprofils an.

Ein Instance-Profil kann nur eine IAM-Rolle enthalten. Sie können eine IAM-Rolle in mehrere Instance-Profile aufnehmen.

Zum Aktualisieren der Berechtigungen für eine Instance ersetzen Sie das Instance-Profil. Das Entfernen einer Rolle aus einem Instance-Profil wird nicht empfohlen, da es bis zu einer Stunde dauern kann, bis diese Änderung wirksam wird.

Weitere Informationen finden Sie unter Verwenden von Instance-Profilen im IAM-Benutzerhandbuch.

Berechtigungen für Ihren Anwendungsfall

Wenn Sie zum ersten Mal eine IAM-Rolle für Ihre Anwendungen erstellen, können Sie manchmal Berechtigungen erteilen, die über das erforderliche hinausgehen. Bevor Sie Ihre Anwendung in Ihrer Produktionsumgebung starten, können Sie eine IAM-Richtlinie generieren, die auf der Zugriffsaktivität für eine IAM-Rolle basiert. IAM Access Analyzer überprüft Ihre AWS CloudTrail Protokolle und generiert eine Richtlinienvorlage, die die Berechtigungen enthält, die von der Rolle in Ihrem angegebenen Zeitraum verwendet wurden. Sie können die Vorlage verwenden, um eine

verwaltete Richtlinie mit definierten Berechtigungen zu erstellen und sie dann an die IAM-Rolle anzuhängen. Auf diese Weise gewähren Sie nur die Berechtigungen, die die Rolle für die Interaktion mit AWS Ressourcen für Ihren speziellen Anwendungsfall benötigt. Dies hilft Ihnen, die Best Practice einzuhalten, die geringsten Privilegien zu gewähren. Weitere Informationen finden Sie unter Richtliniengenerierung von IAM Access Analyzer im IAM-Benutzerhandbuch.

Abrufen von Sicherheitsanmeldeinformationen aus Instance-Metadaten

Eine Anwendung auf der Instance ruft die von der Rolle bereitgestellten Sicherheitsanmeldeinformationen aus dem Instance-Metadatenelement `iam/security-credentials/`Rollenname ab. Über die mit der Rolle verknüpften Sicherheitsanmeldeinformationen werden der Anwendung die Berechtigungen für die Aktionen und Ressourcen gewährt, die Sie für die Rolle definiert haben. Diese Sicherheitsanmeldeinformationen sind temporär und werden automatisch gewechselt. Neue Anmeldeinformationen stehen spätestens fünf Minuten vor dem Ablauf der alten zur Verfügung.

Weitere Informationen zu Instance-Metadaten erhalten Sie unter Verwenden Sie Instanz-Metadaten, um Ihre EC2 Instanz zu verwalten.

> **Warning**
>
> Wenn Sie Services verwenden, die Instance-Metadaten mit IAM-Rollen nutzen, müssen Sie sicherstellen, dass Sie Ihre Anmeldeinformationen nicht zur Verfügung stellen, wenn die Services HTTP-Aufrufe in Ihrem Auftrag senden. Zu den Arten von Diensten, die Ihre Anmeldeinformationen offenlegen könnten, gehören HTTP-Proxys, HTML/CSS Validatordienste und XML-Prozessoren, die XML-Inklusion unterstützen.

Für Ihre EC2 Amazon-Workloads empfehlen wir, dass Sie die Anmeldeinformationen für die Sitzung mithilfe der unten beschriebenen Methode abrufen. Diese Anmeldeinformationen sollten es Ihrem Workload ermöglichen, AWS -API-Anfragen zu stellen, ohne `sts:AssumeRole` verwenden zu müssen, um dieselbe Rolle zu übernehmen, die bereits mit dieser Instance verknüpft ist. Nur wenn Sie Sitzungs-Tags für die attributbasierte Zugriffskontrolle (ABAC) übergeben oder eine Sitzungsrichtlinie übergeben müssen, um die Berechtigungen der Rolle weiter einzuschränken, sind solche Rollenannahmeaufrufe erforderlich, da sie einen neuen Satz derselben temporären Anmeldeinformationen für die Rollensitzung erstellen.

Wenn Ihr Workload eine Rolle verwendet, um sich selbst anzunehmen, müssen Sie eine Vertrauensrichtlinie erstellen, die ausdrücklich zulässt, dass diese Rolle sich selbst annimmt.

Wenn Sie die Vertrauensrichtlinie nicht erstellen, erhalten Sie den Fehler `AccessDenied`. Weitere Informationen finden Sie unter Aktualisieren einer Vertrauensrichtlinie für Rollen im IAM-Benutzerhandbuch.

IMDSv2

Linux

Führen Sie den folgenden Befehl von Ihrer Linux-Instance aus, um die Sicherheitsanmeldeinformationen für eine IAM-Rolle abzurufen.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name
```

Windows

Führen Sie das folgende cmdlet von Ihrer Windows-Instance aus, um die Sicherheitsanmeldeinformationen für eine IAM-Rolle abzurufen.

```
[string]$token = Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name
```

IMDSv1

Linux

Führen Sie den folgenden Befehl von Ihrer Linux-Instance aus, um die Sicherheitsanmeldeinformationen für eine IAM-Rolle abzurufen.

```
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name
```

Windows

Führen Sie das folgende cmdlet von Ihrer Windows-Instance aus, um die Sicherheitsanmeldeinformationen für eine IAM-Rolle abzurufen.

```
Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/security-credentials/role-name
```

Es folgt eine Beispielausgabe. Wenn Sie die Sicherheitsanmeldedaten nicht abrufen können, finden Sie im IAM-Benutzerhandbuch weitere Informationen unter Ich kann nicht auf die temporären Sicherheitsanmeldedaten auf meiner EC2 Instance zugreifen.

```
{
  "Code" : "Success",
  "LastUpdated" : "2012-04-26T16:39:16Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAIOSFODNN7EXAMPLE",
  "SecretAccessKey" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
  "Token" : "token",
  "Expiration" : "2017-05-17T15:09:54Z"
}
```

Für Anwendungen und Tools for PowerShell Windows-Befehle AWS CLI, die auf der Instance ausgeführt werden, müssen Sie die temporären Sicherheitsanmeldedaten nicht explizit abrufen — die AWS SDKs, AWS CLI, und Tools für Windows rufen die Anmeldeinformationen PowerShell automatisch vom EC2 Instanz-Metadatendienst ab und verwenden sie. Für einen Aufruf außerhalb der Instance mithilfe der temporären Sicherheitsanmeldeinformationen (beispielsweise um IAM-Richtlinien zu testen) müssen Sie den Zugriffsschlüssel, den geheimen Schlüssel und das Sitzungs-Token zur Verfügung stellen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden temporärer Sicherheitsanmeldedaten, um Zugriff auf AWS Ressourcen anzufordern.

Gewähren von Berechtigungen zum Anhängen einer IAM-Rolle an eine Instance

Ihre Identitäten AWS-Konto, z. B. IAM-Benutzer, müssen über bestimmte Berechtigungen verfügen, um eine EC2 Amazon-Instance mit einer IAM-Rolle zu starten, einer Instance eine IAM-Rolle zuzuweisen, die IAM-Rolle für eine Instance zu ersetzen oder eine IAM-Rolle von einer Instance zu trennen. Sie müssen die Berechtigung zum Verwenden der folgenden API-Aktionen nach Bedarf gewähren:

- `iam:PassRole`
- `ec2:AssociateIamInstanceProfile`

- `ec2:DisassociateIamInstanceProfile`
- `ec2:ReplaceIamInstanceProfileAssociation`

> **Note**
>
> Wenn Sie die Ressource für `iam:PassRole` als * angeben, würde dies Zugriff gewähren, um eine Ihrer IAM-Rollen an eine Instance zu übergeben. Um der bewährten Methode der geringsten Rechte zu folgen, geben Sie die spezifischen IAM-Rollen mit an`iam:PassRole`, wie in ARNs der folgenden Beispielrichtlinie dargestellt.

Beispielrichtlinie für den programmatischen Zugriff

Die folgende IAM-Richtlinie gewährt Berechtigungen zum Starten von Instances mit einer IAM-Rolle, zum Anhängen einer IAM-Rolle an eine Instance oder zum Ersetzen der IAM-Rolle für eine Instance mithilfe der AWS CLI oder der Amazon-API. EC2

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances",
         "ec2:AssociateIamInstanceProfile",
         "ec2:DisassociateIamInstanceProfile",
         "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/DevTeam*"
    }
  ]
}
```

Zusätzliche Anforderung für den Konsolenzugriff

Um Berechtigungen für die Ausführung derselben Aufgaben mit der EC2 Amazon-Konsole zu erteilen, müssen Sie auch die `iam:ListInstanceProfiles` API-Aktion angeben.

Anfügen einer IAM-Rolle an eine Instance

Sie können eine IAM-Rolle erstellen und sie während des Starts oder danach einer Instance anfügen. Sie können IAM-Rollen auch ersetzen oder trennen.

Um einer Instance beim Start über die EC2 Amazon-Konsole eine IAM-Rolle zuzuweisen, erweitern Sie Erweiterte Details. Bei IAM-Instance-Profil wählen Sie die IAM-Rolle.

> **Note**
>
> Wenn Sie die IAM-Rolle mit der IAM-Konsole erstellt haben, wurde das Instance-Profil für Sie angelegt und hat denselben Namen wie die Rolle erhalten. Wenn Sie Ihre IAM-Rolle mithilfe der AWS CLI API oder eines AWS SDK erstellt haben, haben Sie Ihrem Instance-Profil möglicherweise einen anderen Namen als der Rolle gegeben.

Sie können einer Instance, die ausgeführt wird oder gestoppt wird, eine IAM-Rolle anfügen. Wenn der Instance bereits eine IAM-Rolle zugewiesen ist, müssen Sie diese durch die neue IAM-Rolle ersetzen.

Console

So fügen Sie einer Instance eine IAM-Rolle an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.
4. Wählen Sie Actions (Aktionen), Security (Sicherheit), Modify IAM role (IAM-Rolle ändern) aus.
5. Für IAM-Rolle wählen Sie das IAM-Instance-Profil.
6. Wählen Sie IAM-Rolle aktualisieren.

AWS CLI

So fügen Sie einer Instance eine IAM-Rolle an

Verwenden Sie den associate-iam-instance-profileBefehl, um der Instance die IAM-Rolle zuzuweisen. Wenn Sie das Instance-Profil angeben, können Sie entweder den Amazon-Ressourcenname (ARN) des Instance-Profils oder dessen Namen verwenden.

```
aws ec2 associate-iam-instance-profile \
    --instance-id i-1234567890abcdef0 \
    --iam-instance-profile Name="TestRole-1"
```

PowerShell

So fügen Sie einer Instance eine IAM-Rolle an

Verwenden Sie das cmdlet Register-EC2IamInstanceProfile.

```
Register-EC2IamInstanceProfile `
    -InstanceId i-1234567890abcdef0 `
    -IamInstanceProfile_Name TestRole-1
```

Um die IAM-Rolle in einer Instance zu ersetzen, an die bereits eine IAM-Rolle angefügt ist, muss die Instance ausgeführt werden. Sie können dies tun, wenn Sie die IAM-Rolle für eine Instance ändern möchten, ohne zuvor die vorhandene Instance zu trennen. Sie können dies beispielsweise tun, um sicherzustellen, dass die von Anwendungen auf der Instance ausgeführten API-Aktionen nicht unterbrochen werden.

Console

So ersetzen Sie eine IAM-Rolle für eine Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.
4. Wählen Sie Actions (Aktionen), Security (Sicherheit), Modify IAM role (IAM-Rolle ändern) aus.
5. Für IAM-Rolle wählen Sie das IAM-Instance-Profil.
6. Wählen Sie IAM-Rolle aktualisieren.

AWS CLI

So ersetzen Sie eine IAM-Rolle für eine Instance

1. Verwenden Sie bei Bedarf den Befehl describe-iam-instance-profile-associations, um die Zuordnungs-ID abzurufen.

```
aws ec2 describe-iam-instance-profile-associations \
    --filters Name=instance-id,Values=i-1234567890abcdef0 \
    --query IamInstanceProfileAssociations.AssociationId
```

2. Verwenden Sie den Befehl replace-iam-instance-profile-association. Geben Sie die Zuordnungs-ID für das vorhandene Instance-Profil und den ARN oder Namen des neuen Instance-Profils an.

```
aws ec2 replace-iam-instance-profile-association \
    --association-id iip-assoc-0044d817db6c0a4ba \
    --iam-instance-profile Name="TestRole-2"
```

PowerShell

So ersetzen Sie eine IAM-Rolle für eine Instance

1. Verwenden Sie bei Bedarf das Get-EC2IamInstanceProfileAssociationCmdlet, um die Zuordnungs-ID abzurufen.

```
(Get-EC2IamInstanceProfileAssociation -Filter @{Name="instance-id";
 Values="i-0636508011d8e966a"}).AssociationId
```

2. Verwenden Sie das cmdlet Set-EC2IamInstanceProfileAssociation. Geben Sie die Zuordnungs-ID für das vorhandene Instance-Profil und den ARN oder Namen des neuen Instance-Profils an.

```
Set-EC2IamInstanceProfileAssociation `
    -AssociationId iip-assoc-0044d817db6c0a4ba `
    -IamInstanceProfile_Name TestRole-2
```

Sie können eine IAM-Rolle von einer laufenden oder angehaltenen Instance trennen.

Console

So trennen Sie eine IAM-Rolle von einer Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.
4. Wählen Sie Actions (Aktionen), Security (Sicherheit), Modify IAM role (IAM-Rolle ändern) aus.
5. Klicken Sie unter IAM-Rolle auf die Option Keine IAM-Rolle.
6. Wählen Sie IAM-Rolle aktualisieren.
7. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie Abhängen ein und wählen Sie dann Abhängen aus.

AWS CLI

So trennen Sie eine IAM-Rolle von einer Instance

1. Verwenden Sie bei Bedarf describe-iam-instance-profile-associations, um die Zuordnungs-ID für das zu trennende IAM-Instance-Profil abzurufen.

```
aws ec2 describe-iam-instance-profile-associations \
    --filters Name=instance-id,Values=i-1234567890abcdef0 \
    --query IamInstanceProfileAssociations.AssociationId
```

2. Verwenden Sie den Befehl disassociate-iam-instance-profile.

```
aws ec2 disassociate-iam-instance-profile --association-id iip-
assoc-0044d817db6c0a4ba
```

PowerShell

So trennen Sie eine IAM-Rolle von einer Instance

1. Verwenden Sie bei Bedarf, Get-EC2IamInstanceProfileAssociationum die Zuordnungs-ID für das zu trennende IAM-Instanzprofil abzurufen.

```
(Get-EC2IamInstanceProfileAssociation -Filter @{Name="instance-id";
 Values="i-0636508011d8e966a"}).AssociationId
```

2. Verwenden Sie das cmdlet Unregister-EC2IamInstanceProfile.

```
Unregister-EC2IamInstanceProfile -AssociationId iip-assoc-0044d817db6c0a4ba
```

Instanzidentitätsrollen für EC2 Amazon-Instances

Jede EC2 Amazon-Instance, die Sie starten, hat eine Instance-Identitätsrolle, die ihre Identität repräsentiert. Eine Instance-Identitätsrolle ist eine Art von IAM-Rolle. AWS Dienste und Funktionen, die zur Verwendung der Instanzidentitätsrolle integriert sind, können sie verwenden, um die Instanz für den Dienst zu identifizieren.

Auf die Anmeldeinformationen für die Instance-Identitätsrolle können Sie über den Instance Metadata Service (IMDS) unter `/identity-credentials/ec2/security-credentials/ec2-instance` zugreifen. Die Anmeldeinformationen bestehen aus einem AWS temporären Zugriffsschlüsselpaar und einem Sitzungstoken. Sie werden verwendet, um AWS Sigv4-Anfragen an die AWS Dienste zu signieren, die die Instanzidentitätsrolle verwenden. Die Anmeldeinformationen sind in den Instance-Metadaten vorhanden, unabhängig davon, ob ein Service oder ein Feature, welches Instance-Identitätsrollen verwendet, in der Instance aktiviert ist.

Instance-Identitätsrollen werden automatisch erstellt, wenn eine Instance gestartet wird. Sie haben kein Rollenvertrauensrichtliniendokument und unterliegen keiner Identitäts- oder Ressourcenrichtlinie.

Unterstützte Services

Die folgenden AWS Dienste verwenden die Instanzidentitätsrolle:

- Amazon EC2 — EC2 Instance Connect verwendet die Instance-Identitätsrolle, um die Hostschlüssel für eine Linux-Instance zu aktualisieren.
- Amazon GuardDuty — GuardDuty Runtime Monitoring verwendet die Instance-Identitätsrolle, damit der Runtime-Agent Sicherheitstelemetrie an den GuardDuty VPC-Endpunkt senden kann.
- AWS Security Token Service (AWS STS) — Die Anmeldeinformationen für die Instance-Identitätsrolle können für die AWS STS `GetCallerIdentity`Aktion verwendet werden.
- AWS Systems Manager— Bei Verwendung der Standard-Host-Management-Konfiguration AWS Systems Manager wird die Identität verwendet, die von der Instance-Identitätsrolle bereitgestellt

wird, um EC2 Instances zu registrieren. Nach der Identifizierung Ihrer Instance kann Systems Manager Ihre `AWSSystemsManagerDefaultEC2InstanceManagementRole`-IAM-Rolle an Ihre Instance weitergeben.

Instanzidentitätsrollen können nicht mit anderen AWS Diensten oder Funktionen verwendet werden, da sie nicht mit Instanzidentitätsrollen integriert sind.

Instance-Identitäts-Rollen-ARN

Die Instance-Identitätsrollen-ARN hat das folgende Format:

```
arn:aws-partition:iam::account-number:assumed-role/aws:ec2-instance/instance-id
```

Zum Beispiel:

```
arn:aws:iam::0123456789012:assumed-role/aws:ec2-instance/i-1234567890abcdef0
```

Weitere Informationen zu ARNs finden Sie unter Amazon Resource Names (ARNs) im IAM-Benutzerhandbuch.

Verwaltung von Updates für EC2 Amazon-Instances

Wir empfehlen Ihnen, das Betriebssystem und die Anwendungen auf Ihren EC2 Instances regelmäßig zu patchen, zu aktualisieren und zu sichern. Mit dem AWS Systems Manager Patch Manager können Sie den Prozess der Installation sicherheitsrelevanter Updates sowohl für das Betriebssystem als auch für Anwendungen automatisieren.

Für EC2 Instances in einer Amazon EC2 Auto Scaling Scaling-Gruppe können Sie das AWS-PatchAsgInstanceRunbook verwenden, um zu verhindern, dass Instances, die gerade gepatcht werden, ersetzt werden. Alternativ können Sie alle Services zur automatischen Aktualisierung oder empfohlenen Prozesse für die Installation von Aktualisierungen verwenden, die vom Anwendungsanbieter bereitgestellt werden.

Ressourcen

- AL2023 — Aktualisierung von AL2 023 im Amazon Linux 2023-Benutzerhandbuch
- AL2— Software auf Ihrer Amazon Linux 2-Instance im Amazon Linux 2-Benutzerhandbuch verwalten
- Windows-Instances – the section called “Update-Management”

Bewährte Methoden für die Sicherheit in Windows-Instances

Es wird empfohlen, die folgenden bewährten Methoden für die Sicherheit in Ihren Windows-Instances zu befolgen.

Inhalt

- Bewährte Methoden für die Sicherheit auf hohem Niveau
- Update-Management
- Konfigurationsmanagement
- Änderungsmanagement
- Prüfung und Rechenschaftspflicht für Amazon EC2 Windows-Instances

Bewährte Methoden für die Sicherheit auf hohem Niveau

Für Ihre Windows Instances sollten Sie die folgenden bewährten Methoden für die Sicherheit auf hohem Niveau einhalten:

- Geringster Zugriff – Gewähren Sie Zugriff nur auf vertrauenswürdige und erwartete Systeme und Speicherorte. Dies gilt für alle Microsoft-Produkte wie Active Directory, Microsoft-Geschäftsproduktivitätsserver und Infrastruktur-Services wie Remote Desktop-Dienste, Reverse-Proxy-Server, IIS-Webserver usw. Verwenden Sie AWS Funktionen wie EC2 Amazon-Instance-Sicherheitsgruppen, Netzwerkzugriffskontrolllisten (ACLs) und Amazon public/private VPC-Subnetze, um die Sicherheit über mehrere Standorte in einer Architektur zu verteilen. Innerhalb einer Windows-Instance können Kunden die Windows-Firewall verwenden, um eine weitere defense-in-depth Strategie innerhalb ihrer Implementierung zu entwickeln. Installieren Sie nur die Betriebssystemkomponenten und -anwendungen, die für die gewünschte Funktion des Systems erforderlich sind. Konfigurieren Sie Infrastruktur-Services wie IIS für die Ausführung unter Servicekonten oder für die Verwendung von Funktionen wie Anwendungspool-Identitäten, um lokal und remote auf Ressourcen in Ihrer gesamten Infrastruktur zuzugreifen.
- Geringste Berechtigung – Bestimmen Sie die Mindestberechtigungen, die Instances und Konten benötigen, um ihre Funktionen auszuführen. Schränken Sie diese Server und Benutzer so ein, dass nur diese definierten Berechtigungen gewährt werden. Verwenden Sie Techniken wie rollenbasierte Zugriffskontrollen, um die Angriffsfläche von Administratorkonten zu reduzieren, und erstellen Sie maximal eingeschränkte Rollen für die Ausführung einer Aufgabe. Verwenden Sie Betriebssystemfunktionen wie Encrypting File System (EFS) in NTFS, um sensible Daten im Ruhezustand zu verschlüsseln und den Anwendungs- und Benutzerzugriff darauf zu kontrollieren.

- Konfigurationsmanagement — Erstellen Sie eine grundlegende Serverkonfiguration, die up-to-date Sicherheitspatches und hostbasierte Schutzpakete umfasst, zu denen Viren- und Malware-Schutz, Erkennung und Verhinderung von Eindringlingen und Überwachung der Dateiintegrität gehören. Bewerten Sie jeden Server anhand der aktuell aufgezeichneten Basislinie, um Abweichungen zu identifizieren und zu kennzeichnen. Stellen Sie sicher, dass jeder Server so konfiguriert ist, dass entsprechende Protokoll- und Prüfungsdaten generiert und sicher gespeichert werden.
- Änderungsmanagement – Erstellen Sie Prozesse zur Steuerung von Änderungen an Serverkonfigurationsbasislinien und arbeiten Sie an vollautomatisierten Änderungsprozessen. Nutzen Sie außerdem Just Enough Administration (JEA) mit Windows PowerShell DSC, um den Administratorzugriff auf die minimal erforderlichen Funktionen zu beschränken.
- Patch-Management — Implementieren Sie Prozesse, die das Betriebssystem und die Anwendungen auf Ihren EC2 Instanzen regelmäßig patchen, aktualisieren und sichern.
- Audit-Logs — Überwachen Sie den Zugriff und alle Änderungen an EC2 Amazon-Instances, um die Serverintegrität zu überprüfen und sicherzustellen, dass nur autorisierte Änderungen vorgenommen werden. Nutzen Sie Funktionen wie Enhanced Logging for IIS, um die standardmäßigen Protokollierungsfunktionen zu verbessern. AWS Funktionen wie VPC Flow Logs AWS CloudTrail sind auch verfügbar, um den Netzwerkzugriff zu überprüfen, einschließlich allowed/denied Anfragen bzw. API-Aufrufen.

Update-Management

Um die besten Ergebnisse zu erzielen, wenn Sie Windows Server auf Amazon ausführen EC2, empfehlen wir Ihnen, die folgenden bewährten Methoden zu implementieren:

- Configure Windows Update
- Update drivers
- Use the latest Windows AMIs
- Test performance before migration
- Update launch agents
- Sie können eine Windows-Instance nach der Installation von Updates neu starten. Weitere Informationen finden Sie unter Eine Amazon-EC2-Instance neu starten.

Weitere Informationen über den Upgrade oder die Migration einer Windows-Instance auf eine neuere Version von Windows Server finden Sie unter EC2–Windows-Instance auf eine neuere Version von Windows Server aktualisieren.

Windows Update konfigurieren

Standardmäßig erhalten Instances, die von AWS Windows Server aus gestartet werden, AMIs keine Updates über Windows Update.

Aktualisieren von Windows-Treibern

Sorgen Sie für die neuesten Treiber auf allen EC2 Windows-Instanzen, um sicherzustellen, dass die neuesten Problembehebungen und Leistungsverbesserungen in Ihrer gesamten Flotte angewendet werden. Abhängig von Ihrem Instance-Typ sollten Sie AWS PV, Amazon ENA und AWS NVMe Treiber aktualisieren.

- Verwenden Sie SNS-Themen, um Informationen über neue Treiber-Releases zu erhalten.
- Verwenden Sie das AWS Systems Manager Automation-Runbook AWSSupport-UpgradeWindowsAWSDrivers, um die Updates einfach auf Ihre Instances anzuwenden.

Starten Sie Instances mit dem neuesten Windows AMIs

AWS veröffentlicht AMIs jeden Monat ein neues Windows, das die neuesten Betriebssystem-Patches, Treiber und Launch-Agents enthält. Nutzen Sie das neueste AMI, wenn Sie neue Instances starten oder eigene, benutzerdefinierte Images erstellen.

- Updates für die einzelnen Versionen von AWS Windows AMIs finden Sie im AWS Windows AMI-Versionsverlauf.
- Informationen zum Erstellen mit den neuesten verfügbaren Versionen AMIs finden Sie unter Abfragen des neuesten Windows-AMI mithilfe des Systems Manager Manager-Parameterspeichers.
- Weitere Informationen zu speziellen Windows-Betriebssystemen, mit AMIs denen Sie Instances für Ihre Datenbank starten können, und Anwendungsfällen zur Compliance-Härtung finden Sie unter Specialized Windows AMIs in der AWS Windows AMI-Referenz.

Testen Sie system/application die Leistung vor der Migration

Die Migration von Unternehmensanwendungen zu AWS kann viele Variablen und Konfigurationen beinhalten. Testen Sie die EC2 Lösung immer auf Leistung, um sicherzustellen, dass:

- Die Instance-Typen müssen ordnungsgemäß konfiguriert sein, inklusive Instance-Größe, Enhanced Networking und Tenancy (geteilte oder Dedicated).

- Die Instance-Topologie muss für die Workload geeignet sein und bei Bedarf Hochleistungsfunktionen wie Dedicated Tenancy, Platzierungsgruppen, Instance-Speicher-Volumes und Bare-Metal-Instances nutzen.

Installieren Sie die neueste Version von EC2 Launch v2

Installieren Sie den neuesten EC2 Launch v2-Agenten, um sicherzustellen, dass die neuesten Verbesserungen in Ihrer gesamten Flotte angewendet werden. Weitere Informationen finden Sie unter EC2Launch v2 installieren.

Wenn Sie über eine gemischte Flotte verfügen oder die Agents EC2 Launch (Windows Server 2016 und 2019) oder EC2 Config (nur ältere Betriebssysteme) weiterhin verwenden möchten, aktualisieren Sie auf die neuesten Versionen der jeweiligen Agenten.

Automatische Aktualisierungen werden auf den folgenden Kombinationen von Windows-Server-Version und Launch-Agenten unterstützt. Sie können automatische Updates in der SSM Quick Setup Host Management-Konsole unter Amazon EC2 Launch Agents aktivieren.

Windows-Version	EC2Starten Sie Version 1	EC2Starten Sie v2
2016	✓	✓
2019	✓	✓
2022		✓

- Weitere Informationen zur Aktualisierung auf EC2 Launch v2 finden Sie unterthe section called “EC2Launch v2 installieren”.
- Informationen zur manuellen Aktualisierung von EC2 Config finden Sie unterthe section called “Installieren von EC2Config”.
- Informationen zur manuellen Aktualisierung von EC2 Launch finden Sie unterthe section called “Installieren von EC2Launch”.

Konfigurationsmanagement

Amazon Machine Images (AMIs) bieten eine Erstkonfiguration für eine EC2 Amazon-Instance, die das Windows-Betriebssystem und optionale kundenspezifische Anpassungen wie Anwendungen

und Sicherheitskontrollen umfasst. Erstellen Sie einen AMI-Katalog mit benutzerdefinierten Basislinien für die Sicherheitskonfiguration, um sicherzustellen, dass alle Windows-Instances mit Standardsicherheitskontrollen gestartet werden. Sicherheitsbasislinien können in ein AMI integriert, beim Start einer EC2 Instance dynamisch gebootet oder als Produkt für eine einheitliche Verteilung über AWS Service Catalog-Portfolios verpackt werden. Weitere Informationen zum Sichern eines AMIs finden Sie unter Bewährte Methoden für die Erstellung eines AMIs.

Jede EC2 Amazon-Instance sollte den organisatorischen Sicherheitsstandards entsprechen. Installieren Sie keine Windows-Rollen und -Features, die nicht erforderlich sind, und installieren Sie Software zum Schutz vor bösartigem Code (Antivirus-, Antischadsoftware, Exploit-Begrenzung), überwachen Sie die Host-Integrität und führen Sie Angriffserkennungsmaßnahmen durch. Konfigurieren Sie Sicherheitssoftware, um Betriebssystem-Sicherheitseinstellungen zu überwachen und zu verwalten, die Integrität kritischer Betriebssystemdateien zu schützen und Warnungen zu Abweichungen von der Sicherheitsbasis zu erhalten. Erwägen Sie, empfohlene Sicherheitskonfigurations-Benchmarks zu implementieren, die von Microsoft, dem Center for Internet Security (CIS) oder dem National Institute of Standards and Technology (NIST) veröffentlicht wurden. Erwägen Sie, andere Microsoft-Tools für bestimmte Anwendungsserver zu verwenden, z. B. Best Practice Analyzer for SQL Server.

AWS Kunden können auch Amazon Inspector-Assessments durchführen, um die Sicherheit und Konformität der auf EC2 Amazon-Instances bereitgestellten Anwendungen zu verbessern. Amazon Inspector prüft Anwendungen automatisch auf Schwachstellen oder Abweichungen von bewährten Methoden und enthält eine Wissensdatenbank aus Hunderten von Regeln, die den gängigen Standards der Sicherheits-Compliance (z. B. PCI DSS) und Schwachstellendefinitionen zugeordnet sind. Beispiele für integrierte Regeln sind die Überprüfung, ob die Remote-Root-Anmeldung aktiviert ist oder, ob anfällige Softwareversionen installiert sind. Diese Regeln werden regelmäßig von AWS Sicherheitsforschern aktualisiert.

Beim Sichern von Windows-Instances wird empfohlen, Active-Directory-Domain-Services zu implementieren, um eine skalierbare, sichere und verwaltbare Infrastruktur für verteilte Standorte zu ermöglichen. Darüber hinaus empfiehlt es sich, nach dem Starten von Instances über die EC2 Amazon-Konsole oder mithilfe eines EC2 Amazon-Bereitstellungstools AWS CloudFormation, native Betriebssystemfunktionen wie Microsoft Windows PowerShell DSC zu verwenden, um den Konfigurationsstatus aufrechtzuerhalten, falls es zu einer Konfigurationsabweichung kommt.

Änderungsmanagement

Nachdem die ersten Sicherheitsbaselines beim Start auf EC2 Amazon-Instances angewendet wurden, kontrollieren Sie die laufenden EC2 Amazon-Änderungen, um die Sicherheit Ihrer virtuellen Maschinen zu gewährleisten. Richten Sie einen Change-Management-Prozess ein, um Änderungen an AWS Ressourcen (wie Sicherheitsgruppen, Routing-Tabellen und Netzwerk ACLs) sowie an Betriebssystem- und Anwendungskonfigurationen (wie Windows- oder Anwendungspatching, Software-Upgrades oder Aktualisierungen von Konfigurationsdateien) zu autorisieren und zu integrieren.

AWS stellt mehrere Tools zur Verfügung, mit denen Sie Änderungen an AWS Ressourcen verwalten können AWS CloudTrail, darunter AWS Config CloudFormation, AWS Elastic Beanstalk, und und Management Packs für Systems Center Operations Manager und System Center Virtual Machine Manager. Beachten Sie, dass Microsoft Windows-Patches am zweiten Dienstag im Monat (oder nach Bedarf) veröffentlicht und alle Windows, die von AMIs verwaltet werden, AWS innerhalb von fünf Tagen AWS aktualisiert, nachdem Microsoft einen Patch veröffentlicht hat. Daher ist es wichtig, alle Baseline- AMIs, CloudFormation Aktualisierungs- und Auto Scaling Scaling-Gruppenkonfigurationen kontinuierlich mit dem neuesten AMI IDs zu patchen und Tools zur Automatisierung des laufenden Instance-Patch-Managements zu implementieren.

Microsoft bietet verschiedene Optionen zum Verwalten von Windows-Betriebssystem- und Anwendungsänderungen. SCCM bietet beispielsweise eine vollständige Lebenszyklusabdeckung von Umgebungsänderungen. Wählen Sie Tools aus, die auf Geschäftsanforderungen zugeschnitten sind, und kontrollieren Sie, wie sich Änderungen auf Anwendungen SLAs, Kapazität, Sicherheit und Notfallwiederherstellungsverfahren auswirken. Vermeiden Sie manuelle Änderungen und nutzen Sie stattdessen automatisierte Konfigurationsverwaltungssoftware oder Befehlszeilentools wie EC2 Run Command oder Windows, PowerShell um skriptbasierte, wiederholbare Änderungsprozesse zu implementieren. Um diese Anforderung zu erfüllen, verwenden Sie Bastion-Hosts mit erweiterter Protokollierung für alle Interaktionen mit Ihren Windows-Instances, um sicherzustellen, dass alle Ereignisse und Aufgaben automatisch aufgezeichnet werden.

Prüfung und Rechenschaftspflicht für Amazon EC2 Windows-Instances

AWS CloudTrail AWS Config, und AWS-Config-Regeln stellen Funktionen zur Prüfung und Nachverfolgung von Änderungen an AWS Ressourcen bereit. Konfigurieren Sie Windows-Ereignisprotokolle, um lokale Protokolldateien an ein zentrales Protokollverwaltungssystem zu senden, um Protokolldaten für die Sicherheits- und Betriebsverhaltensanalyse zu führen. Microsoft System Center Operations Manager (SCOM) aggregiert Informationen zu Microsoft-Anwendungen,

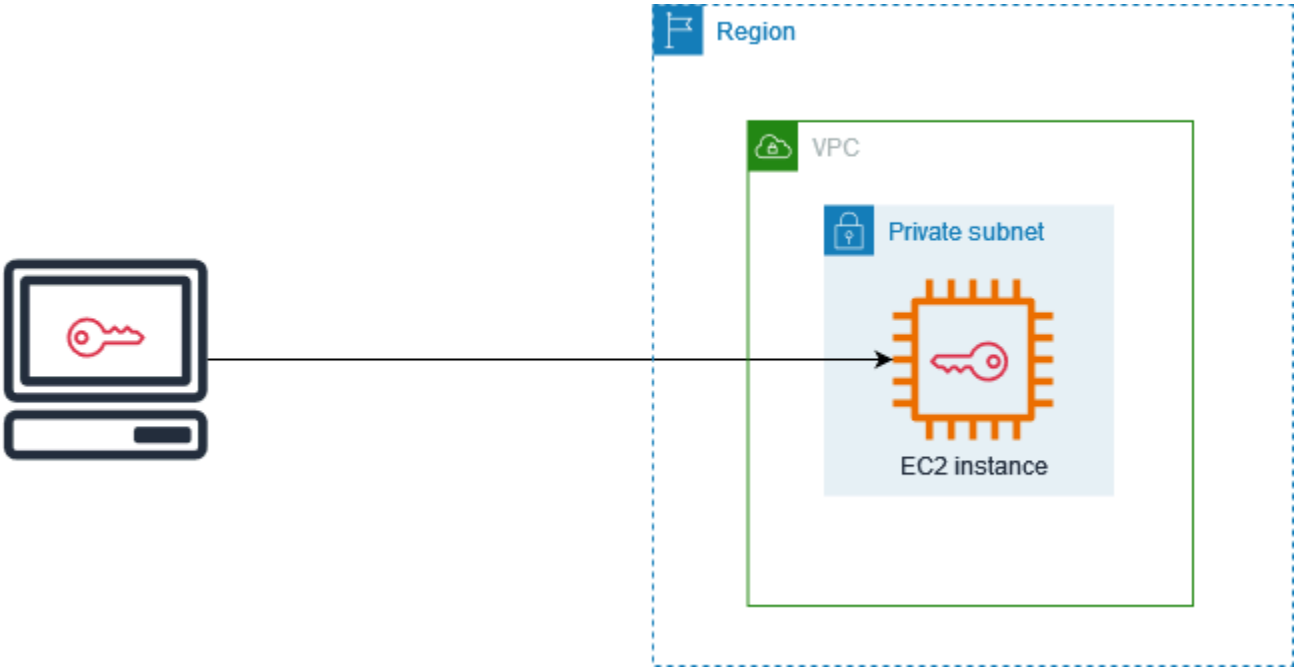
die auf Windows-Instances bereitgestellt werden, und wendet vorkonfigurierte und benutzerdefinierte Regelsätze basierend auf Anwendungsrollen und -services an. System Center Management Packs bauen auf SCOM auf, um anwendungsspezifische Überwachungs- und Konfigurationsrichtlinien bereitzustellen. Diese Management Packs unterstützen Windows Server Active Directory, SharePoint Server 2013, Exchange Server 2013, Lync Server 2013, SQL Server 2014 und viele weitere Server und Technologien.

Zusätzlich zu den Systemverwaltungstools von Microsoft können Kunden Amazon verwenden, CloudWatch um die CPU-Auslastung, die Festplattenleistung und die Netzwerk-I/O von Instanzen zu überwachen und Host- und Instance-Statusprüfungen durchzuführen. Die EC2 Startagenten EC2 Config, EC2 Launch und Launch v2 bieten Zugriff auf zusätzliche, erweiterte Funktionen für Windows-Instances. Sie können beispielsweise Windows-System-, Sicherheits-, Anwendungs- und Internet Information Services (IIS) -Protokolle in Logs exportieren, die dann in CloudWatch Amazon-Metriken und -Alarme integriert werden können. CloudWatch Kunden können auch Skripts erstellen, die Windows-Leistungsindikatoren in CloudWatch benutzerdefinierte Amazon-Metriken exportieren.

EC2 Amazon-Schlüsselpaare und EC2 Amazon-Instances

Ein key pair, bestehend aus einem öffentlichen Schlüssel und einem privaten Schlüssel, ist ein Satz von Sicherheitsanmeldeinformationen, mit denen Sie Ihre Identität nachweisen, wenn Sie eine Verbindung zu einer EC2 Amazon-Instance herstellen. Bei Linux-Instances ermöglicht Ihnen der private Schlüssel eine sichere SSH-Verbindung zu Ihrer Instance herzustellen. Für Windows-Instances ist der private Schlüssel erforderlich, um das Administratorkennwort zu entschlüsseln, das Sie dann verwenden, um sich zu Ihrer Instance zu verbinden.

Amazon EC2 speichert den öffentlichen Schlüssel auf Ihrer Instance, und Sie speichern den privaten Schlüssel, wie in der folgenden Abbildung dargestellt. Es ist wichtig, dass Sie Ihren privaten Schlüssel an einem sicheren Ort aufbewahren, da sich jeder, der Ihren privaten Schlüssel besitzt, mit Ihren Instances verbinden kann, die das Schlüsselpaar verwenden.



Wenn Sie eine Instance starten, können Sie ein Schlüsselpaar angeben, sodass Sie mit einer Methode, die ein Schlüsselpaar erfordert, eine Verbindung zu Ihrer Instance herstellen können. Je nachdem, wie Sie Ihre Sicherheit verwalten, können Sie dasselbe Schlüsselpaar für alle Ihre Instances angeben oder Sie können verschiedene Schlüsselpaare angeben.

Wenn Ihre Instance zum ersten Mal gestartet wird, wird der öffentliche Schlüssel, den Sie beim Start angegeben haben, auf Ihrer Linux-Instance in einem Eintrag innerhalb von `~/.ssh/authorized_keys` platziert. Wenn Sie über SSH eine Verbindung zu Ihrer Linux-Instance herstellen, müssen Sie den privaten Schlüssel angeben, der dem öffentlichen Schlüssel entspricht, um sich anzumelden.

Weitere Informationen zum Herstellen einer Verbindung mit Ihrer EC2 Instance finden Sie unterConnect zu Ihrer EC2 Instance her.

> **Important**
>
> Da Amazon EC2 keine Kopie Ihres privaten Schlüssels aufbewahrt, gibt es keine Möglichkeit, einen privaten Schlüssel wiederherzustellen, wenn Sie ihn verlieren. Es kann jedoch immer noch eine Möglichkeit geben, sich mit Instances zu verbinden, für die Sie den privaten Schlüssel verloren haben. Weitere Informationen finden Sie unter Ich habe meinen privaten Schlüssel verloren. Wie kann ich eine Verbindung zu meiner Instance herstellen?.

Als Alternative zu Schlüsselpaaren können Sie eine Verbindung AWS Systems Manager Session Managerzu Ihrer Instance über eine interaktive browserbasierte Ein-Klick-Shell oder die AWS Command Line Interface ()AWS CLI herstellen.

Inhalt

- Erstellen Sie ein key pair für Ihre EC2 Amazon-Instance
- Ihre Schlüsselpaare beschreiben
- Löschen Ihres Schlüsselpaars
- Einen öffentlichen Schlüssels für Ihre Linux-Instance hinzufügen oder entfernen
- Überprüfen des Fingerabdrucks Ihres Schlüsselpaars

Erstellen Sie ein key pair für Ihre EC2 Amazon-Instance

Sie können Amazon verwenden, EC2 um Ihre Schlüsselpaare zu erstellen, oder Sie können ein Drittanbieter-Tool verwenden, um Ihre Schlüsselpaare zu erstellen und sie dann zu Amazon zu importieren EC2.

Amazon EC2 unterstützt 2048-Bit-SSH-2-RSA-Schlüssel für Linux- und Windows-Instances. Amazon unterstützt EC2 auch ED25519 Schlüssel für Linux-Instances.

Anweisungen zum Herstellen einer Verbindung mit Ihrer Instance nachdem Sie ein Schlüsselpaar erstellt haben finden Sie unter the section called “Herstellen einer Verbindung zu Ihrer Linux-Instance mit SSH” und the section called “Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von RDP”.

Inhalt

- Erstellen Sie ein key pair mit Amazon EC2
- Erstellen Sie ein key pair mit AWS CloudFormation
- Erstellen Sie ein key pair mit einem Drittanbieter-Tool und importieren Sie den öffentlichen Schlüssel zu Amazon EC2

Erstellen Sie ein key pair mit Amazon EC2

Wenn Sie mit Amazon ein key pair erstellen EC2, wird der öffentliche Schlüssel in Amazon gespeichert EC2, und Sie speichern den privaten Schlüssel.

Sie können bis zu 5 000 Schlüsselpaare pro Region erstellen. Erstellen Sie einen Support-Fall, um eine Erhöhung anzufordern. Weitere Informationen finden Sie unter Erstellen eines Support-Falls im Benutzerhandbuch von Support .

Console

Um ein key pair mit Amazon zu erstellen EC2

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Network & Security die Option Key Pairs aus.
3. Wählen Sie Create Key Pair (Schlüsselpaar erstellen) aus.
4. Geben Sie unter Name einen aussagekräftigen Namen für das Schlüsselpaar ein. Amazon EC2 verknüpft den öffentlichen Schlüssel mit dem Namen, den Sie als Schlüsselnamen angeben. Ein Schlüsselname kann bis zu 255 ASCII-Zeichen enthalten. Er darf keine führenden oder nachfolgenden Leerzeichen enthalten.
5. Wählen Sie einen für Ihr Betriebssystem geeigneten Schlüsselpaartyp aus:

   (Linux-Instances) Wählen Sie als Schlüsselpaartyp entweder RSA oder ED25519.

   (Windows-Instances) Wählen Sie als Schlüsselpaartyp die Option RSA aus. ED25519Schlüssel werden für Windows-Instanzen nicht unterstützt.
6. Wählen Sie unter Dateiformat für den privaten Schlüssel das Format aus, in dem der private Schlüssel gespeichert werden soll. Um den privaten Schlüssel in einem Format zu speichern, das mit OpenSSH verwendet werden kann, wählen Sie pem. Um den privaten Schlüssel in einem Format zu speichern, das mit PuTTY verwendet werden kann, wählen Sie ppk.
7. Um dem öffentlichen Schlüssel ein Tag (Markierung) hinzuzufügen, wählen Sie Add Tag (Markierung hinzufügen) und geben Sie den Schlüssel und den Wert für das Tag (Markierung) ein. Wiederholen Sie diesen Schritt für jeden Tag (Markierung).
8. Wählen Sie Create Key Pair (Schlüsselpaar erstellen) aus.
9. Die private Schlüsseldatei wird von Ihrem Browser automatisch runtergeladen. Der Basisdateiname ist der Name, den Sie als Name des Schlüsselpaars angegeben haben und die Dateinamenserweiterung wird durch das ausgewählte Dateiformat bestimmt. Speichern Sie die Datei mit dem privaten Schlüssel an einem sicheren Ort.

> **Important**
>
> Dies ist die einzige Möglichkeit, die private Schlüsseldatei zu speichern.

10. Wenn Sie einen SSH-Kunden auf einem macOS- oder Linux-Computer verwenden möchten, um eine Verbindung zu Ihrer Linux Instance herzustellen, legen Sie mit dem folgenden Befehl die Berechtigungen für Ihre private Schlüsseldatei so fest, dass nur Sie sie lesen können.

```
chmod 400 key-pair-name.pem
```

Wenn Sie diese Berechtigungen nicht festlegen, können Sie unter Verwendung dieses Schlüsselpaars keine Verbindung zu Ihrer Instance herstellen. Weitere Informationen finden Sie unter Fehler: Ungeschützte private Schlüsseldatei.

AWS CLI

Um ein key pair mit Amazon zu erstellen EC2

1. Verwenden Sie den create-key-pair-Befehl wie folgt, um das Schlüsselpaar zu generieren und den privaten Schlüssel in einer `.pem`-Datei zu speichern. Die Option `--query` druckt das private Schlüsselmaterial in die Ausgabe. Die Option `--output` speichert das private Schlüsselmaterial in die angegebene Datei. Die Erweiterung sollte je nach Schlüsselformat entweder `.pem` oder `.ppk` lauten. Der private Schlüssel kann einen Namen haben, der sich vom Namen des öffentlichen Schlüssels unterscheidet. Verwenden Sie jedoch denselben Namen, um die Verwendung zu erleichtern.

```
aws ec2 create-key-pair \
    --key-name my-key-pair \
    --key-type rsa \
    --key-format pem \
    --query "KeyMaterial" \
    --output text > my-key-pair.pem
```

2. Wenn Sie einen SSH-Kunden auf einem macOS- oder Linux-Computer verwenden möchten, um eine Verbindung zu Ihrer Linux Instance herzustellen, legen Sie mit dem folgenden Befehl die Berechtigungen für Ihre private Schlüsseldatei so fest, dass nur Sie sie lesen können.

```
chmod 400 key-pair-name.pem
```

Wenn Sie diese Berechtigungen nicht festlegen, können Sie unter Verwendung dieses Schlüsselpaars keine Verbindung zu Ihrer Instance herstellen. Weitere Informationen finden Sie unter Fehler: Ungeschützte private Schlüsseldatei.

PowerShell

Um ein key pair mit Amazon zu erstellen EC2

Verwenden Sie das cmdlet New-EC2KeyPair wie folgt, um den Schlüssel zu generieren und diesen in einer `.pem`- oder `.ppk`-Datei zu speichern. Das cmdlet Out-File speichert das private Schlüsselmaterial in einer Datei mit der angegebenen Erweiterung. Die Erweiterung sollte je nach Schlüsselformat entweder `.pem` oder `.ppk` lauten. Der private Schlüssel kann einen Namen haben, der sich vom Namen des öffentlichen Schlüssels unterscheidet. Verwenden Sie jedoch denselben Namen, um die Verwendung zu erleichtern.

```
(New-EC2KeyPair `
    -KeyName "my-key-pair" `
    -KeyType "rsa" `
    -KeyFormat "pem").KeyMaterial | Out-File -Encoding ascii -FilePath C:\path\my-key-pair.pem
```

Erstellen Sie ein key pair mit AWS CloudFormation

Wenn Sie mit ein neues key pair erstellen CloudFormation, wird der private Schlüssel im AWS Systems Manager Parameter Store gespeichert. Der Parametername hat das folgende Format:

```
/ec2/keypair/key_pair_id
```

Weitere Informationen finden Sie unter AWS Systems Manager -Parameterspeicher im Benutzerhandbuch für AWS Systems Manager .

Um ein key pair zu erstellen mit CloudFormation

1. Geben Sie die AWS::EC2::KeyPairRessource in Ihrer Vorlage an.

```
Resources:
```

```
  NewKeyPair:
    Type: 'AWS::EC2::KeyPair'
    Properties:
      KeyName: new-key-pair
```

2. Verwenden Sie den describe-key-pairs-Befehl wie folgt, um die ID des Schlüsselpaars abzurufen.

```
aws ec2 describe-key-pairs --filters Name=key-name,Values=new-key-pair --query
 KeyPairs[*].KeyPairId --output text
```

Es folgt eine Beispielausgabe.

```
key-05abb699beEXAMPLE
```

3. Verwenden Sie den get-parameter-Befehl wie folgt, um den Parameter für Ihren Schlüssel abzurufen und das Schlüsselmaterial in einer `.pem`-Datei zu speichern.

```
aws ssm get-parameter --name /ec2/keypair/key-05abb699beEXAMPLE --with-decryption
 --query Parameter.Value --output text > new-key-pair.pem
```

Erforderliche IAM-Berechtigungen

Um Parameter Store-Parameter in Ihrem Namen verwalten CloudFormation zu können, muss die IAM-Rolle, die von CloudFormation oder Ihrem Benutzer übernommen wurde, über die folgenden Berechtigungen verfügen:

- `ssm:PutParameter` – Gewährt die Berechtigung zum Erstellen eines Parameters für das private Schlüsselmaterial.
- `ssm:DeleteParameter` – Gewährt die Berechtigung zum Löschen des Parameters, der das private Schlüsselmaterial gespeichert hat. Diese Berechtigung ist erforderlich, unabhängig davon, ob das Schlüsselpaar importiert oder von CloudFormation erstellt wurde.

Wenn ein key pair CloudFormation gelöscht wird, das von einem Stack erstellt oder importiert wurde, führt es eine Berechtigungsprüfung durch, um festzustellen, ob Sie berechtigt sind, Parameter zu löschen, obwohl ein Parameter nur CloudFormation erstellt wird, wenn er ein key pair erstellt, nicht, wenn er ein key pair importiert. CloudFormation testet anhand eines erfundenen Parameternamens, der mit keinem Parameter in Ihrem Konto übereinstimmt, die erforderliche Berechtigung. Daher

wird in der `AccessDeniedException`-Fehlermeldung möglicherweise ein fiktiver Parametername angezeigt.

Erstellen Sie ein key pair mit einem Drittanbieter-Tool und importieren Sie den öffentlichen Schlüssel zu Amazon EC2

Anstatt Amazon EC2 zum Erstellen eines Schlüsselpaars zu verwenden, können Sie mit einem Drittanbieter-Tool eine RSA oder ein ED25519 key pair erstellen und dann den öffentlichen Schlüssel in Amazon EC2 importieren.

Anforderungen für Schlüsselpaare

- Unterstützte Typen:
  - (Linux und Windows) RSA
  - (Nur Linux) ED25519

    > **Note**
    >
    > ED25519 Schlüssel werden für Windows-Instanzen nicht unterstützt.

  - Amazon EC2 akzeptiert keine DSA-Schlüssel.
- Unterstützte Formate
  - OpenSSH-Format für öffentliche Schlüssel (Für Linux das Format in `~/.ssh/authorized_keys`)
  - (Nur Linux) Wenn Sie eine Verbindung über SSH herstellen und gleichzeitig die EC2 Instance Connect API verwenden, wird das SSH2 Format ebenfalls unterstützt.
  - Das private Schlüsseldateiformat von SSH muss PEM oder PPK sein
  - (Nur RSA) Base64-codiertes DER-Format
  - (Nur RSA) SSH-Dateiformat für öffentliche Schlüssel wie in RFC 4716 angegeben
- Die unterstützten Längen sind:
  - 1 024, 2 048 und 4 096.
  - (Nur Linux) Wenn Sie eine Verbindung über SSH herstellen und gleichzeitig die EC2 Instance Connect API verwenden, sind die unterstützten Längen 2048 und 4096.

So erstellen Sie ein Schlüsselpaar mit einem Tool eines Drittanbieters

1. Generieren Sie ein Schlüsselpaar mit einem Tool eines Drittanbieters Ihrer Wahl. Beispiel: Sie können ssh-keygen (ein mit der standardmäßigen OpenSSH-Installation bereitgestelltes Tool) verwenden. Alternativ bieten Java, Ruby, Python und viele andere Programmiersprachen Standardbibliotheken, die Sie zum Erstellen eines Schlüsselpaars verwenden können.

   > **Important**
   >
   > Der private Schlüssel muss im PEM– oder PPK-Format vorliegen. Verwenden Sie zum Beispiel `ssh-keygen -m PEM`, um den OpenSSH-Schlüssel im PEM-Format zu generieren.

2. Speichern Sie den öffentlichen Schlüssel in einer lokalen Datei. Beispielsweise `~/.ssh/my-key-pair.pub` (Linux, macOS) oder `C:\keys\my-key-pair.pub` (Windows). Die Dateinamenerweiterung für diese Datei ist nicht wichtig.
3. Speichern Sie den privaten Schlüssel in einer lokalen Datei mit der Erweiterung `.pem` oder `.ppk`. Beispielsweise `~/.ssh/my-key-pair.pem` oder `~/.ssh/my-key-pair.ppk` (Linux, macOS) oder `C:\keys\my-key-pair.pem` oder `C:\keys\my-key-pair.ppk` (Windows). Die Dateierweiterung ist wichtig, da Sie je nach dem Tool, das Sie für die Verbindung mit Ihrer Instance verwenden, ein bestimmtes Dateiformat benötigen. OpenSSH benötigt eine `.pem`-Datei, während PuTTY eine `.ppk`-Datei benötigt.

   > **Important**
   >
   > Speichern Sie die Datei mit dem privaten Schlüssel an einem sicheren Ort. Sie müssen den Namen für Ihren öffentlichen Schlüssel beim Starten einer Instance angeben. Der entsprechende private Schlüssel muss jedes Mal angegeben werden, wenn Sie eine Verbindung mit der Instance herstellen.

Nachdem Sie das key pair erstellt haben, verwenden Sie eine der folgenden Methoden, um Ihren öffentlichen Schlüssel zu Amazon zu importieren EC2.

Console

Um den öffentlichen Schlüssel zu Amazon zu importieren EC2

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Key Pairs aus.
3. Wählen Sie Import Key Pair (Schlüsselpaar importieren) aus.
4. Geben Sie unter Name einen aussagekräftigen Namen für den öffentlichen Schlüssel ein. Der Name kann bis zu 255 ASCII-Zeichen enthalten. Er darf keine führenden oder nachfolgenden Leerzeichen enthalten.

   > **Note**
   >
   > Wenn Sie von der EC2 Konsole aus eine Verbindung zu Ihrer Instance herstellen, schlägt die Konsole diesen Namen als Namen für Ihre private Schlüsseldatei vor.

5. Wählen Sie entweder Browse (Durchsuchen), um zu Ihrem öffentlichen Schlüssel zu navigieren und ihn auszuwählen oder fügen Sie den Inhalt Ihres öffentlichen Schlüssels in das Feld Public key contents (Inhalt des öffentlichen Schlüssels) ein.
6. Wählen Sie Import Key Pair (Schlüsselpaar importieren) aus.
7. Stellen Sie sicher, dass der importierte öffentliche Schlüssel in der Liste der Schlüsselpaare angezeigt wird.

AWS CLI

Um den öffentlichen Schlüssel zu Amazon zu importieren EC2

Verwenden Sie den Befehl import-key-pair.

```
aws ec2 import-key-pair \
    --key-name my-key-pair \
    --public-key-material fileb://path/my-key-pair.pub
```

So überprüfen Sie, ob das Schlüsselpaar erfolgreich importiert wurde

Verwenden Sie den Befehl describe-key-pairs.

```
aws ec2 describe-key-pairs --key-names my-key-pair
```

PowerShell

Um den öffentlichen Schlüssel zu Amazon zu importieren EC2

Verwenden Sie das cmdlet Import-EC2KeyPair.

```
$publickey=[Io.File]::ReadAllText("C:\Users\TestUser\.ssh\id_rsa.pub")
Import-EC2KeyPair `
    -KeyName my-key-pair `
    -PublicKey $publickey
```

So überprüfen Sie, ob das Schlüsselpaar erfolgreich importiert wurde

Verwenden Sie das cmdlet Get-EC2KeyPair.

```
Get-EC2KeyPair -KeyName my-key-pair
```

Ihre Schlüsselpaare beschreiben

Sie können die Schlüsselpaare beschreiben, die Sie bei Amazon gespeichert haben EC2. Sie können auch das Material zum öffentlichen Schlüssel abrufen und den öffentlichen Schlüssel identifizieren, der beim Start angegeben wurde.

Aufgaben

- Ihre Schlüsselpaare beschreiben
- Abrufen des Materials zum öffentlichen Schlüssel
- Identifizieren des öffentlichen Schlüssels, der beim Start angegeben wurde

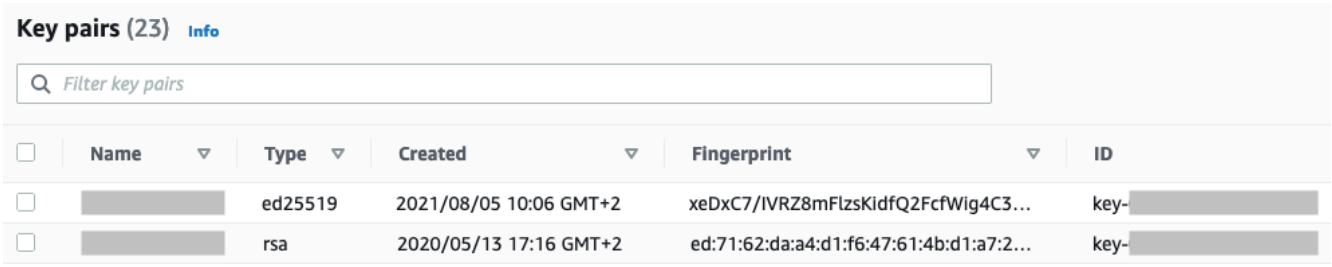
Ihre Schlüsselpaare beschreiben

Sie können die folgenden Informationen zu Ihren öffentlichen Schlüsseln, die in Amazon gespeichert sind, einsehen EC2: Name des öffentlichen Schlüssels, ID, Schlüsseltyp, Fingerabdruck, Material des öffentlichen Schlüssels, Datum und Uhrzeit (in der UTC-Zeitzone), an dem der Schlüssel von Amazon erstellt wurde EC2 (wenn der Schlüssel von einem Drittanbieter-Tool erstellt wurde, sind es Datum und Uhrzeit des Imports des Schlüssels zu Amazon EC2) und alle Tags, die mit dem öffentlichen Schlüssel verknüpft sind.

Console

So zeigen Sie Informationen zu Ihren Schlüsselpaaren an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich Key Pairs (Schlüsselpaare) aus.
3. Sie können Informationen zu jedem öffentlichen Schlüssel in der Tabelle Key pairs (Schlüsselpaare) anzeigen.



4. Um die Tags eines öffentlichen Schlüssels anzuzeigen, aktivieren Sie das Kontrollkästchen neben dem Schlüssel und klicken dann auf Aktionen und Tags verwalten.

AWS CLI

So zeigen Sie Informationen zu einem Schlüsselpaar an

Verwenden Sie den Befehl describe-key-pairs.

```
aws ec2 describe-key-pairs --key-names key-pair-name
```

PowerShell

So zeigen Sie Informationen zu einem Schlüsselpaar an

Verwenden Sie das cmdlet Get-EC2KeyPair.

```
Get-EC2KeyPair -KeyName key-pair-name
```

Abrufen des Materials zum öffentlichen Schlüssel

Sie können das öffentliche Schlüsselmaterial für Ihre Schlüsselpaare abrufen. Es folgt ein Beispiel für einen öffentlichen Schlüssel. Beachten Sie, dass zur besseren Lesbarkeit Zeilenumbrüche hinzugefügt wurden.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

Private key

So rufen Sie das öffentliche Schlüsselmaterial mit ssh-keygen ab (Linux)

Verwenden Sie auf Ihrem lokalen Linux- oder macOS-Computer den Befehl ssh-keygen. Geben Sie den Pfad an, in den Sie Ihren privaten Schlüssel heruntergeladen haben (die `.pem`-Datei).

```
ssh-keygen -y -f /path_to_key_pair/my-key-pair.pem
```

Wenn der Befehl ssh-keygen fehlschlägt, führen Sie den Befehl chmod aus, um sicherzustellen, dass die private Schlüsseldatei über die erforderlichen Berechtigungen verfügt.

```
chmod 400 key-pair-name.pem
```

Um das Material mit öffentlichen Schlüsseln mit Pu TTYgen (Windows) abzurufen

Starten Sie Pu auf Ihrem lokalen Windows-ComputerTTYgen. Wählen Sie Laden aus. Wählen Sie die private `.ppk`- oder `.pem`-Schlüsseldatei aus. Pu TTYgen zeigt den öffentlichen Schlüssel unter Öffentlicher Schlüssel zum Einfügen in die OpenSSH-Datei authorized_keys an. Sie können den öffentlichen Schlüssel auch anzeigen, indem Sie Save public key (Öffentlichen Schlüssel speichern) wählen, einen Namen für die Datei angeben, diese speichern und dann öffnen.

AWS CLI

So rufen Sie das öffentliche Schlüsselmaterial ab

Verwenden Sie den folgenden Befehl und geben Sie die Option an. describe-key-pairs`--include-public-key`

```
aws ec2 describe-key-pairs \
    --key-names key-pair-name \
    --include-public-key \
    --query "KeyPairs[].PublicKey"
```

PowerShell

So rufen Sie das öffentliche Schlüsselmaterial ab

Verwenden Sie das cmdlet Get-EC2KeyPair.

```
(Get-EC2KeyPair -KeyName key-pair-name -IncludePublicKey $true).PublicKey
```

IMDSv2

Linux

Führen Sie die folgenden Befehle in Ihrer Linux-Instance aus.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key
```

Windows

Führen Sie die folgenden cmdlets in Ihrer Windows-Instance aus.

```
[string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri
 http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

IMDSv1

Linux

Führen Sie den folgenden Befehl in Ihrer Linux-Instance aus.

```
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Windows

Führen Sie das folgende cmdlet in Ihrer Windows-Instance aus.

```
Invoke-RestMethod -uri  http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
```

Identifizieren des öffentlichen Schlüssels, der beim Start angegeben wurde

Wenn Sie beim Starten einer Instance einen öffentlichen Schlüssel angeben, wird der Name des öffentlichen Schlüssels von der Instance aufgezeichnet. Der öffentliche Schlüsselname, der für eine Instance berichtet wird, ändert sich nicht, auch wenn Sie den öffentlichen Schlüssel in der Instance ändern oder öffentliche Schlüssel hinzufügen.

Console

So identifizieren Sie den öffentlichen Schlüssel, der beim Start der Instance angegeben wurde

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.
4. Suchen Sie auf der Registerkarte Details unter Instance-Details nach Beim Start zugewiesenes Schlüsselpaar.

AWS CLI

So identifizieren Sie den öffentlichen Schlüssel, der beim Start der Instance angegeben wurde

Verwenden Sie den folgenden describe-instances-Befehl.

```
aws ec2 describe-instances \
    --instance-id i-1234567890abcdef0 \
    --query "Reservations[].Instances[].KeyName" \
    --output text
```

Es folgt eine Beispielausgabe.

```
key-pair-name
```

PowerShell

So identifizieren Sie den öffentlichen Schlüssel, der beim Start der Instance angegeben wurde

Verwenden Sie das cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances | Select KeyName
```

Es folgt eine Beispielausgabe.

```
KeyName
-------
key-pair-name
```

Löschen Ihres Schlüsselpaars

Sie können ein key pair löschen, wodurch der in Amazon gespeicherte öffentliche Schlüssel entfernt wird EC2. Durch das Löschen eines Schlüsselpaars wird der entsprechende private Schlüssel nicht gelöscht.

Wenn Sie einen öffentlichen Schlüssel mit den folgenden Methoden löschen, löschen Sie nur den öffentlichen Schlüssel, den Sie in Amazon gespeichert haben, EC2 als Sie das key pair erstellt oder importiert haben. Durch das Löschen eines öffentlichen Schlüssels wird der öffentliche Schlüssel nicht aus Instances entfernt, zu denen Sie ihn hinzugefügt haben, entweder beim Starten der Instance oder später. Außerdem wird der private Schlüssel dabei nicht auf Ihrem lokalen Computer gelöscht. Sie können weiterhin eine Verbindung zu Instances herstellen, die Sie mit einem öffentlichen Schlüssel gestartet haben, den Sie von Amazon gelöscht haben, EC2 solange Sie noch über die Datei mit dem privaten Schlüssel (`.pem`) verfügen.

> **Important**
>
> Wenn Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe verwenden (z. B. in einer Elastic Beanstalk Beanstalk-Umgebung), stellen Sie sicher, dass der öffentliche Schlüssel, den Sie löschen, nicht in einer zugehörigen Startvorlage oder Startkonfiguration angegeben ist. Wenn Amazon EC2 Auto Scaling eine fehlerhafte Instance erkennt, startet es eine Ersatz-Instance. Der Start der Instance schlägt jedoch fehl, wenn der öffentliche Schlüssel nicht gefunden werden kann. Weitere Informationen finden Sie unter Vorlagen starten im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Console

Um Ihren öffentlichen Schlüssel bei Amazon zu löschen EC2

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Key Pairs aus.
3. Wählen Sie das zu löschende Schlüsselpaar aus und wählen Sie Actions (Aktionen), Delete (Löschen).
4. Geben Sie in das Bestätigungsfeld `Delete` ein und wählen Sie dann Delete (Löschen).

AWS CLI

Um Ihren öffentlichen Schlüssel bei Amazon zu löschen EC2

Verwenden Sie den Befehl delete-key-pair.

```
aws ec2 delete-key-pair --key-name my-key-pair
```

PowerShell

Um Ihren öffentlichen Schlüssel bei Amazon zu löschen EC2

Verwenden Sie das cmdlet Remove-EC2KeyPair.

```
Remove-EC2KeyPair -KeyName my-key-pair
```

Einen öffentlichen Schlüssels für Ihre Linux-Instance hinzufügen oder entfernen

Wenn Sie einen privaten Schlüssel verlieren, verlieren Sie den Zugriff auf alle Instances, die das Schlüsselpaar verwenden. Weitere Informationen zum Herstellen einer Verbindung zu einer Instance mit einem anderen Schlüsselpaar als dem, das Sie beim Start angegeben haben, finden Sie unter Ich habe meinen privaten Schlüssel verloren.

Sie können das Schlüsselpaar beim Starten einer Instance angeben. Wenn Sie beim Start ein Schlüsselpaar angeben, wird das Material zum öffentlichen Schlüssel, wenn Ihre Instance zum ersten

Mal hochfährt, auf Ihrer Linux-Instance in einem Eintrag innerhalb von `~/.ssh/authorized_keys` platziert. Wenn Sie erstmalig über SSH eine Verbindung zu Ihrer Linux-Instance herstellen, müssen Sie den Standardbenutzer und den privaten Schlüssel angeben, der dem in Ihrer Linux-Instance gespeicherten öffentlichen Schlüssel entspricht.

Nachdem Sie eine Verbindung zur Instance hergestellt haben, können Sie das Schlüsselpaar ändern, das für den Zugriff auf das Standard-Systemkonto der Instance verwendet wird, indem Sie einen neuen öffentlichen Schlüssel für die Instance hinzufügen oder den öffentlichen Schlüssel für die Instance ersetzen (Löschen des vorhandenen öffentlichen Schlüssels und Hinzufügen eines neuen Schlüssels). Sie können auch alle öffentlichen Schlüssel aus einer Instance entfernen.

Sie können aus den folgenden Gründen ein Schlüsselpaar hinzufügen oder ersetzen:

- Wenn ein Benutzer in Ihrer Organisation mithilfe eines separaten Schlüsselpaars Zugriff auf den Systembenutzer benötigt, können Sie den öffentlichen Schlüssel zu Ihrer Instance hinzufügen.
- Wenn ein Benutzer eine Kopie des privaten Schlüssels (`.pem`-Datei) besitzt und Sie verhindern möchten, dass er eine Verbindung zu Ihrer Instance herstellt (beispielsweise weil er Ihre Organisation verlassen hat), können Sie den öffentlichen Schlüssel für die Instance löschen und durch einen neuen ersetzen.
- Wenn Sie ein Linux-AMI von einer Instance erstellen, wird das Material zum öffentlichen Schlüssel von der Instance in das AMI kopiert. Wenn Sie eine Instance über das AMI starten, enthält die neue Instance den öffentlichen Schlüssel aus der ursprünglichen Instance. Um zu verhindern, dass ein Benutzer, der im Besitz des privaten Schlüssels ist, eine Verbindung zur neuen Instance herstellen kann, entfernen Sie den öffentlichen Schlüssel aus der ursprünglichen Instance, bevor Sie das AMI erstellen.

Verwenden Sie die folgenden Verfahren, um das Schlüsselpaar für den Standardbenutzer zu ändern, z. B. `ec2-user`. Informationen zum Hinzufügen von Benutzern zu Ihrer Instance finden Sie in der Dokumentation des Betriebssystems Ihrer Instance.

So fügen Sie ein Schlüsselpaar hinzu oder ersetzen es

1. Erstellen Sie mit der EC2Amazon-Konsole oder einem Drittanbieter-Tool ein neues key pair.
2. Rufen Sie den öffentlichen Schlüssel über Ihr neues Schlüsselpaar ab. Weitere Informationen finden Sie unter Abrufen des Materials zum öffentlichen Schlüssel.
3. Verbinden Sie sich mit der Instance.

4. Öffnen Sie die `.ssh/authorized_keys`-Datei in der Instance in einem Texteditor Ihrer Wahl. Fügen Sie die öffentlichen Schlüsselinformationen aus Ihrem neuen Schlüsselpaar unter den vorhandenen öffentlichen Schlüsselinformationen ein und speichern Sie die Datei.
5. Trennen Sie die Verbindung zur Instance. Testen Sie, ob Sie mit dem privaten Schlüssel aus dem neuen Schlüsselpaar eine Verbindung zur Instance herstellen können.
6. Wenn Sie Amazon EC2 Auto Scaling, EC2 Fleet oder eine Startvorlage zum Starten Ihrer Instances verwenden, überprüfen Sie, ob das key pair, das Sie ersetzen, in Ihrer Startvorlage oder Startkonfiguration angegeben ist. Andernfalls schlagen Instance-Starts fehl.
7. (Optional) Falls Sie ein vorhandenes Schlüsselpaar ersetzen, stellen Sie eine Verbindung zu Ihrer Instance her und löschen Sie die Informationen zum öffentlichen Schlüssel für Ihr ursprüngliches Schlüsselpaar aus der `.ssh/authorized_keys`-Datei.

Öffentlichen Schlüssel von einer Instance entfernen

1. Verbinden Sie sich mit der Instance.
2. Öffnen Sie die `.ssh/authorized_keys`-Datei in der Instance in einem Texteditor Ihrer Wahl. Löschen Sie die Informationen zum öffentlichen Schlüssel und speichern Sie die Datei.

> **Warning**
>
> Wenn Sie alle öffentlichen Schlüssel von einer Instance entfernen und die Verbindung zur Instance trennen, können Sie keine neue Verbindung zur Instance herstellen – es sei denn, Sie haben eine alternative Möglichkeit zur Anmeldung konfiguriert.

Überprüfen des Fingerabdrucks Ihres Schlüsselpaars

Um den Fingerabdruck Ihres key pair zu überprüfen, vergleichen Sie den Fingerabdruck, der auf der Seite Schlüsselpaare in der EC2 Amazon-Konsole angezeigt oder vom describe-key-pairsBefehl zurückgegeben wird, mit dem Fingerabdruck, den Sie mit dem privaten Schlüssel auf Ihrem lokalen Computer generieren. Diese Fingerabdrücke sollten übereinstimmen.

Wenn Amazon einen Fingerabdruck EC2 berechnet, fügt Amazon dem Fingerabdruck EC2 möglicherweise zusätzliche Zeichen hinzu. = Andere Tools wie etwa ssh-keygen lassen dieses Padding unter Umständen weg.

Wenn Sie versuchen, den Fingerabdruck Ihrer EC2 Linux-Instance zu verifizieren, nicht den Fingerabdruck Ihres key pair, finden Sie weitere Informationen unter Instance-Fingerabdruck abrufen.

So werden die Fingerabdrücke berechnet

Amazon EC2 verwendet verschiedene Hash-Funktionen, um die Fingerabdrücke für RSA und ED25519 Schlüsselpaare zu berechnen. Darüber hinaus EC2 berechnet Amazon die Fingerabdrücke für RSA-Schlüsselpaare mithilfe verschiedener Hash-Funktionen unterschiedlich, je nachdem, ob das key pair von Amazon erstellt EC2 oder zu Amazon importiert wurde. EC2

In der folgenden Tabelle sind die Hash-Funktionen aufgeführt, die zur Berechnung der Fingerabdrücke für RSA und ED25519 Schlüsselpaare verwendet werden, die von Amazon erstellt EC2 und in Amazon importiert werden. EC2

(Linux-Instances) Hash-Funktion zur Berechnung von Fingerabdrücken

Schlüsselpaar-Quelle	RSA-Schlüsselpaare (Windows und Linux)	ED25519 Schlüsselpaare (Linux)
Erstellt von Amazon EC2	SHA-1	SHA-1
Zu Amazon importiert EC2	MD5[1]	SHA-1

[1] Wenn Sie einen öffentlichen RSA-Schlüssel zu Amazon importieren EC2, wird der Fingerabdruck mithilfe einer MD5 Hash-Funktion berechnet. Dies gilt unabhängig davon, wie Sie das key pair erstellt haben, z. B. mithilfe eines Drittanbietertools oder durch Generieren eines neuen öffentlichen Schlüssels aus einem vorhandenen privaten Schlüssel, der mit Amazon erstellt wurde EC2.

Bei Verwendung des gleichen Schlüsselpaars in verschiedenen Regionen

Wenn Sie dasselbe key pair verwenden möchten, um eine Verbindung zu Instances in verschiedenen Instanzen herzustellen AWS-Regionen, müssen Sie den öffentlichen Schlüssel in alle Regionen importieren, in denen Sie ihn verwenden werden. Wenn Sie Amazon verwenden, EC2 um das key pair zu erstellen, können Sie Abrufen des Materials zum öffentlichen Schlüssel dies tun, damit Sie den öffentlichen Schlüssel in die anderen Regionen importieren können.

Note

- Wenn Sie mit Amazon EC2 ein RSA-Schlüsselpaar erstellen und dann einen öffentlichen Schlüssel aus dem EC2 privaten Amazon-Schlüssel generieren, haben die importierten öffentlichen Schlüssel einen anderen Fingerabdruck als der ursprüngliche öffentliche Schlüssel. Dies liegt daran, dass der Fingerabdruck des ursprünglichen RSA-Schlüssels, der mit Amazon erstellt wurde, mithilfe einer SHA-1-Hash-Funktion berechnet EC2 wird, während der Fingerabdruck der importierten RSA-Schlüssel mithilfe einer MD5 Hash-Funktion berechnet wird.
- Bei ED25519 Schlüsselpaaren sind die Fingerabdrücke identisch, unabhängig davon, ob sie von Amazon erstellt EC2 oder zu Amazon importiert wurden EC2, da dieselbe SHA-256-Hash-Funktion zur Berechnung des Fingerabdrucks verwendet wird.

Generieren eines Fingerabdrucks aus dem privaten Schlüssel

Generieren Sie mit einem der folgenden Befehle einen Fingerabdruck aus dem privaten Schlüssel auf Ihrem lokalen Computer.

Wenn Sie einen lokalen Windows-Computer verwenden, können Sie die folgenden Befehle mit dem Windows-Subsystem für Linux (WSL) ausführen. Installieren Sie WSL und eine Linux-Distribution mithilfe der Anleitung im Installationshandbuch für Linux unter Windows mit WSL. Mit dem in der Anleitung genannten Beispiel wird die Ubuntu-Distribution von Linux installiert, Sie können jedoch jede beliebige Distribution installieren. Sie werden zum Neustart Ihres Computers aufgefordert, damit die Änderungen wirksam werden.

- Wenn Sie das key pair mit Amazon erstellt haben EC2

  Verwenden Sie die OpenSSL-Tools, um einen Fingerabdruck zu generieren, wie in den folgenden Beispielen gezeigt.

  Für RSA-Schlüsselpaare:

```
openssl pkcs8 -in path_to_private_key -inform PEM -outform DER -topk8 -nocrypt |
 openssl sha1 -c
```

  (Linux-Instances) Für ED25519 Schlüsselpaare:

```
ssh-keygen -l -f path_to_private_key
```

- (Nur RSA-Schlüsselpaare) Wenn Sie den öffentlichen Schlüssel zu Amazon importiert haben EC2

  Sie können dieses Verfahren unabhängig davon befolgen, wie Sie das key pair erstellt haben, z. B. indem Sie ein Drittanbieter-Tool verwenden oder indem Sie einen neuen öffentlichen Schlüssel aus einem vorhandenen privaten Schlüssel generieren, der mit Amazon erstellt wurde. EC2

  Verwenden Sie die OpenSSL-Tools, um einen Fingerabdruck zu generieren, wie im folgenden Beispiel gezeigt.

  ```
  openssl rsa -in path_to_private_key -pubout -outform DER | openssl md5 -c
  ```

- Wenn Sie mit OpenSSH 7.8 oder höher ein OpenSSH-Schlüsselpaar erstellt und den öffentlichen Schlüssel zu Amazon importiert haben EC2

  Verwenden Sie ssh-keygen, um einen Fingerabdruck zu generieren, wie in den folgenden Beispielen gezeigt.

  Für RSA-Schlüsselpaare:

  ```
  ssh-keygen -ef path_to_private_key -m PEM | openssl rsa -RSAPublicKey_in -outform DER
   | openssl md5 -c
  ```

  (Linux-Instances) Für Schlüsselpaare: ED25519

  ```
  ssh-keygen -l -f path_to_private_key
  ```

EC2 Amazon-Sicherheitsgruppen für Ihre EC2 Instances

Eine Sicherheitsgruppe fungiert als virtuelle Firewall für Ihre EC2 Instances, um den ein- und ausgehenden Datenverkehr zu kontrollieren. Eingehende Regeln steuern den eingehenden Datenverkehr zu Ihrer Instance und ausgehende Regeln steuern den ausgehenden Datenverkehr von Ihrer Instance. Wenn Sie eine Instance starten, können Sie eine oder mehrere Sicherheitsgruppen angeben. Wenn Sie keine Sicherheitsgruppe angeben, EC2 verwendet Amazon die Standardsicherheitsgruppe für die VPC. Nach dem Start einer Instance können Sie deren Sicherheitsgruppen nicht mehr ändern.

Sicherheit ist eine gemeinsame Verantwortung zwischen Ihnen AWS und Ihnen. Weitere Informationen finden Sie unterSicherheit bei Amazon EC2. AWS stellt Sicherheitsgruppen als eines der Tools zum Schutz Ihrer Instances bereit. Sie müssen sie entsprechend Ihren Sicherheitsanforderungen konfigurieren. Wenn Sie Anforderungen haben, die von Sicherheitsgruppen nicht vollständig erfüllt werden, können Sie zusätzlich zur Verwendung von Sicherheitsgruppen eine eigene Firewall in jeder Ihrer Instances einrichten.

Preisgestaltung

Für die Nutzung von Sicherheitsgruppen fallen keine zusätzlichen Gebühren an.

Inhalt

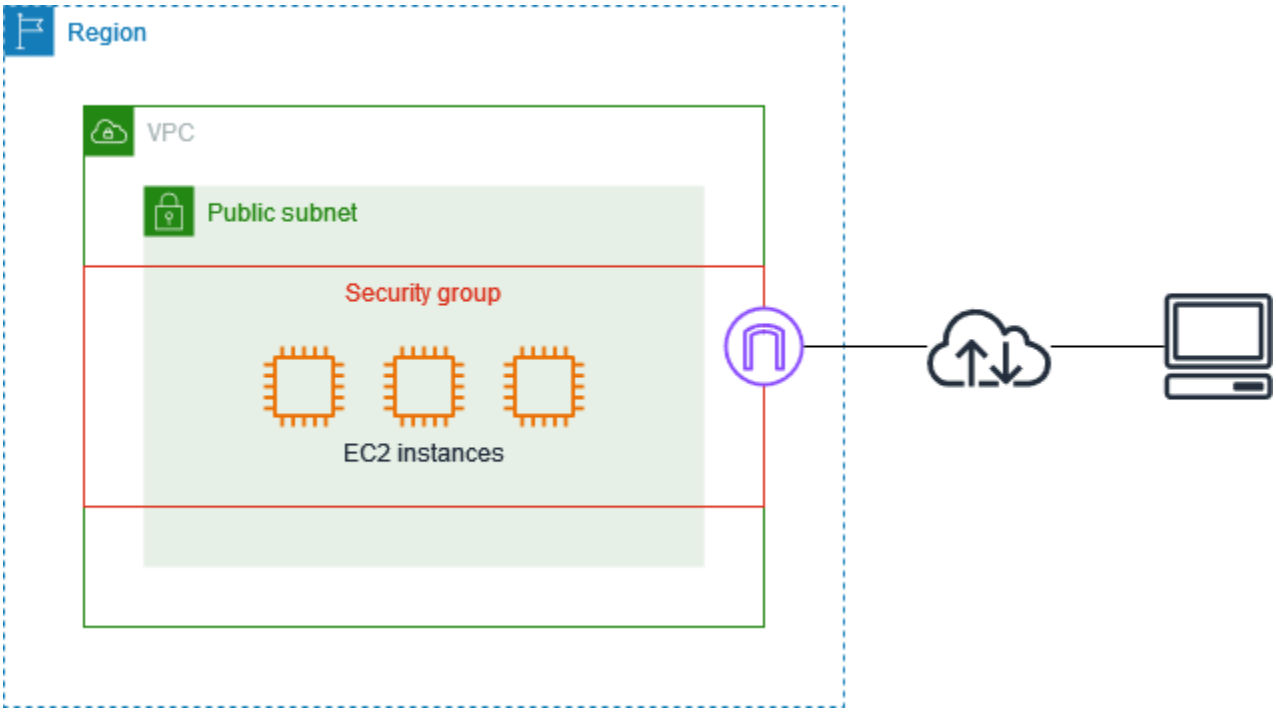
- Übersicht
- Erstellen Sie eine Sicherheitsgruppe für Ihre EC2 Amazon-Instance
- Ändern Sie die Sicherheitsgruppen für Ihre EC2 Amazon-Instance
- Löschen Sie eine EC2 Amazon-Sicherheitsgruppe
- Verbindungsverfolgung EC2 für Amazon-Sicherheitsgruppen
- Sicherheitsgruppenregeln für verschiedene Anwendungsfälle

Übersicht

Sie können jede Instance mehreren Sicherheitsgruppen zuordnen, und Sie können jede Sicherheitsgruppe mehreren Instances zuordnen. Dann fügen Sie jeder Sicherheitsgruppe Regeln hinzu, die den Datenaustausch mit den zugeordneten Instances gestatten. Sie können die Regeln für eine Sicherheitsgruppe jederzeit ändern. Neue und geänderte Regeln werden automatisch auf alle Instances angewendet, die der Sicherheitsgruppe zugeordnet sind. Wenn Amazon EC2 entscheidet, ob Datenverkehr eine Instance erreichen darf, werden alle Regeln aus allen Sicherheitsgruppen ausgewertet, die der Instance zugeordnet sind. Weitere Informationen finden Sie unter Sicherheitsgruppenregeln im Amazon-VPC-Benutzerhandbuch.

Das folgende Diagramm zeigt eine VPC mit einer Sicherheitsgruppe, einem Internet-Gateway und einem Subnetz. Das Subnetz enthält EC2 Instances. Die Sicherheitsgruppe ist mit dem Instances zugeordnet. Der einzige Datenverkehr, der die Instance erreicht, ist der Datenverkehr, der nach den Sicherheitsgruppenregeln zulässig ist. Wenn die Sicherheitsgruppe beispielsweise eine Regel enthält, die SSH-Datenverkehr von Ihrem Netzwerk zur Instance zulässt, können Sie sich mit der Instance von Ihrem Computer aus verbinden. Wenn die Sicherheitsgruppe eine Regel enthält, die den

gesamten Datenverkehr von den ihr zugewiesenen Ressourcen zulässt, kann jede Instance den von den anderen Instances gesendeten Datenverkehr empfangen.



Sicherheitsgruppen sind zustandsbehaftet — wenn Sie von Ihrer Instance eine Anforderung senden, wird der Antwortdatenverkehr für diese Anforderung zugelassen, unabhängig der für diese Sicherheitsgruppe geltenden Regeln für eingehenden Datenverkehr. Außerdem dürfen Antworten auf erlaubten eingehenden Datenverkehr unabhängig von den Regeln für ausgehenden Datenverkehr ablaufen. Weitere Informationen finden Sie unter Verfolgung von Verbindungen.

Erstellen Sie eine Sicherheitsgruppe für Ihre EC2 Amazon-Instance

Sicherheitsgruppen fungieren als Firewall für zugeordnet Instances. Sie steuern den ein- und ausgehenden Datenverkehr auf der Instance-Ebene. Sie können einer Sicherheitsgruppe Regeln hinzufügen, die es Ihnen ermöglichen, über SSH (Linux-Instances) oder RDP (Windows-Instances) eine Verbindung zu Ihrer Instance herzustellen. Sie können auch Regeln hinzufügen, die Client-Verkehr zulassen, z. B. HTTP- und HTTPS-Verkehr zu einem Webserver.

Sie können eine Sicherheitsgruppe einer Instance zuweisen, wenn Sie die Instance starten. Wenn Sie Regeln von verbundenen Sicherheitsgruppen hinzufügen oder entfernen, gelten diese Änderungen automatisch für alle Instances, denen Sie die Sicherheitsgruppe zugewiesen haben.

Nach dem Start einer Instance können Sie weitere Sicherheitsgruppen assoziieren. Weitere Informationen finden Sie unter Ändern Sie die Sicherheitsgruppen für Ihre EC2 Amazon-Instance.

Sie können Regeln für eine Sicherheitsgruppe für den ein- und ausgehenden Datenverkehr erstellen, wenn Sie eine Sicherheitsgruppe erstellen, oder Sie können sie zu einem späteren Zeitpunkt hinzufügen. Weitere Informationen finden Sie unter Sicherheitsgruppenregeln konfigurieren. Für Beispiele für Regeln, die Sie einer Sicherheitsgruppe hinzufügen können, siehe Sicherheitsgruppenregeln für verschiedene Anwendungsfälle.

Überlegungen

- Neue Sicherheitsgruppen starten mit nur einer Regel für ausgehenden Datenverkehr, die sämtlichen von der Ressource ausgehenden Datenverkehr zulässt. Sie müssen Regeln hinzufügen, um eingehenden Datenverkehr zuzulassen oder den ausgehenden Datenverkehr einzuschränken.
- Wenn Sie eine Quelle für eine Regel konfigurieren, die SSH- oder RDP-Zugriff auf Ihre Instances ermöglicht, sollten Sie keinen Zugriff von überall zulassen, da dies den Zugriff auf Ihre Instance von allen IP-Adressen im Internet aus ermöglichen würde. Dies ist zwar für kurze Zeit in einer Testumgebung akzeptabel, aber für Produktionsumgebungen sehr unsicher.
- Wenn es mehr als eine Regel für einen bestimmten Port gibt, EC2 wendet Amazon die toleranteste Regel an. Wenn Sie z. B. eine Regel haben, die den Zugriff auf den TCP-Port 22 (SSH) von der IP-Adresse 203.0.113.1 aus erlaubt, und eine weitere Regel, die den Zugriff auf den TCP-Port 22 von überall aus erlaubt, dann hat jeder Zugriff auf den TCP-Port 22.
- Sie können einer Instance mehrere Sicherheitsgruppen zuweisen. Daher kann eine Instance Hunderte von Regeln haben, die angewendet werden. Dies kann beim Zugriff auf die Instance zu Problemen führen. Wir empfehlen, dass Sie Ihre Regeln so weit wie möglich verdichten.
- Wenn Sie eine Sicherheitsgruppe als Quelle oder Ziel für eine Regel angeben, wirkt sich die Regel auf alle Instances aus, die der Sicherheitsgruppe zugeordnet sind. Eingehender Verkehr ist basierend auf den privaten IP-Adressen der Instances erlaubt, die der Quellsicherheitsgruppe zugeordnet sind (und nicht auf den öffentlichen IP- oder Elastic IP-Adressen). Weitere Informationen über IP-Adressen finden Sie unter IP-Adressierung von Amazon EC2-Instances.
- Amazon EC2 blockiert standardmäßig den Verkehr auf Port 25. Weitere Informationen finden Sie unter Einschränkung für E-Mails, die über Port 25 gesendet werden.

Console

So erstellen Sie eine Sicherheitsgruppe

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus.
4. Geben Sie einen beschreibenden Namen und eine kurze Beschreibung für die Sicherheitsgruppe ein. Sie können den Namen und die Beschreibung einer Sicherheitsgruppe nach der Erstellung nicht mehr ändern.
5. Wählen Sie für VPC die VPC aus, in der Sie Ihre EC2 Amazon-Instances ausführen werden.
6. (Optional) Um Regeln für eingehenden Datenverkehr hinzuzufügen, wählen Sie Eingehende Regeln aus. Wählen Sie für jede Regel Regel hinzufügen aus und geben Sie das Protokoll, den Port und die Quelle an. Um beispielsweise SSH-Verkehr zuzulassen, wählen Sie SSH als Typ und geben Sie die öffentliche IPv4 Adresse Ihres Computers oder Netzwerks als Quelle an.
7. (Optional) Um Regeln für ausgehenden Datenverkehr hinzuzufügen, wählen Sie Ausgehende Regeln aus. Wählen Sie für jede Regel Regel hinzufügen aus und geben Sie das Protokoll, den Port und das Ziel an. Andernfalls können Sie die Standardregel beibehalten, die den gesamten ausgehenden Datenverkehr zulässt.
8. (Optional) Um ein Tag hinzuzufügen, wählen Sie Add new tag (Neuen Tag hinzufügen) aus und geben Sie den Schlüssel und den Wert für den Tag ein.
9. Wählen Sie Sicherheitsgruppe erstellen aus.

AWS CLI

So erstellen Sie eine Sicherheitsgruppe

Verwenden Sie den folgenden create-security-group-Befehl.

```
aws ec2 create-security-group \
    --group-name my-security-group \
    --description "my security group" \
    --vpc-id vpc-1234567890abcdef0
```

Beispiele für das Hinzufügen von Regeln finden Sie unter the section called “Sicherheitsgruppenregeln konfigurieren”.

PowerShell

So erstellen Sie eine Sicherheitsgruppe

Verwenden Sie das cmdlet New-EC2SecurityGroup.

```
New-EC2SecurityGroup `
    -GroupName my-security-group `
    -Description "my security group" `
    -VpcId vpc-1234567890abcdef0
```

Beispiele für das Hinzufügen von Regeln finden Sie unter the section called “Sicherheitsgruppenregeln konfigurieren”.

Ändern Sie die Sicherheitsgruppen für Ihre EC2 Amazon-Instance

Sie können Sicherheitsgruppen für Ihre EC2 Amazon-Instances angeben, wenn Sie sie starten. Nach dem Start einer Instance können Sie deren Sicherheitsgruppen ändern oder entfernen. Sie können auch jederzeit Sicherheitsgruppenregeln für zugehörige Sicherheitsgruppen hinzufügen, entfernen oder bearbeiten.

Sicherheitsgruppen sind mit Netzwerkschnittstellen verknüpft. Durch das Hinzufügen oder Entfernen von Sicherheitsgruppen werden die Sicherheitsgruppen geändert, die mit der primären Netzwerkschnittstelle verknüpft sind. Sie können auch die Sicherheitsgruppen ändern, die mit irgendwelchen sekundären Netzwerkschnittstellen verknüpft sind. Weitere Informationen finden Sie unter Ändern der Netzwerkschnittstellen-Attribute.

Aufgaben

- Sicherheitsgruppen hinzufügen oder entfernen
- Sicherheitsgruppenregeln konfigurieren

Sicherheitsgruppen hinzufügen oder entfernen

Nach dem Start einer Instance können Sie Sicherheitsgruppen zur Liste der zugehörigen Sicherheitsgruppen hinzufügen oder von ihr entfernen. Wenn Sie mehrere Sicherheitsgruppen mit einer Instance verbinden, werden die Regeln jeder Sicherheitsgruppe effektiv zu einem einzigen Regelsatz zusammengeführt. Amazon EC2 verwendet dieses Regelwerk, um zu bestimmen, ob Datenverkehr zugelassen werden soll.

Voraussetzungen

- Die Instance muss sich im `running`- oder `stopped`-Status befinden.

Console

So ändern Sie die Sicherheitsgruppen für eine Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie Ihre Instance und wähle Sie dann Actions (Aktionen), Security (Sicherheit), Change security groups (Sicherheitsgruppen ändern) aus.
4. Wählen Sie für Associated security groups (Zugehörige Sicherheitsgruppen) eine Sicherheitsgruppe aus der Liste aus und klicken Sie auf Add security group (Sicherheitsgruppe hinzufügen).

   Um eine bereits zugeordnete Sicherheitsgruppe zu entfernen, wählen Remove (Entfernen) für diese Sicherheitsgruppe.
5. Wählen Sie Save aus.

AWS CLI

So ändern Sie die Sicherheitsgruppen für eine Instance

Verwenden Sie den folgenden modify-instance-attribute-Befehl.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --groups sg-1234567890abcdef0
```

PowerShell

So ändern Sie die Sicherheitsgruppen für eine Instance

Verwenden Sie das cmdlet Edit-EC2InstanceAttribute.

```
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -Group sg-1234567890abcdef0
```

Sicherheitsgruppenregeln konfigurieren

Nachdem Sie eine Sicherheitsgruppe erstellt haben, können Sie die zugehörigen Sicherheitsgruppenregeln hinzufügen, aktualisieren und löschen. Wenn Sie eine Regel hinzufügen, aktualisieren oder löschen, gilt die aktualisierte Regel automatisch für alle Ressourcen, die der Sicherheitsgruppe zugewiesen sind.

Für Beispiele für Regeln, die Sie einer Sicherheitsgruppe hinzufügen können, siehe Sicherheitsgruppenregeln für verschiedene Anwendungsfälle.

Erforderliche Berechtigungen

Stellen Sie zuerst sicher, dass Sie über die erforderlichen Berechtigungen verfügen. Weitere Informationen finden Sie unter Beispiel: Arbeiten mit Sicherheitsgruppen.

Protokolle und Ports

- Wenn Sie in der Konsole einen vordefinierten Typ auswählen, werden Protokoll und Portbereich für Sie angegeben. Um einen Portbereich einzugeben, müssen Sie einen der folgenden benutzerdefinierten Typen auswählen: Benutzerdefiniertes TCP oder Benutzerdefiniertes UDP.
- Mit dem AWS CLI können Sie mithilfe der `--port` Optionen `--protocol` und eine einzelne Regel mit einem einzigen Port hinzufügen. Um mehrere Regeln oder eine Regel mit einem Portbereich hinzuzufügen, verwenden Sie stattdessen die Option `--ip-permissions`.

Quellen und Ziele

- Mit der Konsole können Sie Folgendes als Quellen für Regeln für eingehenden Datenverkehr oder als Ziele für Regeln für ausgehenden Datenverkehr angeben.
  - Benutzerdefiniert — Ein IPv4 CIDR-Block, ein IPv6 CIDR-Block, eine Sicherheitsgruppe oder eine Präfixliste.
  - Anywhere- IPv4 — Der IPv4 0.0.0.0/0 CIDR-Block.
  - Anywhere- IPv6 — Der: :/0 CIDR-Block. IPv6
  - Meine IP — Die öffentliche IPv4 Adresse Ihres lokalen Computers.
- Mit der AWS CLI können Sie mithilfe der Option einen IPv4 CIDR-Block oder mithilfe der `--cidr` Option eine Sicherheitsgruppe angeben. `--source-group` Verwenden Sie die Option, um eine Präfixliste oder einen IPv6 CIDR-Block anzugeben. `--ip-permissions`

> **Warning**
>
> Wenn Sie eingehende Regeln für die Ports 22 (SSH) oder 3389 (RDP) hinzufügen, empfehlen wir Ihnen dringend, nur die spezifischen IP-Adressen oder Adressbereiche zuzulassen, die Zugriff auf Ihre Instances benötigen. Wenn Sie Anywhere- wählenIPv4, ermöglichen Sie Traffic von allen IPv4 Adressen, über das angegebene Protokoll auf Ihre Instances zuzugreifen. Wenn Sie Anywhere- wählenIPv6, erlauben Sie Traffic von allen IPv6 Adressen, über das angegebene Protokoll auf Ihre Instances zuzugreifen.

Console

Konfigurieren von Sicherheitsgruppenregeln

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.
3. Wählen Sie die Sicherheitsgruppe aus.
4. Wählen Sie unter Aktionen oder auf der Registerkarte Regeln für eingehenden Datenverkehr die Option Bearbeiten von Regeln für eingehenden Datenverkehr aus, um die Regeln für den eingehenden Datenverkehr zu bearbeiten.

   a. Um eine Regel hinzuzufügen, wählen Sie Regel hinzufügen aus und geben Sie den Typ, das Protokoll, den Port und die Quelle für die Regel ein.

      Wenn es sich beim Typ um TCP oder UDP handelt, müssen Sie den zuzulassenden Portbereich eingeben. Für ein benutzerdefiniertes ICMP müssen Sie den Namen des ICMP-Typs aus Protocol (Protokoll= und, falls zutreffend, den Codenamen aus Port range (Portbereich) wählen. Für einen anderen Typ werden das Protokoll und der Portbereich für Sie konfiguriert.

   b. Andern Sie das Protokoll, die Beschreibung und die Quelle nach Bedarf, um eine Regel zu aktualisieren. Sie können jedoch den Quellentyp nicht ändern. Wenn es sich bei der Quelle beispielsweise um einen IPv4 CIDR-Block handelt, können Sie keinen IPv6 CIDR-Block, keine Präfixliste oder keine Sicherheitsgruppe angeben.

   c. Klicken Sie auf die Schaltfläche Löschen, um eine Regel zu löschen.

5. Um die Regeln für den ausgehenden Datenverkehr zu bearbeiten, wählen Sie Regeln für ausgehenden Datenverkehr bearbeiten unter Aktionen oder auf der Registerkarte Regeln für ausgehenden Datenverkehr aus.

a. Um eine Regel hinzuzufügen, wählen Sie Regel hinzufügen aus und geben Sie den Typ, das Protokoll, den Port und das Ziel für die Regel ein. Sie können auch eine optionale Beschreibung eingeben.

   Wenn es sich beim Typ um TCP oder UDP handelt, müssen Sie den zuzulassenden Portbereich eingeben. Für ein benutzerdefiniertes ICMP müssen Sie den Namen des ICMP-Typs aus Protocol (Protokoll= und, falls zutreffend, den Codenamen aus Port range (Portbereich) wählen. Für einen anderen Typ werden das Protokoll und der Portbereich für Sie konfiguriert.

b. Andern Sie das Protokoll, die Beschreibung und die Quelle nach Bedarf, um eine Regel zu aktualisieren. Sie können jedoch den Quellentyp nicht ändern. Wenn es sich bei der Quelle beispielsweise um einen IPv4 CIDR-Block handelt, können Sie keinen IPv6 CIDR-Block, keine Präfixliste oder keine Sicherheitsgruppe angeben.

c. Klicken Sie auf die Schaltfläche Löschen, um eine Regel zu löschen.

6. Wählen Sie Save rules (Regeln speichern) aus.

AWS CLI

So fügen Sie Sicherheitsgruppenregeln hinzu

Verwenden Sie den authorize-security-group-ingressBefehl, um Regeln für eingehenden Datenverkehr hinzuzufügen. Das folgende Beispiel erlaubt eingehenden SSH-Datenverkehr aus den CIDR-Blöcken in der angegebenen Präfixliste.

```
aws ec2 authorize-security-group-ingress \
    --group-id sg-1234567890abcdef0 \
    --ip-permissions
 'IpProtocol=tcp,FromPort=22,ToPort=22,PrefixListIds=[{PrefixListId=pl-
f8a6439156EXAMPLE}]'
```

Verwenden Sie den authorize-security-group-egressBefehl, um Regeln für ausgehenden Datenverkehr hinzuzufügen. Im folgenden Beispiel wird ausgehender TCP-Datenverkehr auf Port 80 für Instances mit der angegebenen Sicherheitsgruppe zugelassen.

```
aws ec2 authorize-security-group-egress \
    --group-id sg-1234567890abcdef0 \
```

```
    --ip-permissions
 'IpProtocol=tcp,FromPort=80,ToPort=80,UserIdGroupPairs=[{GroupId=sg-0aad1c26bb6EXAMPLE}]'
```

So entfernen Sie Sicherheitsgruppenregeln

Verwenden Sie den folgenden revoke-security-group-ingressBefehl, um eine eingehende Regel zu entfernen.

```
aws ec2 revoke-security-group-egress \
    --group id sg-1234567890abcdef0 \
    --security-group-rule-ids sgr-09ed298024EXAMPLE
```

Verwenden Sie den folgenden revoke-security-group-egressBefehl, um eine ausgehende Regel zu entfernen.

```
aws ec2 revoke-security-group-ingress \
    --group id sg-1234567890abcdef0 \
    --security-group-rule-ids sgr-0352250c1aEXAMPLE
```

So modifizieren Sie Sicherheitsgruppenregeln

Verwenden Sie den Befehl modify-security-group-rules. Im folgenden Beispiel wird der IPv4 CIDR-Block der angegebenen Sicherheitsgruppenregel geändert.

```
aws ec2 modify-security-group-rules \
    --group id sg-1234567890abcdef0 \
    --security-group-rules
 'SecurityGroupRuleId=sgr-09ed298024EXAMPLE,SecurityGroupRule={IpProtocol=tcp,FromPort=80,To
```

PowerShell

So fügen Sie Sicherheitsgruppenregeln hinzu

Verwenden Sie das Grant-EC2SecurityGroupIngressCmdlet, um Regeln für eingehenden Datenverkehr hinzuzufügen. Das folgende Beispiel erlaubt eingehenden SSH-Datenverkehr aus den CIDR-Blöcken in der angegebenen Präfixliste.

```
$plid = New-Object -TypeName Amazon.EC2.Model.PrefixListId
$plid.Id = "pl-f8a6439156EXAMPLE"
Grant-EC2SecurityGroupIngress `
```

```
    -GroupId sg-1234567890abcdef0 `
    -IpPermission @{IpProtocol="tcp"; FromPort=22; ToPort=22; PrefixListIds=$plid}
```

Verwenden Sie das Grant-EC2SecurityGroupEgressCmdlet, um Regeln für ausgehenden Datenverkehr hinzuzufügen. Im folgenden Beispiel wird ausgehender TCP-Datenverkehr auf Port 80 für Instances mit der angegebenen Sicherheitsgruppe zugelassen.

```
$uigp = New-Object -TypeName Amazon.EC2.Model.UserIdGroupPair
$uigp.GroupId = "sg-0aad1c26bb6EXAMPLE"
Grant-EC2SecurityGroupEgress `
    -GroupId sg-1234567890abcdef0 `
    -IpPermission @{IpProtocol="tcp"; FromPort=80; ToPort=80; UserIdGroupPairs=
$uigp}
```

So entfernen Sie Sicherheitsgruppenregeln

Verwenden Sie das Revoke-EC2SecurityGroupIngressCmdlet, um Regeln für eingehenden Datenverkehr zu entfernen.

```
Revoke-EC2SecurityGroupIngress `
    -GroupId sg-1234567890abcdef0 `
    -SecurityGroupRuleId sgr-09ed298024EXAMPLE
```

Verwenden Sie das Revoke-EC2SecurityGroupEgressCmdlet, um Regeln für ausgehenden Datenverkehr zu entfernen.

```
Revoke-EC2SecurityGroupEgress `
    -GroupId sg-1234567890abcdef0 `
    -SecurityGroupRuleId sgr-0352250c1aEXAMPLE
```

So modifizieren Sie Sicherheitsgruppenregeln

Verwenden Sie das cmdlet Edit-EC2SecurityGroupRule. Im folgenden Beispiel wird der IPv4 CIDR-Block der angegebenen Sicherheitsgruppenregel geändert.

```
$sgrr = New-Object -TypeName Amazon.EC2.Model.SecurityGroupRuleRequest
$sgrr.IpProtocol = "tcp"
$sgrr.FromPort = 80
$sgrr.ToPort = 80
$sgrr.CidrIpv4 = "0.0.0.0/0"
```

```
$sgr = New-Object -TypeName Amazon.EC2.Model.SecurityGroupRuleUpdate
$sgr.SecurityGroupRuleId = "sgr-09ed298024EXAMPLE"
$sgr.SecurityGroupRule = $sgrr
Edit-EC2SecurityGroupRule  `
    -GroupId sg-1234567890abcdef0 `
    -SecurityGroupRule $sgr
```

Löschen Sie eine EC2 Amazon-Sicherheitsgruppe

Wenn Sie mit einer Sicherheitsgruppe fertig sind, die Sie für die Verwendung mit Ihren EC2 Amazon-Instances erstellt haben, können Sie sie löschen.

Voraussetzungen

- Die Sicherheitsgruppe kann keiner Instance oder Netzwerkschnittstelle zugeordnet werden.
- Die Sicherheitsgruppe kann nicht durch eine Regel in einer anderen Sicherheitsgruppe referenziert werden.

Console

Löschen Sie eine Sicherheitsgruppe wie folgt:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. (Optional) Gehen Sie wie folgt vor, um zu überprüfen, ob Ihre Sicherheitsgruppe keiner Instance zugeordnet ist:
   a. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.
   b. Kopieren Sie die ID der Sicherheitsgruppe, die gelöscht werden soll.
   c. Wählen Sie im Navigationsbereich Instances aus.
   d. Fügen Sie in der Suchleiste den Filter Sicherheitsgruppe IDs ist gleich hinzu und fügen Sie die ID der Sicherheitsgruppe ein. Wenn es keine Ergebnisse gibt, ist die Sicherheitsgruppe keiner Instance zugeordnet. Andernfalls müssen Sie die Zuordnung zur Sicherheitsgruppe trennen, bevor Sie sie löschen können.
3. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.
4. Wählen Sie die Sicherheitsgruppe und dann Aktionen, Sicherheitsgruppe löschen aus.
5. Wenn Sie mehr als eine Sicherheitsgruppe ausgewählt haben, werden Sie zur Bestätigung aufgefordert. Wenn einige der Sicherheitsgruppen nicht gelöscht werden können, wird der

Status der einzelnen Sicherheitsgruppen angezeigt, der angibt, ob sie gelöscht werden. Geben Sie Löschen ein, um den Löschvorgang zu bestätigen.

6. Wählen Sie Löschen aus.

AWS CLI

Löschen Sie eine Sicherheitsgruppe wie folgt:

Verwenden Sie den folgenden delete-security-group-Befehl.

```
aws ec2 delete-security-group --group-id sg-1234567890abcdef0
```

PowerShell

Löschen Sie eine Sicherheitsgruppe wie folgt:

Verwenden Sie das cmdlet Remove-EC2SecurityGroup.

```
Remove-EC2SecurityGroup -GroupId sg-1234567890abcdef0
```

Verbindungsverfolgung EC2 für Amazon-Sicherheitsgruppen

Ihre Sicherheitsgruppen verwenden die Verbindungsverfolgung zur Nachverfolgung des Datenverkehrs zu und von der Instance. Regeln werden auf der Grundlage des Verbindungszustands des Datenverkehrs angewendet, um zu ermitteln, ob der Datenverkehr zulässig ist oder nicht. Bei diesem Ansatz sind Sicherheitsgruppen zustandsbehaftet. Das bedeutet, dass Antworten auf eingehenden Verkehr unabhängig von den Regeln für ausgehende Sicherheitsgruppen aus der Instance fließen dürfen und umgekehrt.

Angenommen, Sie initiieren einen Befehl wie „netcat“ oder ähnliches für Ihre Instances von Ihrem Heimcomputer aus und Ihre eingehenden Sicherheitsgruppenregeln lassen ICMP-Datenverkehr zu. Informationen über die Verbindung (einschließlich der Port-Informationen) werden verfolgt. Antwort-Datenverkehr von der Instance für den -Befehl wird nicht als neue Anfrage verfolgt, sondern als eingerichtete Verbindung; dieser Datenverkehr kann die Instance verlassen, selbst wenn Ihre ausgehenden Sicherheitsgruppenregeln ausgehenden ICMP-Datenverkehr beschränken.

Für andere Protokolle als TCP, UDP oder ICMP werden nur die IP-Adresse und die Protokollnummer verfolgt. Wenn Ihre Instance Datenverkehr an einen anderen Host sendet und der Host innerhalb

von 600 Sekunden dieselbe Art von Datenverkehr an Ihre Instance sendet, akzeptiert die Sicherheitsgruppe für Ihre Instance diesen unabhängig von den Sicherheitsgruppen-Regeln für eingehenden Datenverkehr. Die Sicherheitsgruppe akzeptiert ihn, da er als Antwort-Datenverkehr für den ursprünglichen Datenverkehr angesehen wird.

Wenn Sie eine Sicherheitsgruppenregel ändern, werden ihre nachverfolgten Verbindungen nicht sofort unterbrochen. Die Sicherheitsgruppe lässt Pakete weiterhin zu, bis bei bestehenden Verbindungen eine Zeitüberschreitung (Timeout) auftritt. Um sicherzustellen, dass Datenverkehr sofort unterbrochen wird oder der gesamte Datenverkehr unabhängig vom Nachverfolgungsstatus den Firewall-Regeln unterliegt, können Sie eine Netzwerk-ACL für Ihr Subnetz verwenden. Netzwerke ACLs sind zustandslos und lassen daher nicht automatisch Antwortverkehr zu. Das Hinzufügen einer Netzwerk-ACL, die Datenverkehr in beide Richtungen blockiert, trennt vorhandene Verbindungen. Weitere Informationen finden Sie unter Netzwerk ACLs im Amazon VPC-Benutzerhandbuch.

> **Note**
>
> Sicherheitsgruppen haben keine Auswirkung auf den DNS-Verkehr zum oder vom Route 53 Resolver, der manchmal auch als „VPC+2-IP-Adresse“ bezeichnet wird (siehe Was ist Amazon Route 53 Resolver? im Amazon Route 53 Developer Guide) oder im 'AmazonProvidedDNS' (siehe Arbeiten mit DHCP-Optionssätzen im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch). Wenn Sie DNS-Anfragen über den Route 53 Resolver filtern möchten, können Sie die Route-53-Resolver-DNS-Firewall aktivieren (Informationen unter Route-53-Resolver-DNS-Firewall im Amazon-Route-53-Entwicklerhandbuch).

Unverfolgte Verbindungen

Nicht alle Datenverkehrsflüsse werden verfolgt. Wenn eine Sicherheitsgruppenregel TCP- oder UDP-Abläufe für den gesamten Datenverkehr (0.0.0.0/0 oder ::/0) zulässt und es eine entsprechende Regel in der anderen Richtung gibt, die den gesamten Antwort-Datenverkehr (0.0.0.0/0 oder ::/0) für jeden Port (0-65535) zulässt, dann wird dieser Datenverkehrsablauf nicht verfolgt, es sei denn, er ist Teil einer automatisch verfolgten Verbindung. Der Antwort-Datenverkehr für einen nicht nachverfolgten Fluss wird anhand der Regel für ein- oder ausgehenden Datenverkehr zugelassen, die den Antwort-Datenverkehr erlaubt, und nicht anhand von Nachverfolgungsinformationen.

Ein nicht verfolgter Datenverkehrsfluss wird sofort unterbrochen, wenn die Regel, die ihn ermöglicht, entfernt oder modifiziert wird. Wenn Sie z. B. eine offene (0.0.0.0/0) ausgehende Regel haben und eine Regel entfernen, die den gesamten (0.0.0.0/0) eingehenden SSH-Verkehr (TCP-Port 22) zur

Instance zulässt (oder sie so ändern, dass die Verbindung nicht mehr zulässig wäre), werden Ihre bestehenden SSH-Verbindungen zur Instance sofort gelöscht. Die Verbindung wurde zuvor nicht nachverfolgt, sodass die Änderung die Verbindung unterbricht. Wenn Sie dagegen eine restriktivere Regel für eingehende Verbindungen verwenden, die zunächst eine SSH-Verbindung zulässt (was bedeutet, dass die Verbindung nachverfolgt wurde), diese Regel aber so ändern, dass keine neuen Verbindungen von der Adresse des aktuellen SSH-Clients mehr zugelassen werden, wird die bestehende SSH-Verbindung nicht unterbrochen, weil sie nachverfolgt wird.

Automatisch nachverfolgte Verbindungen

Über die folgenden Optionen hergestellte Verbindungen werden automatisch nachverfolgt, auch wenn die Konfiguration der Sicherheitsgruppe keine Nachverfolgung erfordert:

- Internet-Gateways nur für ausgehenden Datenverkehr
- Accelerators von Global Accelerator
- NAT gateways (NAT-Gateways)
- Firewall-Endpunkte von Network Firewall
- Network Load Balancers
- AWS PrivateLink (Schnittstelle VPC-Endpunkte)
- AWS Lambda (Elastische Hyperplane-Netzwerkschnittstellen)
- DynamoDB-Gateway-Endpunkte – Jede Verbindung zu DynamoDB verbraucht 2 Conntrack-Einträge.

Berechtigungen für die Verfolgung von Verbindungen

Amazon EC2 definiert die maximale Anzahl von Verbindungen, die pro Instance verfolgt werden können. Nach Erreichen des Maximums werden alle gesendeten oder empfangenen Pakete verworfen, da keine neue Verbindung hergestellt werden kann. In diesem Fall können Anwendungen, die Pakete senden und empfangen, nicht ordnungsgemäß kommunizieren. Verwenden Sie die `conntrack_allowance_available`-Netzwerkleistungsmetrik, um die Anzahl der nachverfolgten Verbindungen zu bestimmen, die für diesen Instance-Typ noch verfügbar sind.

Um festzustellen, ob Pakete verworfen wurden, weil der Netzwerkverkehr für Ihre Instance die maximale Anzahl der nachverfolgbaren Verbindungen überschritten hat, verwenden Sie die `conntrack_allowance_exceeded`-Netzwerkleistungsmetrik. Weitere Informationen finden Sie unter Netzwerkleistung für ENA-Einstellungen auf Ihrer EC2-Instance überwachen.

Wenn Sie bei ELB die maximale Anzahl von Verbindungen überschreiten, die pro Instance verfolgt werden können, empfehlen wir, entweder die Anzahl der beim Load Balancer registrierten Instances oder die Größe der beim Load Balancer registrierten Instances zu skalieren.

Überöegungen zu Leistungsaspekten der Verfolgung

Asymmetrisches Routing, bei dem der Datenverkehr über eine Netzwerkschnittstelle in eine Instance eingeht und über eine andere Netzwerkschnittstelle wieder austritt, kann die Spitzenleistung verringern, die eine Instance erzielen kann, wenn Datenflüsse nachverfolgt werden.

Um die Spitzenleistung aufrechtzuerhalten, wenn die Verbindungsverfolgung für Ihre Sicherheitsgruppen aktiviert ist, empfehlen wir die folgende Konfiguration:

- Vermeiden Sie nach Möglichkeit asymmetrische Routing-Topologien.
- Verwenden Sie das Netzwerk, anstatt Sicherheitsgruppen für die Filterung zu verwenden. ACLs
- Wenn Sie Sicherheitsgruppen mit Verbindungsverfolgung verwenden müssen, konfigurieren Sie das kürzeste mögliche Timeout für die Verbindungsverfolgung im Leerlauf. Weitere Informationen zum Timeout der Verfolgung von Verbindungen im Leerlauf finden Sie im folgenden Abschnitt.

Weitere Informationen zur Leistungsoptimierung des Nitro-Systems finden Sie unter Überlegungen zum Nitro-System für die Leistungsoptimierung.

Timeout für die Nachverfolgung von Leerlaufverbindungen

Die Sicherheitsgruppe verfolgt jede bestehende Verbindung nach, um sicherzustellen, dass Rückpakete wie erwartet übertragen werden. Es gibt eine maximale Anzahl von Verbindungen, die pro Instance verfolgt werden können. Im Leerlauf befindliche Verbindungen können zur Erschöpfung der Kapazität der Verbindungsnachverfolgung führen und zur Folge haben, dass Verbindungen nicht nachverfolgt und Pakete verworfen werden. Sie können das Timeout für die Nachverfolgung von Leerlaufverbindungen für eine Elastic-Network-Schnittstelle festlegen.

> **Note**
>
> Dieses Feature ist nur für Nitro-basierte Instances verfügbar.

Es gibt drei konfigurierbare Timeouts:

- Timeout für bestehende TCP-Verbindungen: Timeout (in Sekunden) für bestehende TCP-Verbindungen im Leerlauf.
  - Min: `60` Sekunden
  - Max: `432000` Sekunden
  - Standard: `350` Sekunden für Nitrov6-Instance-Typen, ausgenommen P6e-00. GB2 Und `432000` Sekunden für andere Instance-Typen, einschließlich P6e-00. GB2
  - Empfohlen: Weniger als `432000` Sekunden.
- UDP-Timeout: Timeout (in Sekunden) für UDP-Datenflüsse im Leerlauf, bei denen Datenverkehr nur in eine Richtung oder nur in einer einzelnen Anforderung-Antwort-Transaktion übermittelt wurde.
  - Min: `30` Sekunden
  - Max: `60` Sekunden
  - Standardwert: `30` Sekunden
- UDP-Stream-Timeout: Timeout (in Sekunden) für UDP-Datenflüsse im Leerlauf, die als Streams klassifiziert sind, bei denen mehr als eine Anforderung-Antwort-Transaktion stattgefunden hat.
  - Min: `60` Sekunden
  - Max: `180` Sekunden
  - Standardwert: `180` Sekunden

In folgenden Fällen empfiehlt es sich möglicherweise, die Standard-Timeouts anzupassen:

- Wenn Sie verfolgte Verbindungen mithilfe von EC2 Amazon-Netzwerkleistungsmetriken überwachen, können Sie mit den Kennzahlen conntrack_allowance_exceeded und conntrack_allowance_available verworfene Pakete und die nachverfolgte Verbindungsauslastung überwachen, um die EC2 Instance-Kapazität proaktiv mit Scale-Up- oder Out-Aktionen zu verwalten, um den Bedarf an Netzwerkverbindungen zu decken, bevor Pakete verworfen werden. Wenn Sie feststellen, dass conntrack_allowance_exceeded auf Ihren EC2 Instances ausfällt, können Sie davon profitieren, ein niedrigeres TCP-Timeout festzulegen, um veraltete TCP/UDP Sitzungen zu berücksichtigen, die auf falsche Clients oder Netzwerk-Middleboxen zurückzuführen sind.
- In der Regel haben Load Balancer oder Firewalls ein TCP-Etabliertes Leerlauf-Timeout im Bereich von 60 bis 90 Minuten. Wenn Sie Workloads ausführen, von denen erwartet wird, dass sie eine sehr hohe Anzahl von Verbindungen (mehr als 100.000) von Appliances wie Netzwerk-

Firewalls verarbeiten, empfiehlt es sich, ein ähnliches Timeout für eine Netzwerkschnittstelle zu konfigurieren. EC2

- Wenn Sie einen Workload ausführen, der eine asymmetrische Routing-Topologie verwendet, empfehlen wir Ihnen, ein TCP-Etabliertes Leerlaufzeitlimit von 60 Sekunden zu konfigurieren.
- Wenn Sie Workloads mit einer hohen Anzahl von Verbindungen wie DNS, SIP, SNMP, Syslog, Radius und andere Dienste ausführen, die hauptsächlich UDP zur Bearbeitung von Anfragen verwenden, bietet das Setzen des UDP-Stream-Timeouts auf 60 Sekunden eine höhere scale/performance Kapazität und verhindert Grauausfälle.
- Bei TCP/UDP Verbindungen über Network Load Balancer werden alle Verbindungen nachverfolgt. Der Wert des Leerlauf-Timeouts für TCP-Datenflüsse beträgt 350 Sekunden. Für UDP-Datenflüsse beträgt er 120 Sekunden. Er unterscheidet sich somit von den Timeout-Werten auf Schnittstellenebene. Es empfiehlt sich gegebenenfalls, Timeouts auf Netzwerkschnittstellen-Ebene zu konfigurieren, um beim Timeout mehr Flexibilität zu haben als mit den Standardwerten für den Load Balancer.

Die Timeouts für die Verbindungsnachverfolgung können bei folgenden Tätigkeiten konfiguriert werden:

- Erstellen einer Netzwerkschnittstelle
- Ändern der Netzwerkschnittstellen-Attribute
- Starten Sie eine Instanz EC2
- Erstellen Sie eine Vorlage für den EC2 Instanzstart

Beispiel

Im folgenden Beispiel hat die Sicherheitsgruppe Regeln für eingehenden Verkehr, die TCP- und ICMP-Datenverkehr zulassen, und Regeln für ausgehenden Verkehr, die allen ausgehenden Datenverkehr zulassen.

Eingehend

Protokolltyp	Port-Nummer	Quelle
TCP	22 (SSH)	203.0.113.1/32
TCP	80 (HTTP)	0.0.0.0/0

Protokolltyp	Port-Nummer	Quelle
TCP	80 (HTTP)	::/0
ICMP	Alle	0.0.0.0/0

Ausgehend

Protokolltyp	Port-Nummer	Ziel
Alle	Alle	0.0.0.0/0
Alle	Alle	::/0

Bei einer direkten Netzwerkverbindung zur Instance oder Netzwerkschnittstelle sieht das Nachverfolgungsverhalten wie folgt aus:

- Ein- und ausgehender TCP-Datenverkehr auf Port 22 (SSH) wird nachverfolgt, da die Regel für eingehenden Verkehr nur Datenverkehr von 203.0.113.1/32 und nicht von allen IP-Adressen (0.0.0.0/0) zulässt.
- Ein- und ausgehender TCP-Datenverkehr auf Port 80 (HTTP) wird nicht nachverfolgt, da die Regeln für ein- und ausgehenden Verkehr Datenverkehr von allen IP-Adressen zulassen.
- ICMP-Datenverkehr wird immer nachverfolgt.

Wenn Sie die Regel für ausgehenden IPv4 Datenverkehr entfernen, wird der gesamte eingehende und ausgehende IPv4 Verkehr verfolgt, einschließlich des Datenverkehrs auf Port 80 (HTTP). Das Gleiche gilt für den IPv6 Verkehr, wenn Sie die ausgehende Regel für den Datenverkehr entfernen. IPv6

Sicherheitsgruppenregeln für verschiedene Anwendungsfälle

Sie können eine Sicherheitsgruppe erstellen und dieser Regeln hinzufügen, die die Rolle der Instance reflektieren, mit der die Sicherheitsgruppe verbunden ist. Eine Instance, die als Webserver konfiguriert ist, benötigt beispielsweise Sicherheitsgruppenregeln, die eingehenden HTTP- und HTTPS-Zugriff zulassen. Ebenso benötigt eine Datenbank-Instance Regeln, die den Zugriff für den Datenbanktyp zulassen, wie z.B. den Zugriff über Port 3306 für MySQL.

Es folgen einige Beispiele für die Arten von Regeln, die Sie für bestimmte Zugriffsarten zu Sicherheitsgruppen hinzufügen können.

Beispiele

- Webserverregeln
- Datenbankserverregeln
- Regeln für die Verbindung mit Instances von Ihrem Computer aus
- Regeln für die Verbindung mit Instances von einer Instance mit der gleichen Sicherheitsgruppe aus
- Regeln für Ping/ICMP
- DNS-Server-Regeln
- Amazon EFS-Regeln
- ELB-Regeln

Anweisungen finden Sie unter Eine Sicherheitsgruppe erstellen und the section called “Sicherheitsgruppenregeln konfigurieren”.

Webserverregeln

Die folgenden eingehenden Regeln erlauben den HTTP- und HTTPS-Zugriff von jeder IP-Adresse aus. Wenn Ihre VPC für aktiviert ist, können Sie Regeln hinzufügen IPv6, um den eingehenden HTTP- und HTTPS-Verkehr von IPv6 Adressen zu kontrollieren.

Protokolltyp	Protokoll nummer	Port	Quell-IP	Hinweise
TCP	6	80 (HTTP)	0.0.0.0/0	Ermöglicht eingehenden HTTP-Zugriff von einer beliebigen Adresse IPv4
TCP	6	443 (HTTPS)	0.0.0.0/0	Ermöglicht eingehenden HTTPS-Zugriff von einer beliebigen Adresse IPv4
TCP	6	80 (HTTP)	::/0	Ermöglicht eingehenden HTTP-Zugriff von einer beliebigen Adresse IPv6

Protokolltyp	Protokoll nummer	Port	Quell-IP	Hinweise
TCP	6	443 (HTTPS)	::/0	Ermöglicht eingehenden HTTPS-Zugriff von einer beliebigen Adresse IPv6

Datenbankserverregeln

Die folgenden eingehenden Regeln sind Beispiele für Regeln, die Sie für den Datenbankzugriff hinzufügen können, je nachdem, auf welcher Art von Datenbank Ihre Instance ausgeführt wird. Weitere Informationen zu Amazon RDS-Instances finden Sie im Amazon RDS-Benutzerhandbuch.

geben Sie für die Quell-IP eine der folgenden Optionen an:

- Eine bestimmte IP-Adresse oder ein Bereich von IP-Adressen (in CIDR-Block-Notation) in Ihrem On-Premises-Netzwerk
- Eine Sicherheitsgruppen-ID für eine Gruppe von Instances, die auf die Datenbank zugreifen.

Protokolltyp	Protokollnummer	Port	Hinweise
TCP	6	1433 (MS SQL)	Der Standardport für den Zugriff auf eine Microsoft SQL Server-Datenbank, beispielsweise, auf einer Amazon RDS-Instance
TCP	6	3306 (MYSQL/Aurora)	Der Standardport für den Zugriff auf eine MySQL- oder Aurora-Datenbank, beispielsweise, auf einer Amazon RDS-Instance
TCP	6	5439 (Redshift)	Der Standardport für den zugriff auf eine Amazon Redshift-Cluster-Datenbank
TCP	6	5432 (PostgreSQL)	Der Standardport für den Zugriff auf eine PostgreSQL-Datenbank,

Protokolltyp	Protokollnummer	Port	Hinweise
			beispielsweise, auf einer Amazon RDS-Instance
TCP	6	1521 (Oracle)	Der Standardport für den Zugriff auf eine Oracle-Datenbank, beispielsweise, auf einer Amazon RDS-Instance

Sie können optional den ausgehenden Verkehr von Ihren Datenbankservern einschränken. Sie könnten zum Beispiel den Zugriff auf das Internet für Softwareupdates erlauben, aber alle anderen Arten des Datenverkehrs einschränken. Sie müssen zuerst die standardmäßige ausgehende Regel entfernen, die allen ausgehenden Datenverkehr zulässt.

Protokolltyp	Protokollnummer	Port	Ziel-IP	Hinweise
TCP	6	80 (HTTP)	0.0.0.0/0	Ermöglicht ausgehenden HTTP-Zugriff auf eine beliebige Adresse IPv4
TCP	6	443 (HTTPS)	0.0.0.0/0	Ermöglicht ausgehenden HTTPS-Zugriff auf eine beliebige Adresse IPv4
TCP	6	80 (HTTP)	::/0	(Nur VPC IPv6 aktiviert) Erlaubt ausgehenden HTTP-Zugriff auf jede Adresse IPv6
TCP	6	443 (HTTPS)	::/0	(Nur VPC IPv6 aktiviert) Ermöglicht ausgehenden HTTPS-Zugriff auf jede Adresse IPv6

Regeln für die Verbindung mit Instances von Ihrem Computer aus

Um Ihre Instance zu verbinden, muss Ihre Sicherheitsgruppe über eingehende Regeln verfügen, die den SSH-Zugriff (für Linux-Instances) oder den RDP-Zugriff (für Windows-Instances) erlauben.

Protokolltyp	Protokollnummer	Port	Quell-IP
TCP	6	22 (SSH)	Die öffentliche IPv4 Adresse Ihres Computers oder ein Bereich von IP-Adressen in Ihrem lokalen Netzwerk. Wenn Ihre VPC für aktiviert ist IPv6 und Ihre Instance eine IPv6 Adresse hat, können Sie eine IPv6 Adresse oder einen Bereich eingeben.
TCP	6	3389 (RDP)	Die öffentliche IPv4 Adresse Ihres Computers oder ein Bereich von IP-Adressen in Ihrem lokalen Netzwerk. Wenn Ihre VPC für aktiviert ist IPv6 und Ihre Instance eine IPv6 Adresse hat, können Sie eine IPv6 Adresse oder einen Bereich eingeben.

Regeln für die Verbindung mit Instances von einer Instance mit der gleichen Sicherheitsgruppe aus

Um zuzulassen, dass Instances, die mit derselben Sicherheitsgruppe verbunden sind, miteinander kommunizieren, müssen Sie eine ausdrückliche Regel dafür hinzufügen.

> **Note**
>
> Wenn Sie Routen konfigurieren, um den Datenverkehr zwischen zwei Instances in unterschiedlichen Subnetzen über eine Middlebox-Appliance weiterzuleiten, müssen Sie sicherstellen, dass die Sicherheitsgruppen für beide Instances den Datenverkehr zwischen den Instances zulassen. Die Sicherheitsgruppe für jede Instance muss die private IP-Adresse der anderen Instance oder den CIDR-Bereich des Subnetzes, das die andere Instance

enthält, als Quelle referenzieren. Wenn Sie die Sicherheitsgruppe der anderen Instance als Quelle referenzieren, wird dadurch kein Datenverkehr zwischen den Instances möglich.

Die folgende Tabelle beschreibt die eingehende Regel für eine Sicherheitsgruppe, die zugehörigen Instances erlaubt, miteinander zu kommunizieren. Die Regel lässt alle Arten von Datenverkehr zu.

Protokolltyp	Protokollnummer	Ports	Quell-IP
-1 (All)	-1 (All)	-1 (All)	Die ID der Sicherheitsgruppe oder der CIDR-Bereich des Subnetzes , das die andere Instance enthält (siehe Hinweis).

Regeln für Ping/ICMP

Der ping-Befehl ist eine Art von ICMP-Datenverkehr. Um Ihre Instance anzupingen, müssen Sie eine der folgenden ICMP-Regeln für eingehenden Datenverkehr hinzufügen.

Typ	Protokoll	Quelle		
Benutzerd efiniertes ICMP - IPv4	Echo-Anfo rderung	Die öffentliche IPv4 Adresse Ihres Computers , eine bestimmte IPv4 Adresse IPv4 oder eine IPv6 Oder-Adre sse von überall.		
Alles ICMP - IPv4	IPv4 ICMP (1)	Die öffentliche IPv4 Adresse Ihres Computers , eine bestimmte IPv4 Adresse IPv4 oder eine		

Typ	Protokoll	Quelle		
		IPv6 Oder-Adresse von überall.		

Um den ping6 Befehl zum Pingen der IPv6 Adresse für Ihre Instance zu verwenden, müssen Sie die folgende ICMPv6 Regel für eingehenden Datenverkehr hinzufügen.

Typ	Protokoll	Quelle		
Alles ICMP - IPv6	IPv6 ICMP (58)	Die IPv6 Adresse Ihres Computers, eine bestimmte IPv4 Adresse IPv4 oder eine IPv6 Oder-Adresse von überall.		

DNS-Server-Regeln

Wenn Sie Ihre EC2 Instanz als DNS-Server eingerichtet haben, müssen Sie sicherstellen, dass TCP- und UDP-Verkehr Ihren DNS-Server über Port 53 erreichen kann.

geben Sie für die Quell-IP eine der folgenden Optionen an:

- Eine IP-Adresse oder ein Bereich von IP-Adressen (in CIDR-Block-Notation) in einem Netzwerk
- Eine Sicherheitsgruppen-ID für eine Gruppe von Instances in Ihrem Netzwerk, die Zugriff auf den DNS-Server benötigen

Protokolltyp	Protokollnummer	Port
TCP	6	53
UDP	17	53

Amazon EFS-Regeln

Wenn Sie ein Amazon EFS-Dateisystem mit Ihren EC2 Amazon-Instances verwenden, muss die Sicherheitsgruppe, die Sie Ihren Amazon EFS-Mount-Zielen zuordnen, Datenverkehr über das NFS-Protokoll zulassen.

Protokolltyp	Protokollnummer	Ports	Quell-IP	Hinweise
TCP	6	2049 (NFS)	Die ID der Sicherheitsgruppe	Erlaubt den eingehenden NFS-Zugriff von Ressourcen (einschließlich des Mountingziels), die mit dieser Sicherheitsgruppe verbunden sind

Um ein Amazon EFS-Dateisystem auf Ihrer EC2 Amazon-Instance zu mounten, müssen Sie eine Verbindung zu Ihrer Instance herstellen. Daher muss die mit Ihrer Instance verbundene Sicherheitsgruppe über Regeln verfügen, die den eingehenden SSH-Datenverkehr von ihrem lokalen Computer oder lokalen Netzwerk aus zulassen.

Protokolltyp	Protokollnummer	Ports	Quell-IP	Hinweise
TCP	6	22 (SSH)	Der IP-Adressbereich Ihres lokalen Computers bzw. der Bereich von IP-Adressen (in CIDR-Block-Notation) für Ihr Netzwerk.	Lässt eingehenden SSH-Zugriff von Ihrem lokalen Computer zu.

ELB-Regeln

Wenn Sie Ihre EC2 Instances bei einem Load Balancer registrieren, muss die mit Ihrem Load Balancer verknüpfte Sicherheitsgruppe die Kommunikation mit den Instances zulassen. Weitere Informationen finden Sie in der ELB-Dokumentation im Folgenden.

- Sicherheitsgruppen für Ihren Application Load Balancer
- Sicherheitsgruppen für Ihren Network Load Balancer
- Konfigurieren von Sicherheitsgruppen für Ihren Classic Load Balancer

NitroTPM für Amazon-Instances EC2

Nitro Trusted Platform Module (NitroTPM) ist ein virtuelles Gerät von AWS -Nitro-System und entspricht TPM 2.0. Es speichert sicher Artefakte (etwa Passwörter, Zertifikate oder Verschlüsselungsschlüssel), die zur Authentifizierung der Instance verwendet werden. NitroTPM kann Schlüssel generieren und sie für kryptografische Funktionen nutzen (etwa Hashing, Signieren, Verschlüsselung und Entschlüsselung).

NitroTPM bietet Measured Boot, einen Prozess, bei dem der Bootloader und das Betriebssystem kryptografische Hashes für jede Start-Binärdatei erstellen und diese mit den vorherigen Werten in den internen NitroTPM-Plattformkonfigurationsregistern () kombinieren. PCRs Mit „Measured Boot“ können Sie signierte PCR-Werte von NitroTPM abrufen und diese verwenden, um gegenüber Remote-Entitäten die Integrität der Bootsoftware der Instance zu beweisen. Dieser Vorgang wird als Remote-Bescheinigung bezeichnet.

Mit NitroTPM können Schlüssel und Secrets mit einem bestimmten PCR-Wert gekennzeichnet werden. Wenn sich der Wert des PCRs und damit die Instance-Integrität ändert, kann dadurch nicht mehr auf die Schlüssel und Secrets zugegriffen werden. Diese besondere Form des bedingten Zugangs wird als Sealiung und Unsealing (etwa: Versiegeln und Entsiegeln) bezeichnet. Betriebssystemtechnologien wie können NitroTPM verwenden BitLocker, um einen Laufwerks-Entschlüsselungsschlüssel zu versiegeln, sodass das Laufwerk nur dann entschlüsselt werden kann, wenn das Betriebssystem korrekt gestartet wurde und sich in einem zweifelsfrei funktionierenden Zustand befindet.

Um NitroTPM verwenden zu können, müssen Sie ein Amazon Machine Image (AMI) auswählen, das für Unterstützung von NitroTPM konfiguriert wurde, und dann das AMI zum Starten einer Nitro-basierten Instance verwenden. Sie können eines der AMIs vorgefertigten Produkte von Amazon auswählen oder selbst eines erstellen.

Preisgestaltung

Für die Nutzung von NitroTPM fallen keine zusätzlichen Kosten an. Sie bezahlen nur für die zugrundeliegenden Ressourcen, die Sie nutzen.

Inhalt

- Anforderungen für die Verwendung von NitroTPM mit Amazon-Instances EC2
- Linux-AMIs für NitroTPM aktivieren
- Überprüfen, ob ein AMI für NitroTPM aktiviert ist
- NitroTPM auf einer Amazon-Instance aktivieren oder beenden EC2
- Stellen Sie sicher, dass eine EC2 Amazon-Instance für NitroTPM aktiviert ist
- Rufen Sie den öffentlichen Bestätigungsschlüssel für eine Instanz EC2 ab

Anforderungen für die Verwendung von NitroTPM mit Amazon-Instances EC2

Um eine Instance mit aktiviertem NitroTPM zu starten, müssen Sie die folgenden Anforderungen erfüllen.

Themen

- AMIs
- Instance-Typen
- Überlegungen

AMIs

Für das AMI muss NitroTPM aktiviert sein.

Linux AMIs

Es gibt keine vorkonfigurierten AMIs. Sie müssen Ihr eigenes AMI konfigurieren. Weitere Informationen finden Sie unter Linux-AMIs für NitroTPM aktivieren.

Windows AMIs

Informationen zu einem AWS Windows-AMI, das für NitroTPM und UEFI Secure Boot mit Microsoft-Schlüsseln vorkonfiguriert ist, finden Sie unter Suchen Sie nach einem mit NitroTPM und UEFI Secure Boot AMIs konfigurierten Windows Server in der Windows-Referenz.AWS AMIs

> **Note**
>
> Betriebssystem – Das AMI muss ein Betriebssystem mit einem TPM 2.0 Command Response Buffer (CRB)-Treiber enthalten. Die meisten aktuellen Betriebssysteme enthalten einen TPM-2.0-CRB-Treiber.
> UEFI-Boot-Modus – Das AMI muss für den UEFI-Boot-Modus konfiguriert sein. Weitere Informationen finden Sie unter UEFI Secure Boot für Amazon-EC2-Instances.

Instance-Typen

Sie müssen einen der folgenden virtualisierten Instance-Typen verwenden:

- Allzweck: M5, M5a, M5ad, M5d, M5dn, M5n, M5zn, M6a, M6g, M6gd, M6i, M6id, M6idn, M6in, M7a, M7g, M7gd, M7i, M7i-flex, M8a, M8g, M8gd, M8i, M8i-flex, T3, T3a, T4g
- Computeroptimiert: C5, C5a, C5ad, C5d, C5n, C6a, C6g, C6gd, C6Gn, C6i, C6id, C6in, C7a, C7g, C7gd, C7gn, C7i, C7i-Flex, C8a, C8g, C8GB, C8GD, C8gn, C8i, C8i-Flex
- Speicheroptimiert: R5, R5a, R5ad, R5b, R5d, R5dn, R5n, R6a, R6g, R6gd, R6i, R6id, R6idn, R6in, R7a, R7g, R7g, R7gd, R7iz, R8a, R8g, R8GB, R8gd, R8gn, R8i, R8i-Flex, U7i-6 TB, U7i-8 TB, U7i-12 TB, U7in-16 TB, U7in-24 TB, U7in-32 TB, X2IDN, X2iEDN, X2IEZN, X8G, X8AEDZ, z1d
- Speicheroptimiert: D3, D3en, I3en, I4i, I7i, I7ie, I8g, I8ge, Im4gn
- Beschleunigtes Rechnen: F2, G4dn, G5, G6, G6e, G6f, Gr6, Gr6f, Inf1, Inf2, P5, P5e, P5en, P6-B200, P6-B300, Trn2, Trn2u
- Datenverarbeitung in Hochleistung:: Hpc6a, Hpc6id

Überlegungen

Die folgenden Hinweise gelten für die Verwendung von NitroTPM:

- Wenn Sie nach dem Start einer Instance über ein AMI mit aktiviertem NitroTPM den Instance-Typ ändern möchten, muss der neue Instance-Typ, den Sie wählen, auch NitroTPM unterstützen.
- BitLocker Volumes, die mit NitroTPM-basierten Schlüsseln verschlüsselt sind, können nur auf der ursprünglichen Instanz verwendet werden.
- Der NitroTPM-Status wird in der EC2 Amazon-Konsole nicht angezeigt.
- Der NitroTPM-Status ist nicht in Amazon EBS-Snapshots enthalten.
- Der NitroTPM-Status ist nicht in VM-Import-/Export-Images enthalten.

- NitroTPM wird auf AWS Outposts., Local Zones oder Wavelength Zones nicht unterstützt.

Linux-AMIs für NitroTPM aktivieren

Um NitroTPM für eine Instance zu aktivieren, müssen Sie die Instance mit einem AMI starten, bei dem NitroTPM aktiviert ist. Sie konfigurieren Ihr Linux-AMI für die NitroTPM-Unterstützung bei der Registrierung des AMIs. Sie können die NitroTPM-Unterstützung später nicht mehr konfigurieren.

Eine Liste der Windows AMIs , die für die NitroTPM-Unterstützung vorkonfiguriert sind, finden Sie unter. Anforderungen für die Verwendung von NitroTPM mit Amazon-Instances EC2

Sie müssen ein AMI mit NitroTPM erstellen, das mithilfe der RegisterImageAPI konfiguriert wurde. Sie können die EC2 Amazon-Konsole oder VM Import/Export nicht verwenden.

So aktivieren Sie ein Linux-AMI für NitroTPM

1. Starten Sie eine temporäre Instance mit Ihrem erforderlichen Linux-AMI. Notieren Sie sich die ID des Root-Volumes, die Sie in der Konsole auf der Registerkarte Speicher für die Instance finden.
2. Wenn die Instance den `running`-Status erreicht hat, erstellen Sie einen Snapshot des Root-Volumes der Instance. Weitere Informationen finden Sie unter Erstellen eines Snapshots eines EBS-Volumes.
3. Registrieren Sie den Snapshot, den Sie erstellt haben, als AMI. Geben Sie in der Blockgerät-Zuweisung den Snapshot an, den Sie für das Root-Volume erstellt haben.

   Im Folgenden finden Sie ein Beispiel für den Befehl register-image. Legen Sie für `--tpm-support` die Option `v2.0` fest. Legen Sie für `--boot-mode` die Option `uefi` fest.

   ```
   aws ec2 register-image \
       --name my-image \
       --boot-mode uefi \
       --architecture x86_64 \
       --root-device-name /dev/xvda \
       --block-device-mappings DeviceName=/dev/
   xvda,Ebs={SnapshotId=snap-0abcdef1234567890} \
       --tpm-support v2.0
   ```

   Im Folgenden finden Sie ein Beispiel für das Register-EC2ImageCmdlet.

   ```
   $block = @{SnapshotId=snap-0abcdef1234567890}
   ```

```
Register-EC2Image `
    -Name my-image `
    -Architecture "x86_64" `
    -RootDeviceName /dev/xvda `
    -BlockDeviceMapping @{DeviceName="/dev/xvda";Ebs=$block} `
    -BootMode Uefi `
    -TpmSupport V20
```

4. Beenden Sie die temporäre Instance, die Sie in Schritt 1 gestartet haben.

Überprüfen, ob ein AMI für NitroTPM aktiviert ist

Um NitroTPM für eine Instance zu aktivieren, müssen Sie die Instance mit einem AMI starten, bei dem NitroTPM aktiviert ist. Sie können ein Image beschreiben, um zu überprüfen, ob es für NitroTPM aktiviert ist. Wenn Sie der AMI-Besitzer sind, können Sie das Image-Attribut `tpmSupport` beschreiben.

Die EC2 Amazon-Konsole wird nicht angezeigt`TpmSupport`.

AWS CLI

So überprüfen Sie, ob NitroTPM aktiviert ist

Verwenden Sie den Befehl describe-images.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Images[*].TpmSupport
```

Wenn NitroTPM für das AMI aktiviert ist, sieht die Ausgabe wie folgt aus. Wenn TPM nicht aktiviert ist, ist die Ausgabe leer.

```
[
    "v2.0"
]
```

Wenn Sie der AMI-Besitzer sind, können Sie alternativ den describe-image-attributeBefehl mit dem `tpmSupport` Attribut verwenden.

```
aws ec2 describe-image-attribute \
```

```
    --image-id ami-0abcdef1234567890 \
    --attribute tpmSupport
```

Es folgt eine Beispielausgabe.

```
{
    "ImageId": "ami-0abcdef1234567890",
    "TpmSupport": {
        "Value": "v2.0"
    }
}
```

Um zu suchen, wenn AMIs NitroTPM aktiviert ist

Das folgende Beispiel listet diejenigen auf, die IDs Sie besitzen und bei AMIs denen NitroTPM aktiviert ist.

```
aws ec2 describe-images \
    --owners self \
    --filters Name=tpm-support,Values=v2.0 \
    --query Images[].ImageId
```

PowerShell

So überprüfen Sie, ob NitroTPM aktiviert ist

Verwenden Sie das cmdlet Get-EC2Image.

```
Get-EC2Image `
    -ImageId ami-0abcdef1234567890 | Select TpmSupport
```

Wenn NitroTPM für das AMI aktiviert ist, sieht die Ausgabe wie folgt aus. Wenn TPM nicht aktiviert ist, ist die Ausgabe leer.

```
TpmSupport
----------
v2.0
```

Wenn Sie der AMI-Besitzer sind, können Sie alternativ das Get-EC2ImageAttributeCmdlet mit dem `tpmSupport` Attribut verwenden.

```
Get-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -Attribute tpmSupport
```

Um zu suchen, wenn NitroTPM AMIs aktiviert ist

Das folgende Beispiel listet diejenigen auf, die IDs Sie besitzen und bei AMIs denen NitroTPM aktiviert ist.

```
Get-EC2Image `
    -Owner self `
    -Filter @{Name="tpm-support; Values="v2.0"} | Select ImageId
```

NitroTPM auf einer Amazon-Instance aktivieren oder beenden EC2

Sie können eine EC2 Amazon-Instance für NitroTPM nur beim Start aktivieren. Sobald eine Instance für NitroTPM aktiviert ist, können Sie sie nicht mehr deaktivieren. Wenn Sie NitroTPM nicht mehr verwenden müssen, müssen Sie das Betriebssystem so konfigurieren, dass es nicht mehr verwendet wird.

Themen

- Starten Sie eine Instance mit aktiviertem NitroTPM
- Beenden der Verwendung von NitroTPM für eine Instance

Starten Sie eine Instance mit aktiviertem NitroTPM

Wenn Sie eine Instance mit den Voraussetzungen starten, wird NitroTPM automatisch auf der Instance aktiviert. Sie können NitroTPM für eine Instance nur beim Start aktivieren. Weitere Informationen über das Starten einer Instance finden Sie unter Starten Sie eine EC2 Amazon-Instance.

Beenden der Verwendung von NitroTPM für eine Instance

Nachdem Sie eine Instance mit aktiviertem NitroTPM gestartet haben, können Sie NitroTPM für die Instance nicht deaktivieren. Sie können das Betriebssystem jedoch so konfigurieren, dass es NitroTPM nicht mehr verwendet. Deaktivieren Sie dazu den TPM 2.0-Gerätetreiber für die Instance mithilfe der folgenden Tools:

- Verwenden Sie für Linux-Instances „tpm-tools“.
- Verwenden Sie für Windows-Instances die TPM-Verwaltungskonsole (tpm.msc).

Weitere Informationen über das Deaktivieren des Gerätetreibers finden Sie in der Dokumentation für Ihr Betriebssystem.

Stellen Sie sicher, dass eine EC2 Amazon-Instance für NitroTPM aktiviert ist

Sie können überprüfen, ob eine EC2 Amazon-Instance für NitroTPM aktiviert ist. Wenn die NitroTPM-Unterstützung auf der Instance aktiviert ist, gibt der Befehl `"v2.0"` zurück. Andernfalls ist das `TpmSupport`-Feld in der Ausgabe nicht vorhanden.

In der EC2 Amazon-Konsole wird das `TpmSupport` Feld nicht angezeigt.

AWS CLI

So überprüfen Sie, ob eine Instance für NitroTPM aktiviert ist

Verwenden Sie den Befehl describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].TpmSupport
```

PowerShell

So überprüfen Sie, ob eine Instance für NitroTPM aktiviert ist

Verwenden Sie das cmdlet Get-EC2Instance.

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.TpmSupport
```

NitroTPM-Zugriff auf Ihrer Windows-Instance verifizieren

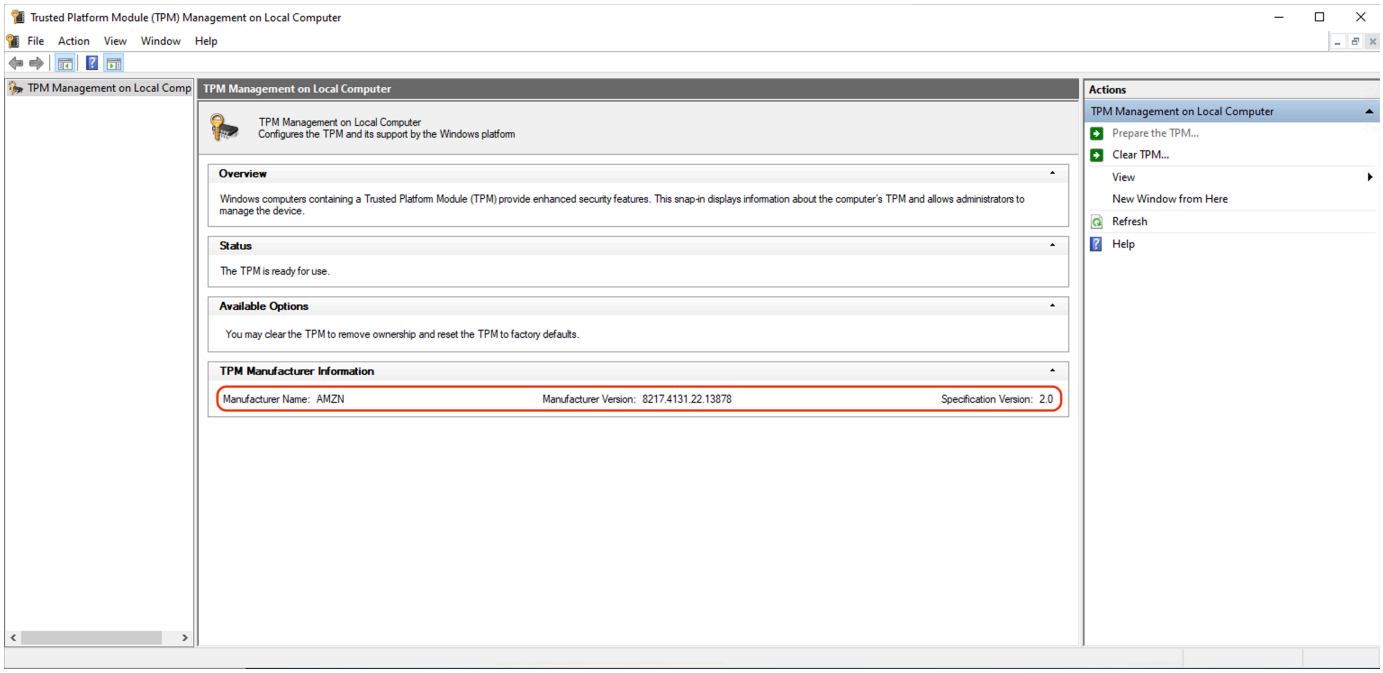
(Nur Windows-Instances) So überprüfen Sie, ob Windows Zugriff auf NitroTPM hat

1. Connect zu Ihrer EC2 Windows-Instanz her.

2. Führen Sie in der Instance das Programm „tpm.msc“ aus.

   Das Fenster TPM Management on Local Computer (TPM-Verwaltung auf lokalem Computer) wird geöffnet.

3. Setzen Sie einen Haken bei dem Feld TPM Manufacturer Information (TPM-Herstellerinformationen). Es enthält den Namen des Herstellers und die Version von NitroTPM auf der Instance.



Rufen Sie den öffentlichen Bestätigungsschlüssel für eine Instanz EC2 ab

Sie können den öffentlichen Bestätigungsschlüssel für eine Instance jederzeit sicher abrufen.

AWS CLI

So rufen Sie den öffentlichen Bestätigungsschlüssel für eine Instance ab

Verwenden Sie den Befehl get-instance-tpm-ek-pub.

Beispiel 1

Das folgende Beispiel ruft den öffentlichen `rsa-2048`-Bestätigungsschlüssel im Format `tpmt` für die angegebene Instance ab.

```
aws ec2 get-instance-tpm-ek-pub \
```

```
    --instance-id i-1234567890abcdef0 \
    --key-format tpmt \
    --key-type rsa-2048
```

Es folgt eine Beispielausgabe.

```
{
    "InstanceId": "i-01234567890abcdef",
    "KeyFormat": "tpmt",
    "KeyType": "rsa-2048",
    "KeyValue": "AAEACwADALIAIINxl2dEhLEXAMPLEUal1yT9UtduBlILZPKh2hszFGmqAAYAgABDA
    EXAMPLEAAABAOiRd7WmgtdGNoV1h/AxmW+CXExblG8pEUfNm0LOLiYnEXAMPLERqApiFa/UhvEYqN4
    Z7jKMD/usbhsQaAB1gKA5RmzuhSazHQkax7EXAMPLEzDthlS7HNGuYn5eG7qnJndRcakS+iNxT8Hvf
    0S1ZtNuItMs+Yp4SO6aU28MT/JZkOKsXIdMerY3GdWbNQz9AvYbMEXAMPLEPyHfzgVO0QTTJVGdDxh
    vxtXCOu9GYf0crbjEXAMPLEd4YTbWdDdgOKWF9fjzDytJSDhrLAOUctNzHPCd/92l5zEXAMPLEOIFA
    Ss50C0/802c17W2pMSVHvCCa9lYCiAfxH/vYKovAAE="
}
```

Beispiel 2

Das folgende Beispiel ruft den öffentlichen `rsa-2048`-Bestätigungsschlüssel im Format `der` für die angegebene Instance ab.

```
aws ec2 get-instance-tpm-ek-pub \
    --instance-id i-1234567890abcdef0 \
    --key-format der \
    --key-type rsa-2048
```

Es folgt eine Beispielausgabe.

```
{
    "InstanceId": "i-1234567890abcdef0",
    "KeyFormat": "der",
    "KeyType": "rsa-2048",
    "KeyValue": "MIIBIjANBgEXAMPLEw0BAQEFAAOCAQ8AMIIBCgKCAQEA6JF3taEXAMPLEXWH8DGZb4
    JcTFuUbykRR82bQs4uJifaKSOv5NGoEXAMPLEG8Rio3hnuMowP+6xuGxBoAHWAoDlGbO6FJrMdEXAMP
    LEnYUHvMO2GVLsc0a5ifl4buqcmd1FxqRL6I3FPwe9/REXAMPLE0yz5inhI7ppTbwxP8lmQ4qxch0x6
    tjcZ1Zs1DP0EXAMPLERUYLQ/Id/OBU7RBNMlUZ0PGG/G1cI670Zh/RytuOdx9iEXAMPLEtZ0N2A4pYX
    1+PMPK0lIOGssA5Ry03Mc8J3/3aXnOD2/ASRQ4gUBKznQLT/zTZEXAMPLEJUe8IJr2VgKIB/Ef+9gqi
    8AAQIDAQAB"
}
```

PowerShell

So rufen Sie den öffentlichen Bestätigungsschlüssel für eine Instance ab

Verwenden Sie das cmdlet Get-EC2InstanceTpmEkPub.

Beispiel 1

Das folgende Beispiel ruft den öffentlichen `rsa-2048`-Bestätigungsschlüssel im Format `tpmt` für die angegebene Instance ab.

```
Get-EC2InstanceTpmEkPub `
    -InstanceId i-1234567890abcdef0 `
    -KeyFormat tpmt `
    -KeyType rsa-2048
```

Beispiel 2

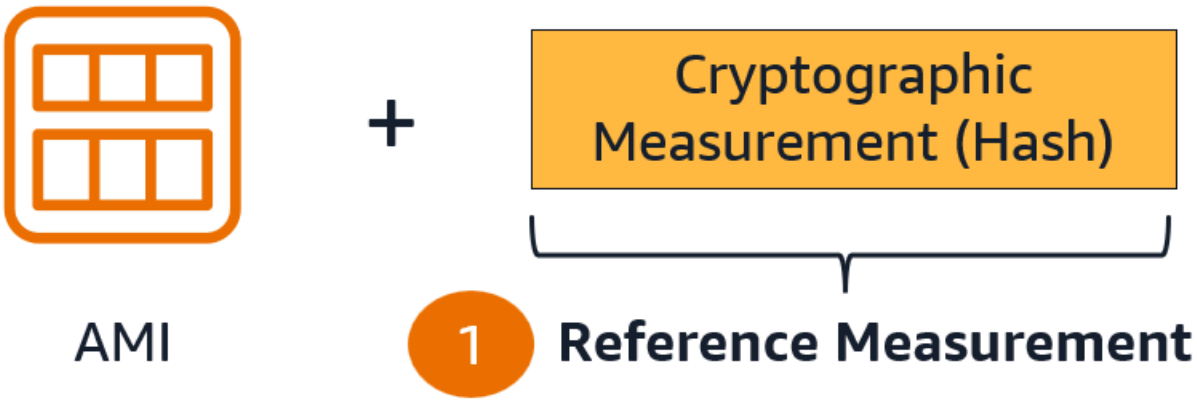
Das folgende Beispiel ruft den öffentlichen `rsa-2048`-Bestätigungsschlüssel im Format `der` für die angegebene Instance ab.

```
Get-EC2InstanceTpmEkPub `
    -InstanceId i-1234567890abcdef0 `
    -KeyFormat der `
    -KeyType rsa-2048
```

Bescheinigung von EC2 Amazon-Instanzen

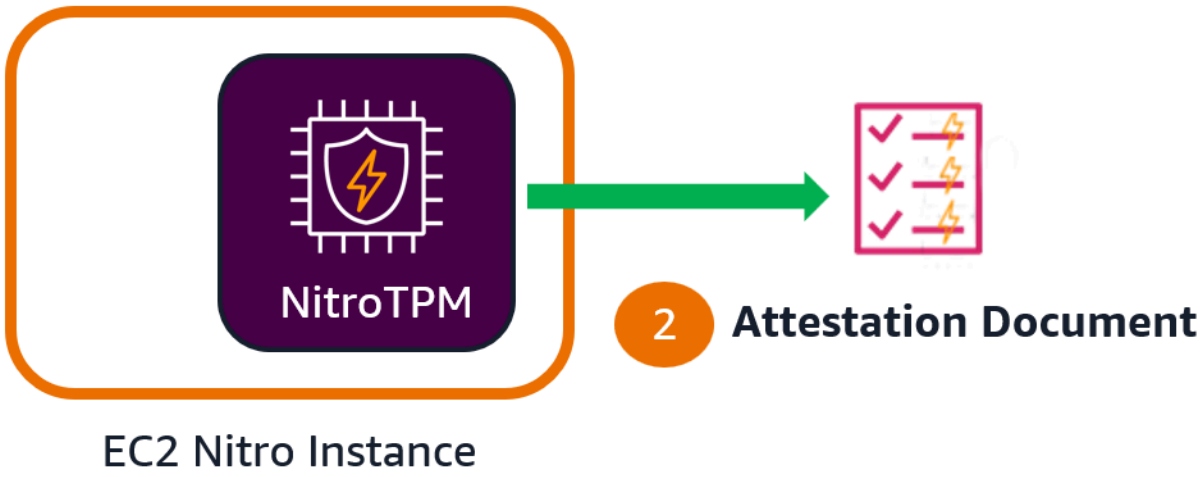
Die Bescheinigung ist ein Prozess, mit dem Sie jeder Partei kryptografisch nachweisen können, dass nur vertrauenswürdige Software, Treiber und Startprozesse auf einer Amazon-Instance ausgeführt werden. EC2 Die EC2 Amazon-Instance-Bescheinigung wird durch das Nitro Trusted Platform Module (NitroTPM) und Attestable unterstützt. AMIs

Der erste Schritt zur Attestierung besteht darin, ein attestierbares AMI zu erstellen und die Referenzmessungen dieses AMI zu bestimmen. Ein attestierbares AMI ist ein AMI, das von Grund auf für die Attestierung erstellt wurde. Bei den Referenzmessungen handelt es sich um Messungen Ihrer gesamten Software und Konfigurationen, die Sie in Ihr AMI aufgenommen haben. Weitere Informationen zum Ermitteln der Referenzmessungen finden Sie unter Beispiel-Image-Beschreibung erstellen.



Der nächste Schritt besteht darin, eine Nitro-TPM-fähige EC2 Instance mit dem Attestable AMI zu starten. Nachdem Sie die Instance gestartet haben, können Sie die NitroTPM-Tools verwenden, um das Attestierungsdokument zu generieren. Anschließend können Sie die tatsächlichen Messungen Ihrer EC2 Instance aus dem Attestierungsdokument mit den Referenzmessungen vergleichen, um zu überprüfen, ob die Instance über die Software und Konfigurationen verfügt, denen Sie vertrauen.

Indem Sie die während der Erstellung des attestierbaren AMI generierten Referenzmessungen mit den Messungen vergleichen, die im Attestierungsdokument einer Instance enthalten sind, können Sie überprüfen, ob nur Software und Code, denen Sie vertrauen, auf der Instance ausgeführt werden.



Integration mit AWS KMS

Um den Vergleich von Messungen zu vereinfachen, können Sie AWS Key Management Service (AWS KMS) als Prüfer für Bescheinigungsdokumente verwenden. Mit AWS KMS können Sie auf Bescheinigungen basierende KMS-Schlüsselrichtlinien erstellen, die bestimmte Operationen mit dem KMS-Schlüssel nur zulassen, wenn Sie ein Bescheinigungsdokument mit Messwerten bereitstellen, die den Referenzmessungen entsprechen. Dazu fügen Sie Ihren KMS-Schlüsselrichtlinien, die die Referenzmessungen als Bedingungsschlüsselwerte verwenden, spezifische Bedingungsschlüssel hinzu und geben dann an, welche KMS-Vorgänge zulässig sind, wenn der Bedingungsschlüssel erfüllt ist.

Wenn Sie KMS-Operationen mit dem KMS-Schlüssel ausführen, müssen Sie der KMS-Anfrage ein Bestätigungsdokument beifügen. AWS KMS validiert dann die Messungen aus dem Bescheinigungsdokument anhand der Referenzmessungen in der KMS-Schlüsselrichtlinie und ermöglicht den Schlüsselzugriff nur, wenn die Messungen übereinstimmen.

Wenn Sie das Attestierungsdokument für eine Instance generieren, müssen Sie außerdem einen öffentlichen Schlüssel für ein Schlüsselpaar angeben, das Sie besitzen. Der angegebene öffentliche Schlüssel ist im Attestierungsdokument enthalten. Wenn das Bestätigungsdokument AWS KMS validiert und eine Entschlüsselung zugelassen wird, verschlüsselt es die Antwort automatisch mit dem öffentlichen Schlüssel, der im Bestätigungsdokument enthalten ist, bevor sie zurückgegeben wird. Dadurch wird sichergestellt, dass die Antwort entschlüsselt werden kann und nur mit dem entsprechenden privaten Schlüssel für den öffentlichen Schlüssel, der in der Bescheinigung enthalten ist, entschlüsselt und verwendet werden kann.

Dadurch wird sichergestellt, dass nur Instances, auf denen vertrauenswürdige Software und vertrauenswürdiger Code ausgeführt werden, kryptografische Vorgänge mit einem KMS-Schlüssel ausführen können.

Attestierung isolierter Rechenumgebungen

Im Allgemeinen können Sie eine EC2 Instanz als isolierte Computerumgebung erstellen und konfigurieren, die keinen interaktiven Zugriff und keinen Mechanismus für Ihre Administratoren und Benutzer bietet, um auf die Daten zuzugreifen, die in der Instanz verarbeitet werden. EC2 Mit der EC2 Instanzbescheinigung können Sie einem Drittanbieter oder Dienst nachweisen, dass Ihre Instanz als isolierte Computerumgebung ausgeführt wird. Weitere Informationen finden Sie unter Isolieren Sie Daten von Ihren eigenen Bedienern.

Ein Beispiel finden Sie in der Beispiel-Image-Beschreibung für Amazon Linux 2023, die eine isolierte Rechenumgebung erstellt. Sie können diese Beispiel-Image-Beschreibung als Ausgangspunkt verwenden und sie an Ihre Anforderungen anpassen.

AWS Modell mit geteilter Verantwortung

NitroTPM und Attestable AMIs sind Bausteine, die Ihnen helfen können, die Bescheinigung für Ihre Instanzen einzurichten und zu konfigurieren. EC2 Sie sind dafür verantwortlich, das AMI so zu konfigurieren, dass es Ihrem jeweiligen Anwendungsfall entspricht. Weitere Informationen finden Sie unter AWS -Modell der geteilten Verantwortung.

Themen

- Bescheinigbar AMIs
- Bereiten Sie sich auf AWS KMS die Bescheinigung vor
- Das NitroTPM-Attestierungsdokument abrufen
- Integration mit AWS KMS
- Isolieren Sie Daten von Ihren eigenen Bedienern

Bescheinigbar AMIs

Ein attestierbares AMI ist ein Amazon Machine Image (AMI) mit einem entsprechenden kryptografischen Hash, der seinen gesamten Inhalt darstellt. Der Hash wird während des AMI-Erstellungsprozesses generiert und auf der Grundlage des gesamten Inhalts dieses AMI berechnet, einschließlich der Anwendungen, des Codes und des Startvorgangs.

Beibehaltung eines attestierbaren Status

Die Messungen einer Instance basieren auf ihrem anfänglichen Startstatus. Alle Software- oder Codeänderungen, die nach dem Start an der Instance vorgenommen werden und auch nach Neustarts bestehen bleiben, wirken sich auf die Messwerte der Instance nach dem Neustart aus. Wenn die Messungen geändert werden, weichen sie von den Referenzmessungen des attestierbaren AMI ab, und die Instance kann nach dem Neustart nicht mehr erfolgreich von AWS KMS attestiert werden. Damit Attestable AMIs nützlich ist, müssen Instances daher nach dem Neustart in ihren ursprünglichen Startstatus zurückkehren.

Wenn Sie immer zum ursprünglichen Startstatus zurückkehren, wird sichergestellt, dass eine Instance nach dem Neustart erfolgreich attestiert werden kann. Die folgenden Hilfsprogramme

können verwendet werden, um sicherzustellen, dass Ihre Instances auch nach einem Neustart attestierbar bleiben:

- `erofs` – Verbessertes schreibgeschütztes Dateisystem. Dieses Hilfsprogramm stellt sicher, dass Ihr Root-Dateisystem schreibgeschützt ist. Mit diesem Hilfsprogramm werden Schreibvorgänge in das Dateisystem, einschließlich `/etc`, `/run` und `/var` im Arbeitsspeicher gespeichert und gehen verloren, wenn die Instance neu gestartet wird, sodass das Root-Dateisystem in seinem ursprünglichen Startstatus belassen wird. Weitere Informationen finden Sie in der erofs-Dokumentation.
- `dm-verity` – Bietet Integritätsschutz für das schreibgeschützte Root-Dateisystem. Das Hilfsprogramm berechnet einen Hash der Dateisystemblöcke und speichert ihn in der Kernel-Befehlszeile. Dadurch kann der Kernel die Integrität des Dateisystems beim Hochfahren überprüfen. Weitere Informationen finden Sie in der dm-verity-Dokumentation.

Voraussetzungen für die Erstellung von Attestable AMIs

Für Attestable gelten die folgenden AMIs Anforderungen:

- Basisbetriebssystem – Amazon Linux 2023 und NixOS
- Architektur – `x86_64`- oder `arm64`-Architektur
- TPM-Unterstützung – NitroTPM muss aktiviert sein. Weitere Informationen finden Sie unter Anforderungen für die Verwendung von NitroTPM mit Amazon-Instances EC2 .
- Startmodus – Der UEFI-Startmodus muss aktiviert sein.

Themen

- Attestable wird erstellt AMIs
- Beispiel-Image-Beschreibung für Amazon Linux 2023 erstellen
- Beispiel-Image-Beschreibung für Amazon Linux 2023
- Die Beispiel-Image-Beschreibung für Amazon Linux 2023 an Ihren Workload anpassen
- PCR-Messungen für ein benutzerdefiniertes AMI berechnen

Attestable wird erstellt AMIs

Um ein attestierbares AMI zu erstellen, müssen Sie Amazon Linux 2023 mit KIWI Next Generation (KIWI NG) verwenden. Amazon Linux 2023 bietet die gesamte Software und sämtliche Hilfsprogramme, die für die Erstellung eines attestierbaren AMI mit KIWI NG erforderlich sind.

KIWI NG ist ein Open-Source-Tool zum Entwickeln von vorkonfigurierten Linux-basierten Images. KIWI NG verwendet XML-Image-Beschreibungen, die den Inhalt eines Images definieren. Die Image-Beschreibung spezifiziert das Basisbetriebssystem, die Software, die Kernelkonfiguration und die Skripts, die ausgeführt werden müssen, um ein ready-to-use AMI für einen bestimmten Anwendungsfall zu erstellen.

Während der AMI-Erstellungszeit müssen Sie das Hilfsprogramm `nitro-tpm-pcr-compute` verwenden, um die Referenzmessungen auf der Grundlage des von KIWI NG generierten Unified Kernel Image (UKI) zu generieren. Weitere Informationen zur Verwendung des Hilfsprogramms `nitro-tpm-pcr-compute` finden Sie unter PCR-Messungen für ein benutzerdefiniertes AMI berechnen.

AWS bietet ein Beispiel für eine Beschreibung eines Amazon Linux 2023-Images, das alle Konfigurationen enthält, die für die Konfiguration einer EC2 Instance in einer isolierten Computerumgebung erforderlich sind. Weitere Informationen finden Sie unter Beispiel-Image-Beschreibung für Amazon Linux 2023 erstellen.

Beispiel-Image-Beschreibung für Amazon Linux 2023 erstellen

AWS bietet ein Beispiel für eine Amazon Linux 2023-Imagebeschreibung, die Sie als Ausgangspunkt für die Erstellung Ihres eigenen benutzerdefinierten Attestable AMIs für Ihre Workloads verwenden können. Die Beschreibung des Beispielimages umfasst Amazon Linux 2023 als Basisbetriebssystem `dm-verity` und `erofs` Konfigurationen für die Unveränderlichkeit des Dateisystems. Außerdem wird jeglicher interaktiver Zugriff (wie SSH, EC2 Instance-Verbindung und serielle Konsole) entfernt, um eine isolierte Rechenumgebung zu schaffen. Weitere Informationen über die Beispiel-Image-Beschreibung finden Sie im Github-Repo.

Die Beispiel-Image-Beschreibung installiert automatisch die NitroTPM-Tools (`nitro-tpm-pcr-compute` und `nitro-tpm-attest`) im erstellten Image im Verzeichnis `/usr/bin/`. Dadurch wird sichergestellt, dass die Tools auf Instances vorinstalliert sind, die über das AMI gestartet werden.

Die Beispiel-Image-Beschreibung umfasst ein Skript, `edit_boot_install.sh`, das die Befehle enthält, die zum Generieren der Referenzmessungen erforderlich sind. Das Skript hängt die von KIWI NG erstellte rohe Festplatten-Image-Datei (`.raw`) auf einem Loopback-Gerät ein, lokalisiert die

UKI mit der Dateierweiterung `.efi` und führt dann das Hilfsprogramm `nitro-tpm-pcr-compute` aus, um die Referenzmessungen für das AMI zu generieren. Das Skript wird während der Build-Zeit automatisch von KIWI NG ausgeführt.

In diesem Tutorial erfahren Sie, wie Sie die Beispiel-Image-Beschreibung erstellen, um ein attestierbares AMI zu erstellen.

Weitere Informationen zum Erstellen eigener Image-Beschreibungen finden Sie in der folgenden KIWI-NG-Dokumentation:

- Schnellstart
- Image-Beschreibung
- Beispiel-Image-Beschreibung für Amazon Linux 2023

So erstellen Sie eine Beispiel-Image-Beschreibung für Amazon Linux 2023 mit KIWI NG

1. Starten Sie eine EC2 Amazon-Instance mit dem neuesten AL2 023-AMI. Um sicherzustellen, dass Ihre Instance über ausreichend Speicherplatz für die Erstellung des AMI verfügt, stellen Sie sicher, dass Sie mindestens 12 GB Speicher bereitstellen.
2. Installieren Sie die erforderlichen Abhängigkeiten. Der folgende Befehl installiert die folgenden Hilfsprogramme:

   - `kiwi-cli`
   - `veritysetup`
   - `erofs-utils`
   - `aws-nitro-tpm-tools`

   ```
   sudo dnf install -y kiwi-cli python3-kiwi kiwi-systemdeps-core python3-poetry-core
    qemu-img veritysetup erofs-utils git cargo aws-nitro-tpm-tools
   ```

3. Installieren Sie das Hilfsprogramm `coldsnap`. Mit diesem Hilfsprogramm können Sie Amazon-EBS-Snapshots aus Image-Rohdaten erstellen. Sie verwenden dieses Hilfsprogramm, um einen EBS-Snapshot aus der von KIWI NG erstellten rohen Festplatten-Image-Datei zu erstellen.

   ```
   git clone https://github.com/awslabs/coldsnap.git
   cd coldsnap
   cargo install --locked coldsnap
   ```

```
cd ..
```

4. Rufen Sie die Dateien der Beispiel-Image-Beschreibung ab.

```
sudo dnf install kiwi-image-descriptions-examples
```

Die Dateien der Beispiel-Image-Beschreibung werden in das folgende Verzeichnis heruntergeladen: `/usr/share/kiwi-image-descriptions-examples/al2023/attestable-image-example`

5. Erstellen Sie die Beispiel-Image-Beschreibung mit dem KIWI-NG-Befehl `system build`. Mit dem folgenden Befehl wird eine rohe Festplatten-Image-Datei im Verzeichnis `./image` erstellt.

```
sudo kiwi-ng \
--color-output \
--loglevel 0 \
system build \
--description /usr/share/kiwi-image-descriptions-examples/al2023/attestable-image-example \
--target-dir ./image
```

Weitere Informationen finden Sie in der Dokumentation kiwi-ng system build.

6. Rufen Sie die Referenzmessungen für das AMI ab. Die Messungen werden vom Hilfsprogramm `nitro-tpm-pcr-compute` während der Image-Erstellung im vorherigen Schritt generiert. Sie können die Referenzmessungen in der folgenden Datei finden: `./image/pcr_measurements.json`.

Die Messungen werden im folgenden JSON-Format bereitgestellt:

```
{
  "Measurements": {
    "HashAlgorithm": "SHA384 { ... }",
    "PCR4": "PCR4_measurement",
    "PCR7": "PCR7_measurement",
    "PCR12": "PCR12_measurement"
  }
}
```

7. Verwenden Sie das Hilfsprogramm `coldsnap`, um das von KIWI NG erstellte rohe Festplatten-Image in einen EBS-Snapshot hochzuladen. Der Befehl gibt die Snapshot-ID zurück. Notieren Sie sich die ID, die Sie im nächsten Schritt benötigen.

```
SNAPSHOT=$(.cargo/bin/coldsnap upload ./image/kiwi*.raw)
echo "Created snapshot: $SNAPSHOT"
```

Weitere Informationen über das `coldsnap` Hilfsprogramm finden Sie im GitHub Coldsnap-Repo.

8. Registrieren Sie ein TPM-2.0-fähiges AMI im UEFI-Startmodus mithilfe des Snapshots aus dem vorherigen Schritt. Geben Sie bei `--architecture` den Wert `x86_64` für Intel oder `arm64` für Graviton an.

```
aws ec2 register-image \
--name "attestable_isolated_al2023_ami" \
--virtualization-type hvm \
--boot-mode uefi \
--architecture x86_64|arm64 \
--root-device-name /dev/xvda \
--block-device-mappings DeviceName=/dev/xvda,Ebs={SnapshotId=${SNAPSHOT}} \
--tpm-support v2.0 \
--ena-support
```

Beispiel-Image-Beschreibung für Amazon Linux 2023

Die Beispiel-Image-Beschreibung für Amazon Linux 2023 hat die folgenden Eigenschaften:

1. Unified Kernel Image (UKI)-Boot – Hochfahren mit einer einzigen, signierten Binärdatei, die den Kernel, `initrd` und die Startparameter zu einem unveränderlichen Image kombiniert.
2. Schreibgeschütztes Root-Dateisystem – Verwenden Sie das Enhanced Read-Only File System (`erofs`) mit dm-verity-Schutz, um sicherzustellen, dass das Root-Dateisystem nicht verändert werden kann und um die kryptografische Integritätsprüfung aufrechtzuerhalten.
3. Flüchtiges Overlay-Dateisystem – Erzeugt ein temporäres Overlay-Dateisystem, das temporäre Schreibvorgänge in Verzeichnisse wie `/etc`, `/run` und `/var` ermöglicht. Da dieses Overlay-Dateisystem nur im Arbeitsspeicher existiert, gehen alle Änderungen automatisch verloren, wenn die Instance neu gestartet wird. Dadurch wird sichergestellt, dass das System zu seinem ursprünglichen vertrauenswürdigen Status zurückkehrt.
4. Deaktivierte Fernzugriffsmethoden – Entfernen Sie die folgenden Fernzugriffsmechanismen, um den Fernzugriff zu verhindern:

Zugriffsmethode	Description	Image-Beschreibung, Implementierung
SSH	Schließt OpenSSH-Server aus. Macht die Instance von Natur aus unfähig, SSH-Verkehr zu verarbeiten.	Das `openssh-server` -Paket ignorieren *
User Data	Entfernt Cloud-Init. Beseitigt die Möglichkeit für Bediener, Benutzerdaten für Instances bereitzustellen und Startzeitskripts auszuführen.	Die Pakete `cloud-init` und `cloud-init-cfg-ec2` ignorieren *
Chrony	Deaktiviert den Chrony-Befehlsport. Hindert Bediener daran, Chrony-Befehle auf laufenden Instances auszuführen.	Das `amazon-chrony-config` -Paket ignorieren *
MOTD	Entfernt das MOTD-Paket. Beseitigt die Möglichkeit für Bediener, Nachrichten oder Funktionen laufender Instances zu ändern.	Das `update-motd` -Paket ignorieren *
AWS SSM	Entfernt den AWS SSM-Agenten. Verhindert den Fernzugriff auf laufende Instanzen mithilfe von AWS SSM.	Das `amazon-ssm-agent` -Paket ignorieren *
EC2 Instanzverbindung	Entfernt das EC2 Instance Connect-Paket. Deaktiviert den SSH-Zugriff mit diesem Tool.	Das `ec2-instance-connect` -Paket ignorieren *

Zugriffsmethode	Description	Image-Beschreibung, Implementierung
Serielle Konsole	Deaktiviert die serielle Konsole. Stellt sicher, dass der Konsolenzugriff für laufende Instances nicht verfügbar ist, und verhindert, dass sich Bediener an der seriellen Konsole anmelden können.	Über den Kernel-Befehlszeilenparameter deaktiviert

* Weitere Informationen finden Sie unter Elemente der Image-Beschreibung.

Die Beispiel-Image-Beschreibung für Amazon Linux 2023 an Ihren Workload anpassen

Sie können die Beispiel-Image-Beschreibung für Amazon Linux 2023 anpassen und die Softwarepakete, Skripts und Dateien hinzufügen, die für Ihren spezifischen Workload benötigt werden. Anpassungen werden durch Hinzufügen oder Ändern verschiedener Elemente in der KIWI-NG-Image-Beschreibung erreicht.

Themen

- Repository-Verwaltung
- Paketmanagement
- Dateien und Verzeichnisse hinzufügen
- Hinzufügen von benutzerdefinierten Skripts

Repository-Verwaltung

Standardmäßig enthält die Beispiel-Image-Beschreibung ein einzelnes `<repository>`-Element, das auf einen Spiegelendpunkt für die Kern-Repositorys von Amazon Linux 2023 verweist. Bei Bedarf können Sie Verweise auf andere Repositorys hinzufügen, von denen aus Sie Ihre benötigte Software installieren können.

Die Beispiel-Image-Beschreibung verwendet den `dnf`-Paketmanager, wie er im `<packagemanager>`-Element definiert ist.

Weitere Informationen zum Hinzufügen von Repositorys finden Sie unter Repositorys einrichten.

Paketmanagement

Standardmäßig enthält die Beispiel-Image-Beschreibung alle Pakete, die zur Erstellung eines Amazon Linux 2023 attestierbaren AMI für eine isolierte Rechenumgebung mit einem schreibgeschützten `erofs`-Dateisystem erforderlich sind.

Sie können zusätzliche Softwarepakete in die Image-Beschreibung aufnehmen, indem Sie sie dem `<packages>`-Element in der Image-Beschreibung hinzufügen. Das `<packages>`-Element definiert die gesamte Software, die im AMI installiert werden soll.

Sie können das `<packages>`-Element auch verwenden, um bestimmte Softwarepakete zu deinstallieren oder zu löschen.

Weitere Informationen zum Hinzufügen oder Entfernen von Paketen in der Image-Beschreibung finden Sie unter Pakete hinzufügen und entfernen.

Dateien und Verzeichnisse hinzufügen

Die Beispiel-Image-Beschreibung enthält einen Overlay-Verzeichnisbaum (`/root/`). Der Overlay-Verzeichnisbaum ist ein Verzeichnis, das Dateien und Verzeichnisse enthält, die während der Image-Erstellung in das Image kopiert werden. Alle Dateien und Verzeichnisse, die Sie im Overlay-Verzeichnisbaum platzieren, werden während der Image-Erstellung direkt in das Root-Dateisystem des Images kopiert.

Der Overlay-Verzeichnisbaum wird in das Image kopiert, nachdem alle Pakete installiert wurden. Neue Dateien werden hinzugefügt und bestehende Dateien werden überschrieben.

Hinzufügen von benutzerdefinierten Skripts

Die Beispiel-Image-Beschreibung enthält ein einzelnes benutzerdefiniertes Skript, `edit_boot_install.sh`. Dieses Skript enthält die Befehle, die zur Ausführung des Hilfsprogramms `nitro-tpm-pcr-compute` erforderlich sind, das die Referenzmessungen auf der Grundlage des Image-Inhalts generiert. Dieses Skript wird unmittelbar nach der Installation des Bootloaders aufgerufen.

Bei Bedarf können Sie Ihre eigenen benutzerdefinierten Skripts in die Image-Beschreibung aufnehmen, um Aufgaben oder Konfigurationen während der Image-Erstellung oder beim ersten Start des Images durchzuführen. Mithilfe von Skripts können Sie Ihre Images auf eine Weise anpassen, die mit der Image-Beschreibung allein nicht erreicht werden kann.

Um benutzerdefinierte Skripts in Ihre Image-Beschreibung aufzunehmen, müssen Sie sie je nach Art des Skripts korrekt benennen und sie demselben Verzeichnis wie die `appliance.kiwi`-Datei

hinzufügen. KIWI NG erkennt die Skripte automatisch und führt sie aus, wenn sie korrekt benannt und an der richtigen Stelle platziert sind, ohne dass in der Image-Beschreibungsdatei explizit auf sie verwiesen werden muss.

Weitere Informationen zu den von KIWI NG unterstützten Skripts finden Sie unter Benutzerdefinierte Skripts.

PCR-Messungen für ein benutzerdefiniertes AMI berechnen

Das Hilfsprogramm `nitro-tpm-pcr-compute` ermöglicht es Ihnen, während der Build-Zeit die Referenzmessungen für ein attestierbares AMI auf der Grundlage seines Unified Kernel Image (UKI) zu generieren.

Die Beispiel-Image-Beschreibung für Amazon Linux 2023 installiert automatisch das Hilfsprogramm im erstellten Image im `/usr/bin/`-Verzeichnis. Die Beispiel-Image-Beschreibung enthält auch ein Skript mit den Befehlen, die zur Ausführung des Hilfsprogramms zur Generierung der Referenzmessungen während der Image-Erstellung erforderlich sind. Wenn Sie die Beispiel-Image-Beschreibung verwenden, müssen Sie das Hilfsprogramm nicht installieren oder manuell ausführen. Weitere Informationen finden Sie unter Beispiel-Image-Beschreibung für Amazon Linux 2023 erstellen.

Das Hilfsprogramm **`nitro-tpm-pcr-compute`** installieren

Wenn Sie Amazon Linux 2023 verwenden, können Sie das Hilfsprogramm `nitro-tpm-pcr-compute` wie folgt aus dem Amazon-Linux-Repository installieren.

```
sudo yum install aws-nitro-tpm-tools
```

Die Tools sind im `/usr/bin`-Verzeichnis installiert.

Das Hilfsprogramm **`nitro-tpm-pcr-compute`** verwenden

Das Hilfsprogramm bietet einen einzigen Befehl, `nitro-tpm-pcr-compute`, zum Generieren der Referenzmessungen.

Wenn Sie den Befehl ausführen, müssen Sie Folgendes angeben:

- Unified Kernel Image (`UKI.efi`) – Erforderlich für Standardstart und UEFI.

So generieren Sie die Referenzmessungen für ein attestierbares AMI:

Verwenden Sie den folgenden Befehl und die folgenden Parameter:

```
/usr/bin/nitro-tpm-pcr-compute \
--image UKI.efi
```

Das Hilfsprogramm gibt die Referenzmessungen im folgenden JSON-Format zurück:

```
{
  "Measurements": {
    "HashAlgorithm": "SHA384 { ... }",
    "PCR4": "PCR4_measurement",
    "PCR7": "PCR7_measurement",
    "PCR12": "PCR12_measurement"
  }
}
```

Ein praktisches Beispiel für die Verwendung des Hilfsprogramms `nitro-tpm-pcr-compute` finden Sie in dem `edit_boot_install.sh`-Skript, das in der Beispielsbeschreibung eines Amazon-Linux-2023-Image enthalten ist.

Bereiten Sie sich auf AWS KMS die Bescheinigung vor

> **Note**
>
> Wenn Sie einen Service eines Drittanbieters attestieren, müssen Sie Ihre eigenen benutzerdefinierten Mechanismen für den Empfang, die Analyse und die Validierung von Attestierungsdokumenten entwickeln. Weitere Informationen finden Sie unter Ein NitroTPM-Attestierungsdokument validieren.

Nachdem Sie Ihr Attestable AMI erstellt haben, sollten Sie über Referenzmessungen verfügen, anhand derer Sie Anfragen von einer EC2 Amazon-Instance validieren können. AWS KMS bietet integrierte Unterstützung für die Bescheinigung mit NitroTPM.

Fügen Sie für den AWS KMS Schlüssel, den Sie zur Verschlüsselung Ihrer geheimen Daten verwendet haben, eine Schlüsselrichtlinie hinzu, die den Schlüsselzugriff nur erlaubt, wenn API-Anfragen ein Bestätigungsdokument mit Messungen enthalten, die den Referenzmessungen entsprechen, die Sie während der Erstellung des Attestable AMI generiert haben. Verwendung PCR4 und PCR12 Maße für Standardstart oder PCR7 Messungen für Secure Boot. Dadurch wird

sichergestellt, dass nur Anfragen von Instances, die mit dem Attestable AMI gestartet wurden, kryptografische Operationen mit dem Schlüssel ausführen können. AWS KMS

AWS KMS stelltkms:RecipientAttestation:NitroTPMPCR4, und kms:RecipientAttestation:NitroTPMPCR12 Bedingungsschlüssel bereitkms:RecipientAttestation:NitroTPMPCR7, mit denen Sie auf Bescheinigungen basierende Bedingungen für NitroTPM KMS-Schlüsselrichtlinien erstellen können. Weitere Informationen finden Sie unter Bedingungsschlüssel für NitroTPM.

Zum Beispiel erlaubt die folgende AWS KMS Schlüsselrichtlinie den Schlüsselzugriff nur, wenn die Anfrage von einer Instanz mit angehängtem Instanzprofil stammt und wenn die MyEC2InstanceRole Anfrage ein Bestätigungsdokument mit spezifischen PCR 4- und PCR 12-Werten enthält.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow requests from instances with attested AMI only",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyEC2InstanceRole"
      },
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateRandom"
      ],
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {

 "kms:RecipientAttestation:NitroTPMPCR4":"EXAMPLE6b9b3d89a53b13f5dfd14a1049ec0b80a9ae4b159adde4

 "kms:RecipientAttestation:NitroTPMPCR12":"000000000000000000000000000000000000000000000000000000
        }
      }
    }
  ]
}
```

Das NitroTPM-Attestierungsdokument abrufen

Das Attestierungsdokument ist ein wichtiger Bestandteil des NitroTPM-Attestierungsprozesses. Es enthält eine Reihe von kryptografischen Messungen, anhand derer die Identität der Instance überprüft und nachgewiesen werden kann, dass auf ihr nur vertrauenswürdige Software ausgeführt wird. Sie können das Bescheinigungsdokument mit verwenden AWS KMS, das integrierte Unterstützung für die NitroTPM-Bescheinigung bietet, oder um Ihre eigenen kryptografischen Bestätigungsmechanismen zu erstellen.

Das `nitro-tpm-attest` Tool ermöglicht es Ihnen, während der Laufzeit ein signiertes NitroTPM-Bestätigungsdokument für eine EC2 Amazon-Instance abzurufen.

Die Beispiel-Image-Beschreibung für Amazon Linux 2023 installiert automatisch das Hilfsprogramm im erstellten Image im `/usr/bin/`-Verzeichnis. Dadurch wird sichergestellt, dass das Hilfsprogramm auf Instances vorinstalliert ist, die mit dem AMI gestartet werden. Sie brauchen das Hilfsprogramm nicht manuell zu installieren. Weitere Informationen finden Sie unter Beispiel-Image-Beschreibung für Amazon Linux 2023 erstellen.

Themen

- Das Hilfsprogramm nitro-tpm-attest installieren
- Das Hilfsprogramm nitro-tpm-attest verwenden
- Inhalt des NitroTPM-Attestierungsdokuments
- Ein NitroTPM-Attestierungsdokument validieren

Das Hilfsprogramm **`nitro-tpm-attest`** installieren

Wenn Sie Amazon Linux 2023 verwenden, können Sie das Hilfsprogramm `nitro-tpm-attest` wie folgt aus dem Amazon-Linux-Repository installieren.

```
sudo yum install aws-nitro-tpm-tools
```

Das Hilfsprogramm **`nitro-tpm-attest`** verwenden

Das Hilfsprogramm stellt einen einzigen Befehl, `nitro-tpm-attest`, zum Abrufen des Attestierungsdokuments bereit. Der Befehl gibt das Attestierungsdokument zurück, das in Concise Binary Object Representation (CBOR) codiert und mit CBOR Object Signing and Encryption (COSE) signiert wurde.

Wenn Sie den Befehl ausführen, können Sie die folgenden optionalen Parameter angeben:

- `public-key`— Ein öffentlicher Schlüssel, der von AWS KMS oder einem externen Dienst verwendet werden kann, um Antwortdaten zu verschlüsseln, bevor sie zurückgegeben werden. Dadurch wird sichergestellt, dass nur der vorgesehene Empfänger, der im Besitz des privaten Schlüssels ist, die Daten entschlüsseln kann. Wenn Sie beispielsweise mit bestätigen, verschlüsselt der Dienst die Klartextdaten mit AWS KMS dem öffentlichen Schlüssel im Bestätigungsdokument und gibt den resultierenden Chiffretext in dem Feld in der Antwort zurück. `CiphertextForRecipient` Es werden nur RSA-Schlüssel unterstützt.
- `user-data` – Die Benutzerdaten können verwendet werden, um zusätzliche signierte Daten an einen externen Service zu übermitteln. Diese Benutzerdaten können verwendet werden, um ein zwischen der anfragenden Instance und dem externen Service vereinbartes Protokoll abzuschließen. Wird AWS KMS nicht für die Bescheinigung mit verwendet.
- `nonce` – Die Nonce kann verwendet werden, um eine Challenge-Response-Authentifizierung zwischen der Instance und dem externen Service einzurichten, um Angriffe mit Identitätsmissbrauch zu verhindern. Mithilfe einer Nonce kann der externe Service überprüfen, ob er mit einer Live-Instance interagiert und nicht mit einem Imitator, der ein altes Attestierungsdokument wiederverwendet. Wird nicht zur Bescheinigung mit verwendet. AWS KMS

So rufen Sie das Attestierungsdokument ab

Verwenden Sie den folgenden Befehl und die optionalen Parameter:

```
/usr/bin/nitro-tpm-attest \
--public-key rsa_public_key \
--user-data user_data \
--nonce nonce
```

Ein vollständiges Beispiel, das zeigt, wie man ein RSA-Schlüsselpaar generiert und wie man eine Bescheinigung mit dem öffentlichen Schlüssel anfordert, finden Sie im Repo. nitro-tpm-attest GitHub

Inhalt des NitroTPM-Attestierungsdokuments

Ein Attestierungsdokument wird vom NitroTPM generiert und vom Nitro-Hypervisor signiert. Es enthält eine Reihe von PCR-Werten (Platform Configuration Registers), die sich auf eine EC2 Amazon-Instance beziehen. Folgendes ist PCRs im Bescheinigungsdokument enthalten:

> **Important**
>
> PCR0 und PCR1 werden im Allgemeinen verwendet, um den anfänglichen Startcode zu messen, der von gesteuert wird. AWS Um sichere Aktualisierungen des frühen Startcodes zu ermöglichen, enthalten PCRs diese immer konstante Werte.

- `PCR0` – Ausführbarer Code für die Kernsystem-Firmware
- `PCR1` – Firmware-Daten des Kernsystems
- `PCR2` – Erweiterter oder austauschbarer ausführbarer Code
- `PCR3` – Erweiterte oder austauschbare Firmware-Daten
- `PCR4` – Boot-Manager-Code
- `PCR5` – Konfiguration des Boot-Manager-Codes sowie Daten- und GPT-Partitionstabelle
- `PCR6` – Angaben zum Hersteller der Hostplattform
- `PCR7` – Secure Boot Policy
- `PCR8 - 15` – Definiert für die Verwendung durch das statische Betriebssystem
- `PCR16` – Debug
- `PCR23` – Anwendungsunterstützung

PCR4PCR7, und werden PCR12speziell verwendet, um zu überprüfen, ob eine Instance mit einem attestierbaren AMI gestartet wurde. PCR4 und PCR12 können zur Validierung mit Standardstart und PCR7 zur Validierung mit Secure Boot verwendet werden.

- PCR4 (Boot Manager Code) — Wenn eine Instanz gestartet wird, erstellt NitroTPM kryptografische Hashes aller Binärdateien, die von seiner UEFI-Umgebung ausgeführt werden. Mit Attestable betten diese Boot-Binärdateien Hashes ein AMIs, die das future Laden von Binärdateien verhindern, die keine passenden Hashes haben. Auf diese Weise kann der binäre Single-Boot-Hash genau beschreiben, welchen Code eine Instance ausführen wird.
- PCR7 (Secure Boot Policy) — UEFI-Boot-Binärdateien können mit einem UEFI Secure Boot-Signaturschlüssel signiert werden. Wenn UEFI Secure Boot aktiviert ist, verhindert UEFI die Ausführung von UEFI-Boot-Binärdateien, die nicht der konfigurierten Richtlinie entsprechen. PCR7 enthält einen Hash der UEFI-Secure-Boot-Richtlinie der Instanz.

  Wenn Sie eine einzige KMS-Richtlinie beibehalten müssen, die für alle Instanzupdates gültig ist, können Sie eine Richtlinie erstellen, die anhand eines UEFI Secure Boot-Zertifikats validiert wird

PCR7 , um es zu validieren. Während der Erstellung eines attestierbaren AMI können Sie dann die Boot-Binärdatei mit Ihrem Zertifikat signieren und sie als einzig zulässiges Zertifikat in den UEFI-Daten des AMI installieren. Beachten Sie, dass Sie bei diesem Modell immer noch ein neues Zertifikat generieren, es in Ihrer Richtlinie installieren und aktualisieren müssen, AMIs wenn Sie verhindern möchten, dass Instanzen, die von einem alten (nicht vertrauenswürdigen) System gestartet wurden, Ihre KMS-Richtlinie AMIs erfüllen.

- PCR12— Enthält den Hash der Befehlszeile, die an die UEFI-Boot-Binärdatei übergeben wurde. In Verbindung mit PCR4 für den Standardstart erforderlich, um zu überprüfen, ob die Befehlszeile nicht geändert wurde.

Ein NitroTPM-Attestierungsdokument validieren

> **Note**
>
> Dieses Thema richtet sich an Benutzer, die einen Schlüsselverwaltungsservice eines Drittanbieters verwenden und ihre eigenen Mechanismen zur Überprüfung von Attestierungsdokumenten erstellen müssen.

Dieses Thema bietet einen detaillierten Überblick über den gesamten Ablauf der NitroTPM-Attestierung. Es wird auch erläutert, was vom AWS Nitro-System generiert wird, wenn ein Bestätigungsdokument angefordert wird, und es wird erklärt, wie ein Schlüsselverwaltungsdienst ein Bestätigungsdokument verarbeiten sollte.

Themen

- Das Attestierungsdokument
- Validierung des Attestierungsdokuments

Der Zweck einer Attestierung besteht darin, anhand des Codes und der Konfiguration, die sie ausführt, nachzuweisen, dass es sich bei einer Instance um eine vertrauenswürdige Entität handelt. Die Vertrauensbasis für die Instanz liegt im AWS Nitro-System, das Bescheinigungsdokumente bereitstellt.

Bescheinigungsdokumente werden von der AWS Nitro Attestation Public Key Infrastructure (PKI) signiert, zu der auch eine veröffentlichte Zertifizierungsstelle gehört, die in jeden Dienst integriert werden kann.

Das Attestierungsdokument

Attestierungsdokumente werden in Concise Binary Object Representation (CBOR) codiert und mit CBOR Object Signing and Encryption (COSE) signiert.

Weitere Informationen zu CBOR finden Sie unter RFC 8949: Concise Binary Object Representation (CBOR).

Spezifikation des Attestierungsdokuments

Im Folgenden wird die Struktur eines Attestierungsdokuments gezeigt.

```
AttestationDocument = {
    module_id: text,                    ; issuing Nitro hypervisor module ID
    timestamp: uint .size 8,            ; UTC time when document was created, in
                                        ; milliseconds since UNIX epoch
    digest: digest,                     ; the digest function used for calculating the
                                        ; register values
    nitrotpm_pcrs: { + index => pcr },  ; map of PCRs at the moment the Attestation
 Document was generated
    certificate: cert,                  ; the public key certificate for the public
 key
                                        ; that was used to sign the Attestation
 Document
    cabundle: [* cert],                 ; issuing CA bundle for infrastructure
 certificate
    ? public_key: user_data,            ; an optional DER-encoded key the attestation
                                        ; consumer can use to encrypt data with
    ? user_data: user_data,             ; additional signed user data, defined by
 protocol
    ? nonce: user_data,                 ; an optional cryptographic nonce provided by
 the
                                        ; attestation consumer as a proof of
 authenticity
}

cert = bytes .size (1..1024)       ; DER encoded certificate
user_data = bytes .size (0..1024)
pcr = bytes .size (32/48/64)       ; PCR content
index = 0..31
digest = "SHA384"
```

Die optionalen Parameter im Attestierungsdokument (`public_key`, `user_data` und `nonce`) können verwendet werden, um ein benutzerdefiniertes Validierungsprotokoll zwischen einer attestierbaren Instance und dem externen Service einzurichten.

Validierung des Attestierungsdokuments

Wenn Sie ein Attestierungsdokument vom Nitro Hypervisor anfordern, erhalten Sie einen binären Blob, der das signierte Attestierungsdokument enthält. Das signierte Attestierungsdokument ist ein CBOR-kodiertes, COSE-signiertes Objekt (unter Verwendung der Cose_Sign1-Signaturstruktur). Der gesamte Validierungsprozess umfasst die folgenden Schritte:

1. Dekodieren Sie das CBOR-Objekt und ordnen Sie es einer COSE_Sign1-Struktur zu.
2. Extrahieren Sie das Attestierungsdokument aus der COSE_Sign1-Struktur.
3. Überprüfen Sie die Zertifikatskette.
4. Stellen Sie sicher, dass das Attestierungssdokument ordnungsgemäß signiert ist.

Bescheinigungsdokumente werden von der AWS Nitro Attestation PKI signiert, die ein Stammzertifikat für die kommerziellen Partitionen enthält. AWS Das Stammzertifikat kann von https://aws-nitro-enclaves.amazonaws.com//AWS_NitroEnclaves_Root-G1.zip heruntergeladen und mit dem folgenden Fingerabdruck verifiziert werden.

```
64:1A:03:21:A3:E2:44:EF:E4:56:46:31:95:D6:06:31:7E:D7:CD:CC:3C:17:56:E0:98:93:F3:C6:8F:79:BB:5B
```

Das Stammzertifikat basiert auf einem AWS Certificate Manager privaten Schlüssel der Private Certificate Authority (AWS Private CA) und hat eine Lebensdauer von 30 Jahren. Der Betreff des PCA hat das folgende Format:

```
CN=aws.nitro-enclaves, C=US, O=Amazon, OU=AWS
```

Themen

- COSE und CBOR
- Semantische Validität
- Zertifikatsgültigkeit
- Gültigkeitsdauer der Zertifikatskette

COSE und CBOR

Normalerweise wird die COSE_Sign1-Signaturstruktur verwendet, wenn nur eine Signatur auf einer Nachricht platziert werden soll. Die Parameter, die sich mit dem Inhalt und der Signatur befassen, werden im geschützten Header platziert, anstatt die Trennung von COSE_Sign zu haben. Die Struktur kann entweder mit oder ohne Tags kodiert werden, je nachdem, in welchem Kontext sie verwendet wird. Eine mit COSE_Sign1 markierte Struktur wird durch das CBOR-Tag 18 identifiziert.

Das CBOR-Objekt, das den Hauptteil, die Signatur und die Informationen über den Hauptteil und die Signatur enthält, wird als COSE_Sign1-Struktur bezeichnet. Die COSE_Sign1-Struktur ist ein CBOR-Array. Das Array enthält die folgenden Felder:

```
[
  protected:   Header,
  unprotected: Header,
  payload:     This field contains the serialized content to be signed,
  signature:   This field contains the computed signature value.
]
```

Im Kontext eines Attestierungsdokuments umfasst das Array Folgendes.

```
18(/* COSE_Sign1 CBOR tag is 18 */
    {1: -35}, /* This is equivalent with {algorithm: ECDS 384} */
    {}, /* We have nothing in unprotected */
    $ATTESTATION_DOCUMENT_CONTENT /* Attestation Document */,
    signature /* This is the signature */
)
```

Weitere Informationen zu CBOR finden Sie unter RFC 8949: Concise Binary Object Representation (CBOR).

Semantische Validität

Das CA-Paket eines Attestierungsdokuments wird immer in der folgenden Reihenfolge aufgeführt.

```
[ ROOT_CERT - INTERM_1 - INTERM_2 .... - INTERM_N]
      0          1          2             N - 1
```

Beachten Sie diese Reihenfolge, da einige vorhandene Tools, wie z. B. das von Java CertPath aus dem Java PKI API Programmer's Guide, möglicherweise eine andere Reihenfolge erfordern.

Um die Zertifikate zu validieren, beginnen Sie mit dem CA-Paket des Attestierungsdokuments und generieren Sie die erforderliche Kette, wobei `TARGET_CERT` das Zertifikat im Attestierungsdokument ist.

```
[TARGET_CERT, INTERM_N, ..... , INTERM_2, INTERM_1, ROOT_CERT]
```

Zertifikatsgültigkeit

Für alle Zertifikate in der Kette müssen Sie sicherstellen, dass das aktuelle Datum innerhalb des im Zertifikat angegebenen Gültigkeitszeitraums liegt.

Gültigkeitsdauer der Zertifikatskette

Im Allgemeinen kann eine Kette von mehreren Zertifikaten erforderlich sein, die aus einem Zertifikat des Besitzers des öffentlichen Schlüssels besteht, das von einer Zertifizierungsstelle signiert wurde, und aus null oder mehreren zusätzlichen Zertifikaten, die von einer anderen CAs signiert wurden. CAs Solche Ketten, die als Zertifizierungspfade bezeichnet werden, sind erforderlich, da ein Benutzer mit einem öffentlichen Schlüssel nur mit einer begrenzten Anzahl von gesicherten öffentlichen Schlüsseln der Zertifizierungsstelle initialisiert wird. Die Verfahren zur Validierung des Zertifizierungspfads für die Internet-PKI basieren auf dem in X.509 enthaltenen Algorithmus. Bei der Verarbeitung des Zertifizierungspfads wird die Bindung zwischen dem eindeutigen Namen des Antragstellers, dem alternativen Namen des and/or Antragstellers und dem öffentlichen Schlüssel des Antragstellers überprüft. Die Bindung wird durch Einschränkungen begrenzt, die in den Zertifikaten angegeben sind, die den Pfad umfassen, und durch Eingaben, die von der vertrauenden Partei angegeben werden. Die grundlegenden Einschränkungen und Erweiterungen der Richtlinieneinschränkungen ermöglichen es der Verarbeitungslogik für den Zertifizierungspfad, den Entscheidungsprozess zu automatisieren.

> **Note**
>
> CRL muss bei der Validierung deaktiviert sein.

Bei Verwendung von Java erfolgt die Kettenvalidierung, ausgehend vom Root-Pfad und der generierten Zertifikatskette, wie folgt.

```
validateCertsPath(certChain, rootCertficate) {
    /* The trust anchor is the root CA to trust */
```

```
    trustAnchors.add(rootCertificate);

    /* We need PKIX parameters to specify the trust anchors
     * and disable the CRL validation
     */
    validationParameters = new PKIXParameters(trustAnchors);
    certPathValidator = CertPathValidator.getInstance(PKIX);
    validationParameters.setRevocationEnabled(false);

    /* We are ensuring that certificates are chained correctly */
    certPathValidator.validate(certPath, validationParameters);
}
```

Integration mit AWS KMS

Ihre Instanz sollte über eine Anwendung verfügen, die AWS KMS API-Anfragen mit dem vom NitroTPM abgerufenen Bestätigungsdokument stellen kann. Wenn Sie eine Anfrage mit einem Bestätigungsdokument stellen, werden die Messungen im bereitgestellten Bestätigungsdokument AWS KMS anhand der Referenzmessungen in der KMS-Schlüsselrichtlinie validiert. Anfragen sind nur zulässig, wenn die Messungen im Attestierungsdokument mit den Referenzmaßen in der KMS-Schlüsselrichtlinie übereinstimmen.

Wenn Sie die Operationen Decrypt,, DeriveSharedSecretGenerateDataKeyGenerateDataKeyPair, oder GenerateRandomAPI mit einem Bestätigungsdokument aufrufen, APIs verschlüsseln diese den Klartext in der Antwort unter dem öffentlichen Schlüssel aus dem Bestätigungsdokument und geben Chiffretext statt Klartext zurück. Dieser Geheimtext kann nur mit dem privaten Schlüssel entschlüsselt werden, der in der Instance generiert wurde.

Weitere Informationen finden Sie in der Kryptographischen Attestierung für NitroTPM im Entwicklerhandbuch für AWS Key Management Service .

> **Note**
>
> Wenn Sie einen Service eines Drittanbieters attestieren, müssen Sie Ihre eigenen benutzerdefinierten Mechanismen für den Empfang, die Analyse und die Validierung von Attestierungsdokumenten entwickeln. Weitere Informationen finden Sie unter Ein NitroTPM-Attestierungsdokument validieren.

Isolieren Sie Daten von Ihren eigenen Bedienern

Das Nitro-System hat keinen Bedienerzugriff. AWS Es gibt keinen Mechanismus, mit dem sich ein AWS System oder eine Person bei Amazon EC2 Nitro-Hosts anmelden, auf den Speicher von EC2 Instances zugreifen oder auf Kundendaten zugreifen kann, die auf lokal verschlüsselten Instance-Speichern oder remote verschlüsselten Amazon EBS-Volumes gespeichert sind.

Bei der Verarbeitung hochsensibler Daten könnten Sie erwägen, den Zugriff auf diese Daten einzuschränken, indem Sie verhindern, dass auch Ihre eigenen Operatoren auf die Instance zugreifen. EC2

Sie können benutzerdefinierte Attestable erstellen, die so konfiguriert sind AMIs , dass sie eine isolierte Computerumgebung bereitstellen. Die AMI-Konfiguration hängt von Ihrer Workload und Ihren Anwendungsanforderungen ab. Beachten Sie diese bewährten Methoden, wenn Sie Ihr AMI zum Erstellen einer isolierten Rechenumgebung erstellen.

- Entfernen Sie jeglichen interaktiven Zugriff, um zu verhindern, dass Ihre Bediener oder Benutzer auf die Instance zugreifen.
- Stellen Sie sicher, dass nur vertrauenswürdige Software und vertrauenswürdiger Code im AMI enthalten sind.
- Konfigurieren Sie eine Netzwerk-Firewall innerhalb der Instance, um den Zugriff zu blockieren.
- Schreibgeschützten und unveränderlichen Status für alle Speicher- und Dateisysteme sicherstellen.
- Beschränken Sie den Instance-Zugriff auf authentifizierte, autorisierte und protokollierte API-Aufrufe.

Attestable, die keinen interaktiven Zugriff haben AMIs , werden aktualisiert

Sobald Sie eine Instance mit einem AMI für eine isolierte Rechenumgebung gestartet haben, kann kein Benutzer oder Bediener eine Verbindung zu der Instance herstellen. Das bedeutet, dass es nach dem Start keine Möglichkeit gibt, Software auf der Instance zu installieren oder zu aktualisieren.

Wenn neue Software oder ein Softwareupdate erforderlich ist, müssen Sie ein neues attestierbares AMI erstellen, das die erforderliche Software oder Softwareupdates enthält. Verwenden Sie dann dieses AMI, um eine neue Instance zu starten oder um ein Root-Volume auf der ursprünglichen Instance zu ersetzen. Alle am AMI vorgenommenen Softwareänderungen führen dazu, dass ein neuer Hash generiert wird.

Die folgenden Maßnahmen führen zu einer Änderung der Referenzmessungen im NitroTPM-Attestierungsdokument:

- Anhalten und Starten einer Instance, die mit einem attestierbaren AMI gestartet wurde
- Einen Root-Volume-Ersatz mit einem anderen AMI durchführen

Wenn Sie eine dieser Aktionen durchführen, müssen Sie anschließend Ihren Attestierungsservice mit den neuen Referenzmessungen aktualisieren. Beispielsweise müssen Sie Ihre KMS-Schlüsselrichtlinie auf die neuen Referenzmessungen aktualisieren, wenn Sie diese AWS KMS für Bescheinigungen verwenden.

Eine Instance behält ihr NitroTPM-Schlüsselmaterial für den gesamten Instance-Lebenszyklus bei und setzt sie auch während des Austauschs von Root-Volumes stop/starts fort.

Credential Guard für Windows-Instances

Das AWS Nitro-System unterstützt Credential Guard für Amazon Elastic Compute Cloud (Amazon EC2) Windows-Instances. Credential Guard ist ein virtualisierungsbasiertes Windows-Sicherheitsfeature (VBS), die die Erstellung isolierter Umgebungen ermöglicht, um Sicherheitsressourcen wie Windows-Benutzeranmeldeinformationen und die Durchsetzung der Codeintegrität über den Windows-Kernelschutz hinaus zu schützen. Wenn Sie EC2 Windows-Instances ausführen, verwendet Credential Guard das AWS Nitro-System, um zu verhindern, dass Windows-Anmeldeinformationen aus dem Speicher des Betriebssystems extrahiert werden.

Inhalt

- Voraussetzungen
- Unterstützte Instance starten
- Speicherintegrität deaktivieren
- Credential Guard anschalten
- Überprüfen, ob Credential Guard ausgeführt wird

Voraussetzungen

Ihre Windows-Instance muss die folgenden Voraussetzungen erfüllen, um Credential Guard verwenden zu können.

Amazon-Maschinenbilder (AMIs)

Das AMI muss vorkonfiguriert sein, um NitroTPM und UEFI Secure Boot zu aktivieren. Weitere Informationen zur Unterstützung finden AMIs Sie unterthe section called “Voraussetzungen”.

Speicherintegrität

Speicherintegrität, auch bekannt als Hypervisor-Protected Code Integrity (HVCI) oder Hypervisor Enforced Code Integrity, wird nicht unterstützt. Bevor Sie Credential Guard aktivieren, müssen Sie sicherstellen, dass dieses Feature deaktiviert ist. Weitere Informationen finden Sie unter Speicherintegrität deaktivieren.

Instance-Typen

Die folgenden Instance-Typen unterstützen Credential Guard in allen Größen, sofern nicht anders notiert: `C5`, `C5d`, `C5n`, `C6i`, `C6id`, `C6in`, `C7i`, `C7i-flex`, `M5`, `M5d`, `M5dn`, `M5n`, `M5zn`, `M6i`, `M6id`, `M6idn`, `M6in`, `M7i`, `M7i-flex`, `R5`, `R5b`, `R5d`, `R5dn`, `R5n`, `R6i`, `R6id`, `R6idn`, `R6in` `R7i`, `R7iz`, `T3`.

> **Note**
>
> - NitroTPM hat zwar einige erforderliche Instance-Typen gemeinsam, aber der Instance-Typ muss einer der oben genannten sein, um Credential Guard zu unterstützen.
> - Credential Guard wird für Folgendes nicht unterstützt:
>   - Bare-Metal-Instances.
>   - Die folgenden Instance-Typen unterstützen EFAs: `C7i.48xlarge`, `M7i.48xlarge` und `R7i.48xlarge`.

Weitere Informationen zu Instance-Typen finden Sie im Amazon EC2 Instance Types Guide.

Unterstützte Instance starten

Sie können die EC2 Amazon-Konsole oder AWS Command Line Interface (AWS CLI) verwenden, um eine Instance zu starten, die Credential Guard unterstützt. Sie benötigen zum Starten Ihrer Instance eine kompatible AMI-ID, die für jede AWS-Region eindeutig ist.

> **Tip**
>
> Sie können den folgenden Link verwenden, um Instances mit kompatiblem Amazon zu finden und zu starten, die AMIs in der EC2 Amazon-Konsole bereitgestellt werden: https://console.aws.amazon.com/ec2/v2/home?#Images:visibility=public-images;v=3;search=:TPM-Windows_Server;ownerAlias=amazon

Console

So starten Sie eine Instance

Befolgen Sie die Schritte zum Starten einer Instance, während Sie einen unterstützten Instance-Typ und ein vorkonfiguriertes Windows-AMI angeben.

AWS CLI

So starten Sie eine Instance

Verwenden Sie den run-instances-Befehl, um eine Instance mit einem unterstützten Instance-Typ und einem vorkonfigurierten Windows-AMI zu starten.

```
aws ec2 run-instances \
    --image-id resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-English-Full-Base \
    --instance-type c6i.large \
    --region us-east-1 \
    --subnet-id subnet-0abcdef1234567890
    --key-name key-name
```

PowerShell

So starten Sie eine Instance

Verwenden Sie den New-EC2Instance-Befehl, um eine Instance mit einem unterstützten Instance-Typ und einem vorkonfigurierten Windows-AMI zu starten.

```
New-EC2Instance `
    -ImageId resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-English-Full-Base `
```

```
    -InstanceType c6i.large `
    -Region us-east-1 `
    -SubnetId subnet-0abcdef1234567890 `
    -KeyName key-name
```

Speicherintegrität deaktivieren

Sie können den Editor für lokale Gruppenrichtlinien verwenden, um die Speicherintegrität in unterstützten Szenarios zu deaktivieren. Die folgenden Richtlinien können für jede Konfigurationseinstellung unter Virtualisierungsbasierter Schutz der Code-Integrität angewendet werden:

- Ohne Sperre aktiviert – Ändern Sie die Einstellung auf Deaktiviert, um die Speicherintegrität zu deaktivieren.
- Mit UEFI-Sperre aktiviert – Die Speicherintegrität wurde mit UEFI-Sperre aktiviert. Die Speicherintegrität kann nicht deaktiviert werden, nachdem sie mit der UEFI-Sperre aktiviert wurde. Wir empfehlen, eine neue Instance mit deaktivierter Speicherintegrität zu erstellen und die nicht unterstützte Instance zu beenden, wenn sie nicht verwendet wird.

So deaktivieren Sie die Speicherintegrität mit dem Editor für lokale Gruppenrichtlinien

1. Stellen Sie über das Remote Desktop Protocol (RDP) als Benutzerkonto mit Administratorrechten eine Verbindung zu Ihrer Instance her. Weitere Informationen finden Sie unter the section called “Verbindung mit einem RDP-Client herstellen”.
2. Öffnen Sie das Startmenü und suchen Sie nach **cmd**, um eine Eingabeaufforderung zu starten.
3. Führen Sie den folgenden Befehl aus, um den Editor für lokale Gruppenrichtlinien zu öffnen: `gpedit.msc`
4. Wählen Sie im Editor für lokale Gruppenrichtlinien Computerkonfiguration, Administrative Vorlagen, System, Geräteschutz aus.
5. Wählen Sie Virtualisierungsbasierte Sicherheit aktivieren und dann Richtlinieneinstellung bearbeiten aus.
6. Öffnen Sie das Dropdownmenü mit den Einstellungen für Virtualisierungsbasierter Schutz der Codeintegrität, wählen Sie Deaktiviert und anschließend Anwenden.
7. Starten Sie die Instance neu, um die Änderungen zu übernehmen.

Credential Guard anschalten

Nachdem Sie eine Windows-Instance mit einem unterstützten Instance-Typ und einem kompatiblen AMI gestartet und bestätigt haben, dass die Speicherintegrität deaktiviert ist, können Sie Credential Guard aktivieren.

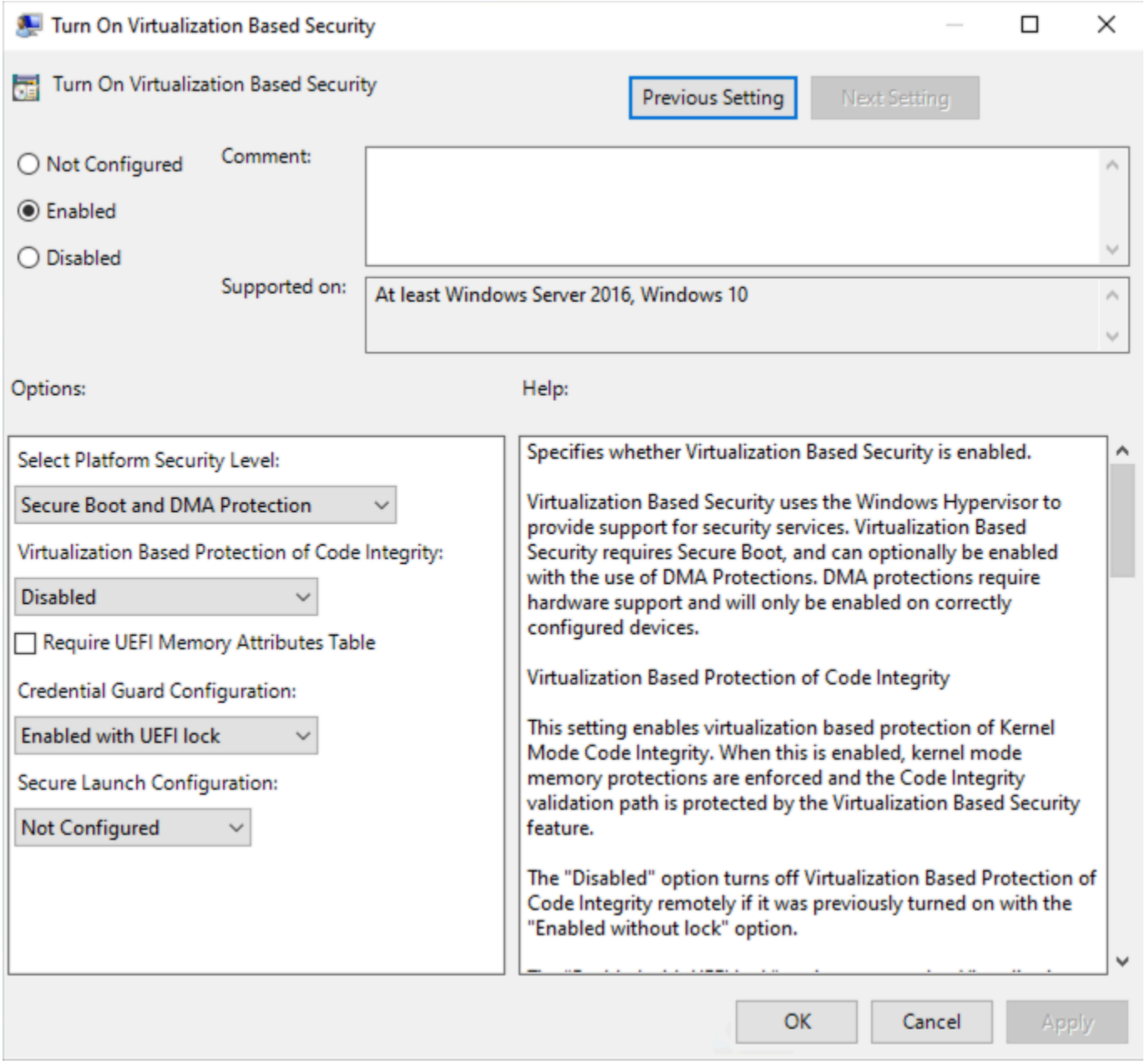
> **Important**
>
> Sie benötigen Administratorrechte, um die folgenden Schritte zum Aktivieren von Credential Guard auszuführen.

Aktivieren von Credential Guard

1. Stellen Sie über das Remote Desktop Protocol (RDP) als Benutzerkonto mit Administratorrechten eine Verbindung zu Ihrer Instance her. Weitere Informationen finden Sie unter the section called “Verbindung mit einem RDP-Client herstellen”.
2. Öffnen Sie das Startmenü und suchen Sie nach **`cmd`**, um eine Eingabeaufforderung zu starten.
3. Führen Sie den folgenden Befehl aus, um den Editor für lokale Gruppenrichtlinien zu öffnen: `gpedit.msc`
4. Wählen Sie im Editor für lokale Gruppenrichtlinien Computerkonfiguration, Administrative Vorlagen, System, Geräteschutz aus.
5. Wählen Sie Virtualisierungsbasierte Sicherheit aktivieren und dann Richtlinieneinstellung bearbeiten aus.
6. Wählen Sie Aktiviert im Menü Virtualisierungsbasierte Sicherheit aktivieren aus.
7. Wählen Sie unter Plattformsicherheitsstufe auswählen die Optionen Sicherer Start und DMA-Schutz aus.
8. Wählen Sie für Credential-Guard-Konfiguration die Option Aktiviert mit UEFI-Sperre aus.

   > **Note**
   >
   > Die verbleibenden Richtlinieneinstellungen sind nicht erforderlich, um Credential Guard zu aktivieren, und können auf Nicht konfiguriert belassen werden.

   Das folgende Image zeigt die wie zuvor beschrieben konfigurierten VBS-Einstellungen:



9. Starten Sie die Instance neu, um die Einstellungen zu übernehmen.

Überprüfen, ob Credential Guard ausgeführt wird

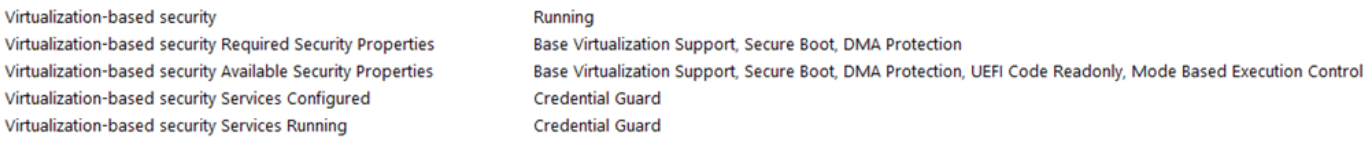
Sie können das Microsoft-Tool Systeminformationen (`Msinfo32.exe`) verwenden, um zu bestätigen, dass Credential Guard ausgeführt wird.

> **Important**
>
> Sie müssen die Instance zuerst neu starten, um die Anwendung der Richtlinieneinstellungen abzuschließen, die zum Aktivieren von Credential Guard erforderlich sind.

So überprüfen Sie, ob Credential Guard ausgeführt wird

1. Stellen Sie über das Remote Desktop Protocol (RDP) eine Verbindung zu Ihrer Instance her. Weitere Informationen finden Sie unter the section called “Verbindung mit einem RDP-Client herstellen”.
2. Öffnen Sie innerhalb der RDP-Sitzung zu Ihrer Instance das Startmenü und suchen Sie nach **`cmd`**, um eine Eingabeaufforderung zu starten.
3. Öffnen Sie die Systeminformationen, indem Sie den folgenden Befehl ausführen: `msinfo32.exe`
4. Das Microsoft-Tool Systeminformationen listet die Details zur VBS-Konfiguration auf. Bestätigen Sie neben virtualisierungsbasierte Sicherheitsservices, dass Credential Guard als Wird ausgeführt angezeigt wird.

   Das folgende Image zeigt, dass VBS wie zuvor beschrieben ausgeführt wird:



Greifen EC2 Sie über einen VPC-Endpunkt mit Schnittstelle auf Amazon zu

Sie können die Sicherheitslage Ihrer VPC verbessern, indem Sie eine private Verbindung zwischen Ressourcen in Ihrer VPC und der EC2 Amazon-API herstellen. Sie können auf die EC2 Amazon-API zugreifen, als wäre sie in Ihrer VPC, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder Direct Connect eine Verbindung verwenden zu müssen. EC2 Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um auf die EC2 Amazon-API zuzugreifen.

Weitere Informationen finden Sie AWS PrivateLink im AWS PrivateLink Leitfaden unter Zugriff AWS-Services durch.

Inhalt

- Erstellen eines Schnittstellen-VPC-Endpunkts
- Erstellen einer Endpunktrichtlinie

Erstellen eines Schnittstellen-VPC-Endpunkts

Erstellen Sie einen Schnittstellenendpunkt für Amazon EC2 mit dem folgenden Servicenamen:

- com.amazonaws. ***region***.ec2 — Erzeugt einen Endpunkt für die EC2 Amazon-API-Aktionen.

Weitere Informationen finden Sie im AWS PrivateLink Handbuch unter Zugreifen und AWS-Service Verwenden eines Schnittstellen-VPC-Endpunkts.

Erstellen einer Endpunktrichtlinie

Eine Endpunktrichtlinie ist eine IAM-Ressource, die Sie Ihrem Schnittstellen-Endpunkt anfügen können. Die standardmäßige Endpunktrichtlinie ermöglicht den vollen Zugriff auf die EC2 Amazon-API über den Schnittstellenendpunkt. Um den Zugriff auf die EC2 Amazon-API von Ihrer VPC aus zu kontrollieren, fügen Sie dem Schnittstellenendpunkt eine benutzerdefinierte Endpunktrichtlinie hinzu.

Eine Endpunktrichtlinie gibt die folgenden Informationen an:

- Die Prinzipale, die Aktionen ausführen können.
- Die Aktionen, die ausgeführt werden können.
- Die Ressource, auf der die Aktionen ausgeführt werden können.

> **Important**
>
> Wenn eine nicht standardmäßige Richtlinie auf einen VPC-Schnittstellen-Endpunkt für Amazon angewendet wird EC2, werden bestimmte fehlgeschlagene API-Anfragen, z. B. solche, die von fehlschlagen`RequestLimitExceeded`, möglicherweise nicht bei Amazon protokolliert. AWS CloudTrail CloudWatch

Weitere Informationen finden Sie unter Steuern des Zugriffs auf Services mit Endpunktrichtlinien im AWS PrivateLink -Leitfaden.

Das folgende Beispiel zeigt eine VPC-Endpunktrichtlinie, die die Berechtigung zum Erstellen unverschlüsselter Volumes oder zum Starten von Instances mit unverschlüsselten Volumes ablehnt. Die Beispielrichtlinie gewährt auch die Erlaubnis, alle anderen EC2 Amazon-Aktionen durchzuführen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Action": "ec2:*",
        "Effect": "Allow",
        "Resource": "*",
        "Principal": "*"
    },
    {
        "Action": [
            "ec2:CreateVolume"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    },
    {
        "Action": [
            "ec2:RunInstances"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    }]
}
```

Speicheroptionen für Ihre Amazon-EC2-Instances

Amazon EC2 bietet flexible, kostengünstige und benutzerfreundliche Datenspeicheroptionen für Ihre Instances. Jede Option bietet eine einzigartige Kombination von Leistungs- und Beständigkeitsmerkmalen. Diese Speicheroptionen können Ihren Anforderungen entsprechend unabhängig voneinander oder kombiniert verwendet werden.

Blockspeicher

- Amazon EBS – Amazon EBS bietet Volumes für einen dauerhaften Speicher auf Blockebene, die Sie einer Instance anfügen und von dieser trennen können. Sie können einer Instance mehrere EBS-Volumes zuordnen. Ein EBS-Volume bleibt unabhängig von der Betriebsdauer der zugeordneten Instance erhalten. Sie können Ihre EBS-Volumes verschlüsseln. Sie können eine Sicherungskopie Ihrer Daten anfertigen, indem Sie Snapshots von Ihren EBS-Volumes erstellen. Snapshots werden in Amazon S3 gespeichert. Sie können ein EBS-Volume aus einem Snapshot erstellen.
- Instance-Speicher temporärer Speicher auf Blockebene für EC2-Instances – Der Instance-Speicher stellt temporären Speicher auf Blockebene für Instances bereit. Anzahl, Größe und Typ der Instance-Speicher-Volumes werden durch den Instance-Typ und die Instance-Größe bestimmt. Die Daten auf einem Instance-Speicher-Volume bleiben nur während der Nutzungsdauer der zugewiesenen Instance erhalten; wenn Sie eine Instance anhalten, in den Ruhezustand versetzen oder beenden, gehen alle Daten auf den Instance-Speicher-Volumes verloren.

Objektspeicher

- Amazon S3 – Amazon S3 bietet Zugriff auf eine zuverlässige und kostengünstige Datenspeicher-Infrastruktur. Es ist darauf ausgelegt, die Webskalierung der Rechenleistung zu erleichtern, indem es Ihnen ermöglicht, jede beliebige Datenmenge jederzeit über Amazon EC2 oder das Internet zu speichern und abzurufen. Sie können Amazon S3 beispielsweise verwenden, um Backup-Kopien Ihrer Daten und Anwendungen zu speichern. Amazon EC2 verwendet Amazon S3, um EBS-Snapshots und Amazon-S3-gestützte AMIs zu speichern.

Dateispeicherung

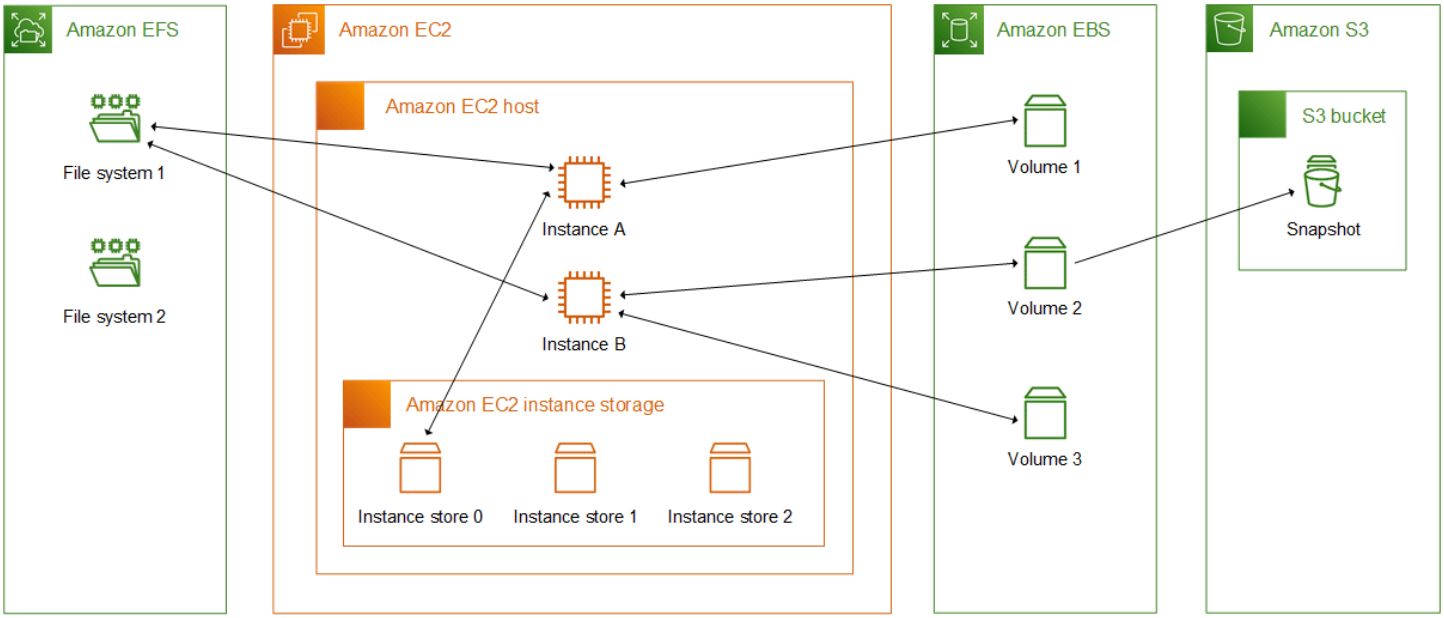
- Amazon EFS (Linux-Instances) – Amazon EFS bietet skalierbaren Dateispeicher für die Verwendung mit Amazon EC2. Sie können ein EFS-Dateisystem erstellen und Ihre Instances so konfigurieren, dass das Dateisystem gemountet wird. Sie können ein EFS-Dateisystem als gemeinsame Datenquelle für Workloads und Anwendungen verwenden, die jeweils auf mehr als einer Instance ausgeführt werden.

- Amazon FSx – Mit Amazon FSx können Sie leistungsstarke Dateisysteme mit reichhaltigem Feature-Umfang in der Cloud starten, ausführen und skalieren. Amazon FSx ist ein vollständig verwalteter Service, der eine Vielzahl von Workloads unterstützt. Sie können zwischen diesen weitverbreiteten Dateisystemen wählen: Lustre, NetApp ONTAP, OpenZFS und Windows File Server.

Datei-Caching

- Amazon File Cache mit Amazon-EC2-Instances verwenden – Amazon File Cache bietet temporären Hochleistungs-Cache in AWS für die Verarbeitung von Dateidaten. Der Cache bietet Lese- und Schreibdatenzugriff auf Datenverarbeitungs-Workloads auf Amazon EC2 mit Latenzen unter einer Millisekunde, einem Durchsatz von bis zu Hunderten von GB/s und bis zu Millionen von IOPS.

Im folgenden Image ist die Beziehung zwischen diesen Speicheroptionen und Ihrer Instance dargestellt.



AWS-Speicherpreise

Öffnen Sie AWS-Preise, scrollen Sie zu Preise für AWS-Produkte und wählen Sie Speicher. Wählen Sie das Speicherprodukt aus, um die entsprechende Preisseite zu öffnen.

Persistenter Amazon EBS-Blockspeicher für Amazon-Instances EC2

Amazon Elastic Block Store (Amazon EBS) bietet skalierbare, leistungsstarke Blockspeicherressourcen, die mit EC2 Amazon-Instances verwendet werden können. Mit Amazon EBS können Sie die folgenden Blockspeicherressourcen erstellen und verwalten:

- Amazon EBS-Volumes — Dies sind Speichervolumes, die Sie EC2 Amazon-Instances zuordnen. Nachdem Sie einer Instance ein Volume angefügt haben, können Sie es genauso verwenden wie Blockspeicher. Die Instance kann mit dem Volume wie mit einem lokalen Laufwerk interagieren.
- Amazon EBS-Snapshots — Dies sind point-in-time Backups von Amazon EBS-Volumes, die unabhängig vom Volume selbst bestehen bleiben. Sie können Snapshots erstellen, um die Daten auf Ihren Amazon-EBS-Volumes zu sichern. Sie können dann jederzeit neue Volumes aus diesen Snapshots wiederherstellen.

Sie können während des Starts EBS-Volumes erstellen und an eine Instance anhängen, und Sie können EBS-Volumes jederzeit nach dem Start erstellen und an eine Instance anhängen. Sie können auch die Größe oder Leistung Ihrer EBS-Volumes erhöhen, ohne das Volume zu trennen oder Ihre Instance neu zu starten.

Sie können EBS-Snapshots jederzeit nach der Erstellung von einem EBS-Volume erstellen. Sie können EBS-Schnappschüsse verwenden, um die auf Ihren Volumes gespeicherten Daten zu sichern. Sie können diese Snapshots dann verwenden, um Volumes sofort wiederherzustellen oder Daten zwischen AWS-Konten AWS Regionen oder Availability Zones zu migrieren. Sie können Amazon Data Lifecycle Manager verwenden oder AWS Backup um die Erstellung, Aufbewahrung und Löschung Ihrer EBS-Snapshots zu automatisieren.

Ein verwaltetes EBS-Volume wird von einem Serviceanbieter wie Amazon EKS Auto Mode verwaltet. Sie können die Einstellungen eines verwalteten EBS-Volumes nicht direkt ändern. Verwaltete EBS-Volumes werden durch einen Wahr-Wert im Feld Verwaltet identifiziert. Weitere Informationen finden Sie unter Verwaltete Amazon-EC2-Instances.

Weitere Informationen über die Verwendung von Volumes und Snapshots finden Sie im Amazon-EBS-Benutzerhandbuch.

Amazon EBS-Volumenlimits für Amazon-Instances EC2

Die maximale Anzahl von Amazon-EBS-Volumes, die Sie einer Instance anfügen können, hängt vom Instance-Typ und der Instance-Größe ab. Wenn Sie das Limit für Volume-Anhänge für eine Instance überschreiten, schlägt die Anhangsanforderung mit dem Fehler `AttachmentLimitExceeded` fehl.

Wenn Sie überlegen, wie viele Volumes Sie Ihrer Instance zuordnen möchten, sollten Sie berücksichtigen, ob Sie eine höhere I/O Bandbreite oder eine höhere Speicherkapazität benötigen.

Bandbreite vs. Kapazität

Für konsistente und vorhersehbare Bandbreitennutzungsfälle sollten Sie Amazon-EBS-optimierte Instances mit Allzweck-SSD-Volumes oder Bereitgestellte-IOPS-SSD-Volumes verwenden. Für maximale Leistung passen Sie die IOPS, die Sie für Ihre Volumes bereitgestellt haben, an die für Ihren Instance-Typ verfügbare Bandbreite an.

Bei RAID-Konfigurationen stellen Sie möglicherweise fest, dass Arrays, die größer als 8 Volumes sind, aufgrund des erhöhten I/O Overheads eine geringere Leistung aufweisen. Testen Sie die Leistung der einzelnen Anwendungen und nehmen Sie entsprechende Abstimmungen vor.

Inhalt

- Volume-Limits für Instances, die auf dem Nitro-System basieren
  - Dediziertes EBS-Volume-Limit
  - Gemeinsames EBS-Volume-Limit
- Volume-Limits für Xen-basierte Instances
  - Linux-Instances
  - Windows-Instances

Volume-Limits für Instances, die auf dem Nitro-System basieren

Die Volume-Limits für Instances, die auf dem Nitro-System basieren, hängen vom Instance-Typ ab. Einige Nitro-Instance-Typen haben ein dediziertes EBS-Volume-Limit, während die meisten ein gemeinsames Volume-Limit haben. Die Limits für Volume-Anhänge für jeden Instance-Typ finden Sie im Folgenden:

- Amazon-EBS-Spezifikationen – Allzweck
- Amazon-EBS-Spezifikationen – Für Datenverarbeitung optimiert

- Amazon-EBS-Spezifikationen – Arbeitsspeicheroptimiert
- Amazon-EBS-Spezifikationen – Speicheroptimiert
- Amazon-EBS-Spezifikationen – Beschleunigte Datenverarbeitung
- Amazon-EBS-Spezifikationen – Hochleistungs-Datenverarbeitung
- Amazon-EBS-Spezifikationen – Vorherige Generation

Dediziertes EBS-Volume-Limit

Für die folgenden Nitro-Instance-Typen gilt je nach Instance-Größe ein dediziertes EBS-Volumenlimit, abhängig von der Größe der Instance. Das Limit wird nicht mit anderen Geräteanhängen geteilt. Mit anderen Worten, Sie können eine beliebige Anzahl von EBS-Volumes bis zum Limit für Volumenanhänge anhängen, unabhängig von der Anzahl der angeschlossenen Geräte, wie z. B. NVMe Instance-Speicher-Volumes und Netzwerkschnittstellen.

- Allzweck: M7a | M7i | M7i-flex | M8a | M8g | M8gd | M8i | M8i-flex
- Für Datenverarbeitung optimiert: C7a | C7i | C7i-Flex | C8a | C8g | C8GB | C8GD | C8Gn | C8i | C8i-Flex
- Speicheroptimiert: R7a | R7i | R7iZ | R8a | R8G | R8GB | R8GD | R8Gn | R8i | R8i-Flex | U7i-6TB | U7i-8TB | U7i-12TB | U7in-16 TB | U7in-24 TB | U7in-32 TB | U7in-32 TB | x8AEDZ
- Speicheroptimiert: I7i | I7ie | I8g | I8ge
- Beschleunigtes Rechnen: F2 | G6 | G6e | G6f | Gr6 | Gr6f | P4d | P4de | P5 | P5e | P5en | P6-B200 | P6-B300 | GB2 P6e-00 | Trn2 | Trn2u
- Hochleistungs-Datenverarbeitung Hpc7a

Gemeinsames EBS-Volume-Limit

Alle anderen Nitro-Instance-Typen (nicht aufgeführt unterDediziertes EBS-Volume-Limit) haben ein Limit für Volumenanhänge, das von Amazon EBS-Volumes, Netzwerkschnittstellen und NVMe Instance-Speicher-Volumes gemeinsam genutzt wird. Sie können eine beliebige Anzahl von Amazon EBS-Volumes bis zu diesem Limit anhängen, abzüglich der Anzahl der angeschlossenen Netzwerkschnittstellen und NVMe Instance-Speicher-Volumes. Beachten Sie, dass jede Instance über mindestens eine Netzwerkschnittstelle verfügen muss und dass NVMe Instance-Speicher-Volumes beim Start automatisch angehängt werden.

Die meisten Nitro-Instances unterstützen maximal 28 Anhänge. In den folgenden Beispielen wird gezeigt, wie berechnet wird, wie viele EBS-Volumes Sie anfügen können.

Beispiele

- Mit einer `m5.xlarge`-Instance, die nur über die primäre Netzwerkschnittstelle verfügt, können Sie 27 EBS-Volumes anhängen.

  28 Volumes – 1 Netzwerkschnittstelle = 27
- Mit einer `m5.xlarge`-Instance mit zwei zusätzlichen Netzwerkschnittstellen können Sie 25 EBS-Volumes anhängen.

  28 Volumes – 3 Netzwerkschnittstellen = 25
- Mit einer `m5d.xlarge`-Instance mit zwei zusätzlichen Netzwerkschnittstellen können Sie 24 EBS-Volumes anhängen.

  28 Volumes — 3 Netzwerkschnittstellen — 1 NVMe Instance-Speicher-Volume = 24

Volume-Limits für Xen-basierte Instances

Die Volumenbeschränkungen für XEN-basierte Instances wie T2 hängen vom Betriebssystem ab.

Weitere Informationen erhalten Sie unter Xen-basierte Instances.

Linux-Instances

Das Anfügen von mehr als 40 Volumes an eine Xen-basierte Linux-Instance kann zu Startfehlern führen. Diese Zahl umfasst das Root-Volume sowie alle angefügten Instance-Speicher-Volumes und Amazon-EBS-Volumes.

Wenn bei einer Instance mit einer großen Anzahl von Volumes Startprobleme auftreten, beenden Sie die Instance, trennen Sie alle Volumes, die für den Startvorgang nicht unbedingt erforderlich sind, starten Sie die Instance und fügen Sie die Volumes nach der Ausführung der Instance wieder an.

> **Important**
>
> Das Anfügen von mehr als 40 Volumes an eine Xen-basierte Linux-Instance wird nur nach bestem Bemühen unterstützt und kann nicht garantiert werden.

Windows-Instances

Die folgende Tabelle zeigt die Volume-Limits für Xen-basierte Windows-Instances basierend auf dem verwendeten Treiber. Diese Zahlen beinhalten das Root-Volume sowie alle angefügten Instance-Speicher-Volumes und Amazon-EBS-Volumes.

Treiber	Volume-Limit
AWS PV	26
Citrix PV	26
Red Hat PV	17

Wir empfehlen, nicht mehr als 26 Volumes an eine Xen-basierte Windows-Instanz mit AWS PV- oder Citrix PV-Treibern anzuhängen, da dies zu Leistungsproblemen führen kann. Informationen zur Ermittlung der PV-Treiber, die Ihre Instance verwendet, oder zum Upgrade Ihrer Windows-Instance von Red-Hat- auf Citrix-PV-Treiber finden Sie unter the section called “Upgrade für PV-Treiber”.

> **Important**
>
> Das Anfügen von mehr als der folgenden Anzahl von Volumes an eine Xen-basierte Windows-Instance wird nur nach bestem Bemühen unterstützt und kann nicht garantiert werden.

Weitere Informationen darüber, wie Gerätenamen mit Volumes verbunden sind, finden Sie unter Volumes für Amazon-EC2-Windows-Instances anhängen und zuordnen.

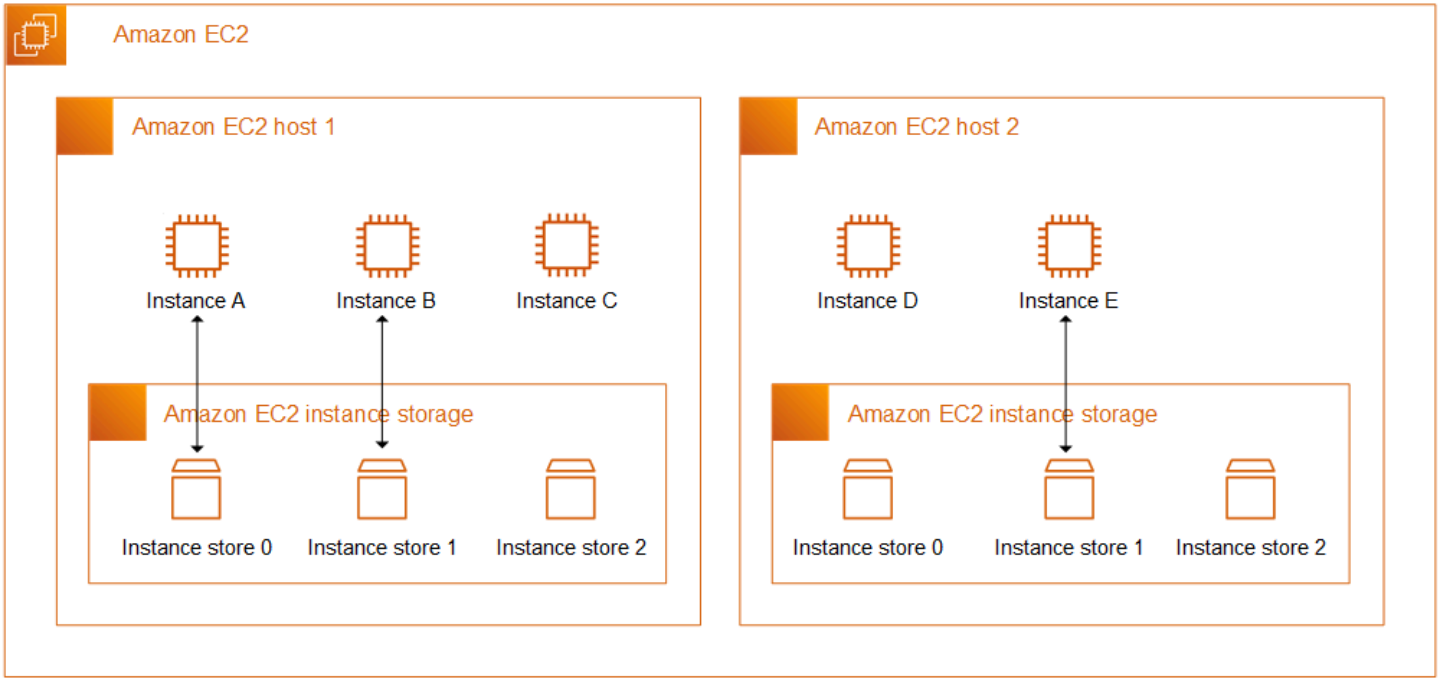
Instance-Speicher temporärer Speicher auf Blockebene für EC2-Instances

Ein Instance-Speicher stellt für Ihre EC2-Instance temporären Speicher auf Blockebene bereit. Dieser Speicher wird von Laufwerken bereitgestellt, die physisch mit dem Host-Computer verbunden sind. Der Instance-Speicher ist ideal für die temporäre Speicherung von Informationen, die sich häufig ändern, wie Puffer, Caches, Arbeitsdaten und andere temporäre Inhalte. Es kann auch verwendet

werden, um temporäre Daten zu speichern, die über eine Flotte von Instances, z. B. einen load balanced Pool von Webservern, repliziert werden.

Ein Instance-Speicher besteht aus einem oder mehreren Instance-Speicher-Volumes, die als Blockgeräte verfügbar gemacht werden. Die Größe eines Instance-Speichers sowie die Anzahl der verfügbaren Geräte variiert je nach Instance-Typ und Instance-Größe. Beispielsweise stellt nicht jeder Instance-Typ Instance-Speicher-Volumes bereit. Weitere Informationen finden Sie unter Volumenlimits für den Instance-Speicher für EC2-Instances.

Die virtuellen Geräte für Instance-Speicher-Volumes sind mit den Namen der virtuellen Geräte in der Reihenfolge von `ephemeral0` bis `ephemeral23` ausgestattet. Bei einem Instance-Typ, der ein Instance-Speicher-Volume unterstützt, lautet der virtuelle Gerätename des einen Volumes beispielsweise `ephemeral0`. Bei einem Instance-Typ, der vier Instance-Speicher-Volumes unterstützt, lauten die virtuellen Gerätenamen der vier Volumes wie folgt: `ephemeral0`, `ephemeral1`, `ephemeral2` und `ephemeral3`.



Preise für Instance-Speicher

Für die Nutzung der für Ihre Instance bereitgestellten Instance-Speicher-Volumes fallen keine zusätzlichen Gebühren an. Instance-Speicher-Volumes sind als Teil der Nutzungskosten für die Instance enthalten.

Inhalt

- Datenpersistenz für Amazon-EC2-Instance-Speicher-Volumes

- Volumenlimits für den Instance-Speicher für EC2-Instances
- SSD-Instance-Speicher-Volumes für EC2-Instances
- Instance-Speicher-Volumes zu einer EC2-Instance hinzufügen
- Das Instance-Speicher-Swap-Volume für M1- und C1-EC2-Instances aktivieren
- Instance-Speicher-Volumes auf EC2-Instances initialisieren
- Detaillierte Leistungsstatistiken für Instance-Speicher-Volumes von Amazon EC2

Datenpersistenz für Amazon-EC2-Instance-Speicher-Volumes

Instance-Speicher-Volumes werden nur beim Start der Instance angehängt. Sie können ein Instance-Speicher-Volume nicht an eine Instance anfügen, nachdem Sie sie gestartet haben. Sie können ein Instance-Speicher-Volume nicht von einer Instance trennen und an eine andere Instance anfügen.

Ein Instance-Speicher-Volume ist nur während der Lebensdauer der Instance, an die es angehängt ist, vorhanden. Sie können ein Instance-Speicher-Volume nicht so konfigurieren, dass es über die Nutzungsdauer der jeweiligen Instance hinaus erhalten bleibt.

Die Daten auf einem Instance-Speicher-Volume der Instance bleiben erhalten, wenn die Instance neu gestartet wird. Die Daten bleiben jedoch nicht erhalten, wenn die Instance angehalten, in den Ruhezustand versetzt oder beendet wird. Wenn die Instance angehalten, in den Ruhezustand versetzt oder beendet wird, jeder Block der Instance-Speicher-Volumes der Instance kryptografisch gelöscht.

Deshalb sollten Sie in einem Instance-Speicher keine wertvollen, langfristigen Daten ablegen. Wenn Sie die auf einem Instance-Speicher-Volume gespeicherten Daten über die Lebensdauer der Instance hinaus beibehalten müssen, müssen Sie diese Daten manuell in einen persistenteren Speicher kopieren, z. B. ein Amazon EBS-Volume, einen Amazon-S3-Bucket oder ein Amazon-EFS-Dateisystem.

Es gibt einige Ereignisse, die dazu führen können, dass Ihre Daten nicht während der gesamten Lebensdauer der Instance erhalten bleiben. Die folgende Tabelle gibt an, ob Daten auf Instance-Speicher-Volumes während bestimmter Ereignisse gespeichert werden, und zwar sowohl für virtualisierte als auch für Bare-Metal-Instances.

Ereignis	Was passiert mit Ihren Daten?
Vom Benutzer initiierte Instance-Lebenszyklusereignisse	

Ereignis	Was passiert mit Ihren Daten?
Die Instance wird neu gestartet	The data persists
Die Instance wird angehalten	The data does not persist
Die Instance ist im Ruhezustand	The data does not persist
Die Instance wurde beendet	The data does not persist
Die Instance wurde geändert	The data does not persist *
Von der Instance wird ein EBS-gestütztes AMI erstellt	The data does not persist in the created AMI **
Von der Instance wird ein Amazon-S3-gestütztes AMI erstellt (Linux instances)	The data persists in the AMI bundle uploaded to Amazon S3 ***
Vom Benutzer initiierte Betriebssystemereignisse	
A shutdown is initiated	The data does not persist †
A restart is initiated	The data persists
AWS geplante Ereignisse	
Instance anhalten	The data does not persist
Instance-Neustart	The data persists
Systemneustart	The data persists
Ausmusterung einer Instance	The data does not persist
Ungeplante Ereignisse	
Vereinfachte automatische Wiederherstellung	The data does not persist
Aktionsbasierte Wiederherstellung durch CloudWatch	The data does not persist
The underlying disk fails	The data on the failed disk does not persist

Ereignis	Was passiert mit Ihren Daten?
Power failure	The data persists upon reboot

* Wenn der neue Instance-Typ Instance-Speicher unterstützt, erhält die Instance die Anzahl der Instance-Speicher-Volumes, die vom neuen Instance-Typ unterstützt werden, aber die Daten werden nicht auf die neue Instance übertragen. Wenn der neue Instance-Typ den Instance-Speicher nicht unterstützt, erhält die Instance die Instance-Speicher-Volumes nicht.

** Die Daten sind nicht im EBS-gestützten AMI enthalten und sie sind nicht in Instance-Speicher-Volumes enthalten, die an Instances angehängt sind, die von diesem AMI aus gestartet wurden.

*** Die Daten sind in dem AMI-Bündel enthalten, das auf Amazon S3 hochgeladen wird. Wenn Sie eine Instance von diesem AMI aus starten, erhält die Instance die im AMI gebündelten Instance-Speicher-Volumes mit den Daten, die sie zum Zeitpunkt der Erstellung des AMI enthielten.

† Der Terminierungsschutz und der Stoppschutz schützen Instances nicht vor Instancestopps oder -beendigungen als Folge von Shutdowns, die durch das Betriebssystem der Instance ausgelöst wurden. Daten, die auf Instance-Speicher-Volumes gespeichert sind, bleiben sowohl bei Stopp- als auch bei Terminierungsereignissen der Instance nicht erhalten.

Volumenlimits für den Instance-Speicher für EC2-Instances

Anzahl, Größe und Typ der Instance-Speicher-Volumes werden durch den Instance-Typ bestimmt. Einige Instance-Typen wie M6, C6 und R6 unterstützen keine Instance-Speicher-Volumes, während andere Instance-Typen wie M5d, C6gd und R6gd Instance-Speicher-Volumes unterstützen. Sie können einer Instance nicht mehr Instance-Speicher-Volumes zuordnen, als von ihrem Instance-Typ unterstützt werden. Bei den Instance-Typen, die Instance-Speicher-Volumes unterstützen, variieren Anzahl und Größe der Instance-Speicher-Volumes je nach Instance-Größe. `m5d.large`Unterstützt beispielsweise 1 x 75 GB Instance-Speicher-Volume und `m5d.24xlarge` unterstützt 4 x 900 GB-Instance-Speicher-Volumes.

Bei Instance-Typen mit NVMe-Instance-Speicher-Volumes werden alle unterstützten Instance-Speicher-Volumes beim Start automatisch an die Instance angehängt. Zum Beispiel bei Typen mit Nicht-NVMe-Instance-Speicher-Volumes, wie C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 und X1e, müssen Sie die Blockgerät-Zuweisungen für die Instance-Speicher-Volumes, die Sie beim Start anhängen möchten, manuell angeben. Nach dem Start der Instance müssen Sie dann die angehängten Instance-Speicher-Volumes formatieren und bereitstellen, bevor Sie sie verwenden

können. Sie können ein Instance-Speicher-Volume nicht verfügbar machen, nachdem Sie die Instance gestartet haben.

Einige Instance-Typen verwenden NVMe- oder SATA-basierte SSDs, während andere SATA-basierte Festplatten-Volumes (HDD) verwenden. SSDs bieten eine hohe zufällige I/O-Leistung, wenn Sie Speicher mit sehr niedriger Latenz benötigen, die Daten aber nicht erhalten bleiben müssen, wenn die Instance beendet wird oder Sie fehlertolerante Architekturen nutzen können. Weitere Informationen finden Sie unter SSD-Instance-Speicher-Volumes für EC2-Instances.

Die Daten auf der NVMe-Instance speichern Volumes und einige HDD-Instance-Speicher-Volumes werden im Ruhezustand verschlüsselt. Weitere Informationen finden Sie unter Datenschutz bei Amazon EC2.

Verfügbare Instance-Speicher-Volumes

Der Leitfaden für Amazon-EC2-Instance-Typen gibt einen Überblick über die Anzahl, Größe, den Typ und die Leistungsoptimierungen von Instance-Speicher-Volumes, die für die einzelnen unterstützten Instance-Typen verfügbar sind. Weitere Informationen finden Sie hier:

- Spezifikationen des Instance-Speichers – Allgemeiner Zweck
- Spezifikationen des Instance-Speichers – Für Berechnungen optimiert
- Spezifikationen des Instance-Speichers – Arbeitsspeicheroptimiert
- Spezifikationen des Instance-Speichers – Speicheroptimiert
- Spezifikationen des Instance-Speichers – Beschleunigte Datenverarbeitung
- Spezifikationen des Instance-Speichers – Hochleistungsrechnen
- Spezifikationen des Instance-Speichers – vorherige Generation

Console

So rufen Sie Volume-Informationen des Instance-Speichers ab

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instance Types (Instance-Typen) aus.
3. Fügen Sie den Filter Lokaler Instance-Speicher = wahr hinzu. Die Spalte Speicher gibt die Gesamtgröße des Instance-Speichers für den Instance-Typ an.
4. (Optional) Klicken Sie auf das Symbol Einstellungen und aktivieren Sie dann die Anzahl der Speicherdatenträger. Diese Spalte gibt die Anzahl der Instance-Speicher-Volumes an.

5. (Optional) Fügen Sie Filter hinzu, um den Anwendungsbereich auf bestimmte Instance-Typen von Interesse zu erweitern.

AWS CLI

So rufen Sie Volume-Informationen des Instance-Speichers ab

Verwenden Sie den Befehl describe-instance-types. Im folgenden Beispiel wird die Gesamtgröße des Instance-Speichers für jeden Instance-Typ in der R6i-Instance-Familie mit Instance-Speicher-Volumes angezeigt.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r6i*" "Name=instance-storage-
supported,Values=true" \
    --query "InstanceTypes[].[InstanceType, InstanceStorageInfo.TotalSizeInGB]" \
    --output table
```

Es folgt eine Beispielausgabe.

```
----------------------------
|  DescribeInstanceTypes   |
+----------------+---------+
|  r6id.16xlarge  |  3800  |
|  r6idn.16xlarge |  3800  |
|  r6idn.8xlarge  |  1900  |
|  r6id.2xlarge   |  474   |
|  r6idn.xlarge   |  237   |
|  r6id.12xlarge  |  2850  |
|  r6idn.2xlarge  |  474   |
|  r6id.xlarge    |  237   |
|  r6idn.24xlarge |  5700  |
|  r6id.4xlarge   |  950   |
|  r6id.32xlarge  |  7600  |
|  r6id.24xlarge  |  5700  |
|  r6idn.large    |  118   |
|  r6idn.4xlarge  |  950   |
|  r6id.large     |  118   |
|  r6id.8xlarge   |  1900  |
|  r6idn.32xlarge |  7600  |
|  r6idn.metal    |  7600  |
|  r6id.metal     |  7600  |
|  r6idn.12xlarge |  2850  |
```

```
+----------------+--------+
```

So rufen Sie die vollständigen Instance-Speicherdetails für einen Instance-Typ ab

Verwenden Sie den Befehl describe-instance-types.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r6id.16xlarge" \
    --query "InstanceTypes[].InstanceStorageInfo"
```

Die Beispielausgabe zeigt, dass dieser Instance-Typ über zwei 1900 GB NVMe SSD-Volumes verfügt, für insgesamt 3800 GB Instance-Speicher.

```
[
    {
        "TotalSizeInGB": 3800,
        "Disks": [
            {
                "SizeInGB": 1900,
                "Count": 2,
                "Type": "ssd"
            }
        ],
        "NvmeSupport": "required",
        "EncryptionSupport": "required"
    }
]
```

PowerShell

So rufen Sie Volume-Informationen des Instance-Speichers ab

Verwenden Sie das cmdlet Get-EC2InstanceType. Im folgenden Beispiel wird die Gesamtgröße des Instance-Speichers für jeden Instance-Typ in der R6i-Instance-Familie mit Instance-Speicher-Volumes angezeigt.

```
(Get-EC2InstanceType -Filter @{Name="instance-type";
 Values="r6i*"},@{Name="instance-storage-supported"; Values="true"})
 | Format-Table @{Name="InstanceType";Expression={$_.InstanceType}},
 @{Name="TotalSize";Expression={$_.InstanceStorageInfo.TotalSizeInGB}}
```

Es folgt eine Beispielausgabe.

```
InstanceType   TotalSize
------------   ---------
r6idn.16xlarge      3800
r6id.16xlarge       3800
r6id.xlarge          237
r6idn.8xlarge       1900
r6idn.2xlarge        474
r6id.12xlarge       2850
r6idn.xlarge         237
r6id.2xlarge         474
r6id.4xlarge         950
r6idn.24xlarge      5700
r6id.32xlarge       7600
r6id.24xlarge       5700
r6idn.large          118
r6id.large           118
r6idn.4xlarge        950
r6id.8xlarge        1900
r6id.metal          7600
r6idn.32xlarge      7600
r6idn.metal         7600
r6idn.12xlarge      2850
```

So rufen Sie die vollständigen Instance-Speicherdetails für einen Instance-Typ ab

Verwenden Sie das cmdlet Get-EC2InstanceType. Die Ausgabe wird in das JSON-Format konvertiert.

```
(Get-EC2InstanceType -Filter @{Name="instance-type";
 Values="r6id.16xlarge"}).InstanceStorageInfo | ConvertTo-Json
```

Die Beispielausgabe zeigt, dass dieser Instance-Typ über zwei 1900 GB NVMe SSD-Volumes verfügt, für insgesamt 3800 GB Instance-Speicher.

```
{
  "Disks": [
    {
      "Count": 2,
      "SizeInGB": 1900,
      "Type": "ssd"
    }
  ],
```

```
  "EncryptionSupport": {
    "Value": "required"
  },
  "NvmeSupport": {
    "Value": "required"
  },
  "TotalSizeInGB": 3800
}
```

SSD-Instance-Speicher-Volumes für EC2-Instances

Wie bei anderen Instance-Speicher-Volumes müssen Sie die SSD-Instance-Speicher-Volumes für Ihre Instance beim Start zuordnen. Die Daten auf einem SSD-Instance-Volume bleiben nur für die Dauer der zugehörigen Instance erhalten. Weitere Informationen finden Sie unter Instance-Speicher-Volumes zu einer EC2-Instance hinzufügen.

NVMe-SSD-Volumes

Einige Instances stellen nicht flüchtige Memory Express (NVMe)-Solid State Drives (SSD)-Instance-Speicher-Volumes bereit. Weitere Informationen dazu, welcher Typ von Instance-Speicher-Volume von den einzelnen Instance-Typen jeweils unterstützt wird, finden Sie unter Volumenlimits für den Instance-Speicher für EC2-Instances.

Die Daten zum NVMe-Instance-Speicher sind mittels einer XTS-AES-256-Blockverschlüsselung verschlüsselt, die in einem Hardwaremodul auf der Instance implementiert ist. Die Verschlüsselungsschlüssel werden mithilfe des Hardwaremoduls erstellt und sind für jedes NVMe-Instance-Speichergerät eindeutig. Alle Verschlüsselungsschlüssel werden zerstört, wenn die Instance angehalten oder beendet wird, und können nicht wiederhergestellt werden. Sie können diese Verschlüsselung nicht deaktivieren und keine eigenen Verschlüsselungsschlüssel bereitstellen.

Linux-Instances

Für den Zugriff auf NVMe-Volumes müssen die NVMe-Treiber installiert sein. Die folgenden AMIs erfüllen diese Anforderung:

- AL2023
- Amazon Linux 2
- Amazon-Linux-AMI 2018.03 und höher
- Ubuntu 14.04 oder höher mit `linux-aws`-Kernel

> **Note**
>
> AWS-Graviton-basierte Instance-Typen erfordern Ubuntu 18.04 oder höher mit `linux-aws`-Kernel

- Red Hat Enterprise Linux 7.4 oder höher
- SUSE Linux Enterprise Server 12 SP2 oder höher
- CentOS 7.4.1708 oder höher
- FreeBSD 11.1 oder höher
- Debian GNU/Linux 9 oder höher

- Bottlerocket

Nachdem Sie die Verbindung mit Ihrer Instance hergestellt haben, können Sie die NVMe-Geräte mithilfe des Befehls lspci auflisten. Nachstehend finden Sie eine Beispiel-Ausgabe für eine `i3.8xlarge`-Instance, die vier NVMe-Geräte unterstützt.

```
[ec2-user ~]$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371SB PIIX3 IDE [Natoma/Triton II]
00:01.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 01)
00:02.0 VGA compatible controller: Cirrus Logic GD 5446
00:03.0 Ethernet controller: Device 1d0f:ec20
00:17.0 Non-Volatile memory controller: Device 1d0f:cd01
00:18.0 Non-Volatile memory controller: Device 1d0f:cd01
00:19.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1a.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1f.0 Unassigned class [ff80]: XenSource, Inc. Xen Platform Device (rev 01)
```

Wenn Sie ein unterstütztes Betriebssystem verwenden, aber die NVMe-Geräte nicht angezeigt werden, überprüfen Sie mit dem folgenden Befehl, ob das NVMe-Modul geladen ist.

- Amazon Linux, Amazon Linux 2, Ubuntu 14/16, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, CentOS 7

```
$ lsmod | grep nvme
```

```
nvme           48813  0
```

- Ubuntu 18

```
$ cat /lib/modules/$(uname -r)/modules.builtin | grep nvme
s/nvme/host/nvme-core.ko
kernel/drivers/nvme/host/nvme.ko
kernel/drivers/nvmem/nvmem_core.ko
```

Die NVMe-Volumes erfüllen die Spezifikation NVMe 1.0a. Sie können die NVMe-Befehle bei Ihren NVMe-Volumes verwenden. In Amazon Linux können Sie das `nvme-cli`-Paket aus dem Repository mit dem Befehl yum install installieren. Bei anderen unterstützten Linux-Versionen können Sie das `nvme-cli`-Paket herunterladen, wenn es im Image nicht verfügbar ist.

Windows-Instances

Die neuesten AWS Windows-AMIs der folgenden Betriebssysteme enthalten die AWS NVMe-Treiber, die für die Interaktion mit SSD-Instance-Speicher-Volumes verwendet werden, die einer besseren Leistung halber als NVMe-Blockgeräte angezeigt werden:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Nachdem Sie eine Verbindung mit Ihrer Instance hergestellt haben, können Sie überprüfen, ob die NVMe-Volumes in der Datenträgerverwaltung angezeigt werden. Öffnen Sie auf der Taskleiste das Kontextmenü (Rechtsklick) für das Windows-Logo und wählen Sie Datenträgerverwaltung.

Die von Amazon bereitgestellten AWS Windows AMIs beinhalten den AWS NVMe-Treiber. Wenn Sie nicht die neuesten AWS Windows-AMIs verwenden, können Sie den aktuellen AWS NVMe-Treiber installieren.

Nicht-NVMe-SSD-Volumes

Die folgenden Instances unterstützen Instance-Speicher-Volumes, die Nicht-NVMe-SSDs verwenden, um hohe Random-I/O-Leistung bereitzustellen: C3, I2, M3, R3, und X1. Weitere Informationen zu

den von den einzelnen Instance-Typen unterstützten Instance-Speicher-Volumes finden Sie unter Volumenlimits für den Instance-Speicher für EC2-Instances.

I/O-Leistung des SSD-basierten Instance-Speicher-Volumes

Die Anzahl der erreichten Schreib-IOPS nimmt in dem Maß ab, in dem Sie die SSD-basierten Instance-Speicher-Volumes für Ihre Instance mit Daten belegen. Der Grund dafür ist der zusätzliche Arbeitsaufwand für den SSD-Controller, der verfügbaren Speicherplatz suchen, vorhandene Daten neu schreiben und ungenutzten Speicherplatz löschen muss, sodass er neu beschrieben werden kann. Dieser Prozess der Garbage Collection führt zu einer internen Write Amplification in der SSD; diese wird im Verhältnis der SSD-Schreibvorgänge zu den Benutzer-Schreibvorgängen ausgedrückt. Dieser Leistungsabfall ist sogar noch größer, wenn die Schreibvorgänge nicht in Vielfachen von 4 096 Byte durchgeführt oder nicht auf eine 4 096 Byte-Grenze ausgerichtet werden. Wenn eine kleinere Anzahl von Bytes oder nicht ausgerichtete Bytes geschrieben werden, muss der SSD-Controller die Daten in der Umgebung auslesen und an einem neuen Ort speichern. Dieses Muster führt zu einer erheblich größeren Write Amplification, einer höheren Latenz und zu dramatischen I/O-Leistungseinbußen.

SSD-Controller können verschiedenen Strategien anwenden, um die Auswirkungen der Write Amplification zu verringern. Eine dieser Strategien besteht darin, Speicherplatz des SSD-Instance-Speichers zu reservieren, sodass der Controller den für Schreibvorgänge verfügbaren Speicherplatz effizienter verwalten kann. Diese Methode wird als Overprovisioning (übermäßige Bereitstellung) bezeichnet. Die SSD-basierten Instance-Speicher-Volumes haben keinen reservierten Speicherplatz für Überprovisionierung zur Verfügung. Um die Schreibverstärkung zu reduzieren, empfehlen wir, 10 Prozent des Volumes unpartitioniert zu lassen, damit der SSD-Controller es für Over-Provisioning nutzen kann. Dadurch steht zwar weniger Speicherplatz zur Verfügung, aber die Leistung wird verbessert – auch wenn der Datenträger fast vollständig belegt ist.

Bei Instance-Speicher-Volumes, die TRIM unterstützen, können Sie den TRIM-Befehl dazu verwenden, dem SSD-Controller mitzuteilen, wann immer Sie Daten nicht mehr benötigen, die Sie geschrieben haben. Auf diese Weise hat der Controller mehr freien Speicherplatz zur Verfügung, wodurch die Write Amplification reduziert und die Leistung erhöht wird. Weitere Informationen finden Sie unter TRIM-Unterstützung für Instance-Speicher-Volumes.

TRIM-Unterstützung für Instance-Speicher-Volumes

Einige Instance-Typen unterstützen SSD-Volumes mit TRIM. Weitere Informationen finden Sie unter Volumenlimits für den Instance-Speicher für EC2-Instances.

> **Note**
>
> (Nur Windows-Instances) Instances, die Windows Server 2012 R2 ausführen, unterstützen TRIM ab AWS-PV-Treiber Version 7.3.0. Instances, die frühere Versionen von Windows Server ausführen, unterstützen TRIM nicht.

Instance-Speicher-Volumes, die TRIM unterstützen, werden vollständig gekürzt, bevor sie Ihrer Instance zugeordnet werden. Diese Volumes sind beim Start einer Instance nicht mit einem Dateisystem formatiert, deshalb müssen Sie sie formatieren, bevor sie gemountet und verwendet werden können. Um den Zugriff auf diese Volumes zu beschleunigen, sollten Sie die TRIM-Operation beim Formatieren überspringen.

(Windows-Instances) Um die TRIM-Unterstützung während der ersten Formatierung vorübergehend zu deaktivieren, verwenden Sie den Befehl `fsutil behavior set DisableDeleteNotify 1`. Nachdem die Formatierung abgeschlossen ist, aktivieren Sie die TRIM-Unterstützung mithilfe von `fsutil behavior set DisableDeleteNotify 0` erneut.

Bei Instance-Speicher-Volumes, die TRIM unterstützen, können Sie den TRIM-Befehl dazu verwenden, dem SSD-Controller mitzuteilen, wann Sie Daten nicht mehr benötigen, die Sie geschrieben haben. Auf diese Weise hat der Controller mehr freien Speicherplatz zur Verfügung, wodurch die Write Amplification reduziert und die Leistung erhöht wird. In Linux-Instances verwenden Sie den Befehl `fstrim`, um periodisches TRIM zu aktivieren. Verwenden Sie in Windows-Instances den `fsutil behavior set DisableDeleteNotify 0`-Befehl, um sicherzustellen, dass die TRIM-Unterstützung während des normalen Betriebs aktiviert ist.

Instance-Speicher-Volumes zu einer EC2-Instance hinzufügen

Bei Instance-Typen mit NVMe-Instance-Speicher-Volumes werden alle unterstützten Instance-Speicher-Volumes beim Start automatisch an die Instance angehängt. NVMe-Instance-Speicher-Volumes werden automatisch aufgezählt und ihnen wird ein Gerätename zugeordnet.

Zum Beispiel bei Typen mit Nicht-NVMe-Instance-Speicher-Volumes, wie C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 und X1e, müssen Sie die Blockgerät-Zuweisungen für die Instance-Speicher-Volumes, die Sie beim Start anhängen möchten, manuell angeben. Blockgerätezuordnungen können in der Instance-Startanforderung oder in dem AMI, das zum Starten der Instance verwendet wird, angegeben werden. Jeder Eintrag in einer Blockgerät-Zuweisung beinhaltet einen gewählten Namen und das Volume, dem er zugeordnet ist. Weitere Informationen finden Sie unter . Blockgerät-Zuweisungen auf Amazon-EC2-Instances blockieren

> **Important**
>
> Sie können Instance-Speicher-Volumes für eine Instance nur dann angeben, wenn Sie sie starten. Sie können ein Instance-Speicher-Volume nicht an eine Instance anfügen, nachdem Sie sie gestartet haben.

Nachdem Sie eine Instance gestartet haben, müssen Sie sicherstellen, dass die Instance-Speicher-Volumes für Ihre Instance formatiert und gemountet sind, bevor Sie sie verwenden. Das Root-Volume des Instance-Speichers wird automatisch gemountet.

Berücksichtigung der Stamm-Volumes

Eine Blockgerät-Zuweisung gibt stets das Stamm-Volume für die Instance an. Das Root-Volume wird automatisch gemountet.

Linux-Instances – Das Root-Volume ist entweder ein Amazon-EBS-Volume oder ein Instance-Speicher-Volume. Bei Instances mit einem Instance-Speicher-Volume für das Stamm-Volume variiert die Größe dieses Volumes je nach AMI, aber die Maximalgröße ist 10 GB. Weitere Informationen finden Sie unter Root-Volume-Typ.

Windows-Instances – Bei dem Root-Volume muss es sich um ein Amazon-EBS-Volume handeln. Instance-Speicher wird für das Root-Volume nicht unterstützt.

Inhalt

- Instance-Speicher-Volumes zu einem Amazon-EC2-AMI hinzufügen
- Instance-Speicher-Volumes während des Startens zu einer EC2-Instance hinzufügen
- Instance-Speicher-Volumes für die Verwendung in einer EC2-Instance verfügbar machen

Instance-Speicher-Volumes zu einem Amazon-EC2-AMI hinzufügen

Sie können ein AMI mit einer Blockgerät-Zuweisung erstellen, die Instance-Speicher-Volumes enthält.

Wenn Sie eine Instance mit einem Instance-Typ starten, der non-NVMe-Instance-Speicher-Volumes unterstützt, und ein AMI, das Instance-Speicher-Volumes in seiner Blockgerät-Zuweisung angibt, enthält die Instance diese Instance-Speicher-Volumes. Wenn die Anzahl der Instance-Speicher-Volumes in der Blockgerät-Zuweisung die für eine Instance verfügbare Anzahl an Instance-Speicher-Volumes übersteigt, werden die überzähligen Instance-Speicher-Volumes ignoriert.

Wenn Sie eine Instance mit einem Instance-Typ starten, der non-NVMe-Instance-Speicher-Volumes unterstützt, und ein AMI, das Instance-Speicher-Volumes in seiner Blockgerät-Zuweisung angibt, enthält die Instance diese Instance-Speicher-Volumes. Instances, die NVMe-Instance-Store-Volumes unterstützen, erhalten alle ihre unterstützten Instance-Speicher-Volumes, unabhängig von den Blockgerätezuordnungen, die in der Instance-Startanforderung und im AMI angegeben sind. Die Gerätezuordnung dieser Volumes hängt von der Reihenfolge ab, in der das Betriebssystem die Volumes aufzählt.

Überlegungen

- Die Anzahl der verfügbaren Instance-Speicher-Volumes hängt vom Instance-Typ ab. Weitere Informationen finden Sie unter the section called “Verfügbare Instance-Speicher-Volumes”.
- Sie müssen für jedes Blockgerät einen Gerätenamen angeben. Weitere Informationen finden Sie unter Gerätenamen für Volumes auf Amazon-EC2-Instances.
- Wenn Sie eine Instance starten, können Sie die in der AMI-Blockgerät-Zuweisung angegebenen Nicht-NVMe-Instance-Speicher-Volumes auslassen oder Instance-Speicher-Volumes hinzufügen.
- Bei M3-Instances spezifizieren Sie Instance-Speicher-Volumes in der Blockgerät-Zuweisung für die Instance angeben, nicht im AMI. Amazon EC2 ignoriert möglicherweise Instance-Speicher-Volumes, die nur in der Blockgerät-Zuweisung des AMI angegeben sind.

Console

So fügen Sie Instance-Speicher-Volumes zu einem Amazon-EBS-gestützten AMI hinzu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie die Instance aus.
3. Wählen Sie Actions (Aktionen), Image and templates (Image und Vorlagen), Create image (Image erstellen).
4. Fügen Sie im Dialogfeld Create image (Image erstellen) einen aussagekräftigen Namen und eine Beschreibung für Ihr Image hinzu.
5. Wählen Sie zum Hinzufügen jedes Instance-Speicher-Volumes Add volume (Volume hinzufügen), von Volume type (Volume-Typ) ein Instance-Speicher-Volume und aus Device (Gerät) einen Gerätenamen aus.
6. Wählen Sie Create Image (Image erstellen) aus.

AWS CLI

So fügen Sie Instance-Speicher-Volumes zu einem AMI hinzu

Verwenden Sie den Befehl create-image mit der Option `--block-device-mappings` zum Angeben einer Blockgerät-Zuweisung für ein EBS-gestütztes AMI. Verwenden Sie den Befehl register-image mit der Option `--block-device-mappings` zum Angeben einer Blockgerät-Zuweisung für ein Amazon-S3-gestütztes AMI.

```
--block-device-mappings file://mapping.json
```

Mit der folgenden Blockgerät-Zuweisung werden zwei Instance-Speicher-Volumes hinzugefügt.

```
[
    {
        "DeviceName": "/dev/sdc",
        "VirtualName": "ephemeral0"
    },
    {
        "DeviceName": "/dev/sdd",
        "VirtualName": "ephemeral1"
    }
]
```

PowerShell

So fügen Sie Instance-Speicher-Volumes zu einem AMI hinzu

Verwenden Sie das cmdlet New-EC2Image mit dem Parameter `-BlockDeviceMapping` zum Angeben einer Blockgerät-Zuweisung für ein EBS-gestütztes AMI. Verwenden Sie das cmdlet Register-EC2Image mit dem Parameter `-BlockDeviceMapping` zum Angeben einer Blockgerät-Zuweisung für ein Amazon-S3-gestütztes AMI.

```
-BlockDeviceMapping $bdm
```

Mit der folgenden Blockgerät-Zuweisung werden zwei Instance-Speicher-Volumes hinzugefügt.

```
$bdm = @()

$sdc = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdc.DeviceName = "/dev/sdc"
$sdc.VirtualName = "ephemeral0"
```

```
$bdm += $sdc

$sdd = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdd.DeviceName = "/dev/sdd"
$sdd.VirtualName = "ephemeral1"
$bdm += $sdd
```

Instance-Speicher-Volumes während des Startens zu einer EC2-Instance hinzufügen

Wenn Sie einen Instance-Typ mit Nicht-NVMe-Instance-Speicher-Volumes starten, wie z. B. C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 und X1e, müssen Sie die Blockgerät-Zuweisungen für die Instance-Speicher-Volumes angeben, die Sie beim Start anhängen möchten. Die Blockgerätezuordnungen müssen in der Instance-Startanforderung oder in dem AMI angegeben werden, mit dem die Instance gestartet wurde.

Wenn das AMI Blockgerätezuordnungen für die Instance-Speicher-Volumes enthält, müssen Sie Block-Gerätezuordnungen in der Instance-Startanforderung nicht angeben, es sei denn, Sie benötigen mehr Instance-Speicher-Volumes als im AMI enthalten sind.

Wenn das AMI keine Blockgerätezuordnungen enthält für Instance-Speicher-Volumes enthält, müssen Sie die Blockgerätezuordnungen in der Instance-Startanforderung angeben.

Bei Instance-Typen mit NVMe-Instance-Speicher-Volumes werden alle unterstützten Instance-Speicher-Volumes beim Start automatisch an die Instance angehängt.

Überlegungen

- Die Anzahl der verfügbaren Instance-Speicher-Volumes hängt vom Instance-Typ ab. Weitere Informationen finden Sie unter the section called “Verfügbare Instance-Speicher-Volumes”.
- Sie müssen für jedes Blockgerät einen Gerätenamen angeben. Weitere Informationen finden Sie unter Gerätenamen für Volumes auf Amazon-EC2-Instances.
- Bei M3-Instances erhalten Sie möglicherweise Instance-Speicher-Volumes auch dann, wenn Sie sie nicht in der Blockgerät-Zuweisung für die Instance angeben.

Console

So geben Sie eine Blockgerät-Zuweisung in einer Instance-Startanfrage an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie auf dem Dashboard Launch Instance aus.
3. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) das zu verwendende AMI aus.
4. Im Abschnitt Speicher konfigurieren werden unter dem Abschnitt Instance-Speicher-Volumes die Instance-Speicher-Volumes aufgeführt, die an die Instance angehängt werden können.
5. Wählen Sie für jedes anzufügende Instance-Speicher-Volume unter Gerätename den zu verwendenden Gerätenamen aus.
6. Konfigurieren Sie die übrigen Instance-Einstellungen nach Bedarf, und wählen Sie dann Instance starten.

AWS CLI

So geben Sie eine Blockgerät-Zuweisung in einer Instance-Startanfrage an

Verwenden den Befehl run-instances mit der Option `--block-device-mappings`.

```
--block-device-mappings file://mapping.json
```

Mit der folgenden Blockgerät-Zuweisung werden zwei Instance-Speicher-Volumes hinzugefügt.

```
[
    {
        "DeviceName": "/dev/sdc",
        "VirtualName": "ephemeral0"
    },
    {
        "DeviceName": "/dev/sdd",
        "VirtualName": "ephemeral1"
    }
]
```

PowerShell

So geben Sie eine Blockgerät-Zuweisung in einer Instance-Startanfrage an

Verwenden Sie das cmdlet New-EC2Instance mit der Option `-BlockDeviceMapping`.

```
-BlockDeviceMapping $bdm
```

Mit der folgenden Blockgerät-Zuweisung werden zwei Instance-Speicher-Volumes hinzugefügt.

```
$bdm = @()

$sdc = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdc.DeviceName = "/dev/sdc"
$sdc.VirtualName = "ephemeral0"
$bdm += $sdc

$sdd = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdd.DeviceName = "/dev/sdd"
$sdd.VirtualName = "ephemeral1"
$bdm += $sdd
```

Instance-Speicher-Volumes für die Verwendung in einer EC2-Instance verfügbar machen

Nachdem Sie eine Instance mit angefügten Instance-Speicher-Volumes gestartet haben, müssen Sie die Volumes mounten, bevor Sie auf sie zugreifen können.

Linux-Instances

Sie können Volumes mit dem Dateisystem Ihrer Wahl formatieren, nachdem Sie Ihre Instance gestartet haben.

So machen Sie ein Instance-Speicher-Volume unter Linux verfügbar

1. Stellen Sie eine Verbindung mit der Instance über einen SSH-Client her. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance mit SSH.
2. Verwenden Sie den Befehl `df -h`, um die Volumes anzuzeigen, die formatiert und gemountet sind.

   ```
   $ df -h
   Filesystem      Size  Used Avail Use% Mounted on
   devtmpfs        3.8G   72K  3.8G   1% /dev
   tmpfs           3.8G     0  3.8G   0% /dev/shm
   /dev/nvme0n1p1  7.9G  1.2G  6.6G  15% /
   ```

3. Verwenden Sie den Befehl `lsblk`, um Volumes anzuzeigen, die beim Start zugeordnet, aber nicht formatiert und gemountet wurden.

   ```
   $ lsblk
   ```

```
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme0n1       259:1    0    8G  0 disk
##nvme0n1p1   259:2    0    8G  0 part /
##nvme0n1p128 259:3    0    1M  0 part
nvme1n1       259:0    0 69.9G  0 disk
```

4. Um ein Instance-Speicher-Volume zu formatieren und zu mounten, das nur zugeordnet wurde, gehen Sie folgendermaßen vor:

   a. Erstellen Sie mithilfe des Befehls `mkfs` ein Dateisystem auf dem Gerät.

   ```
   $ sudo mkfs -t xfs /dev/nvme1n1
   ```

   b. Erstellen Sie mithilfe des Befehls `mkdir` ein Verzeichnis, in dem das Gerät gemountet werden soll.

   ```
   $ sudo mkdir /data
   ```

   c. Mounten Sie mithilfe des Befehls `mount` das Gerät in dem neu erstellten Verzeichnis.

   ```
   $ sudo mount /dev/nvme1n1 /data
   ```

Windows-Instances

Bei Windows-Instances werden die Instance-Speicher-Volumes mit dem NTFS-Dateisystem neu formatiert.

Sie können die Instance-Speicher-Volumes auch mithilfe der Windows-Datenträgerverwaltung anzeigen. Weitere Informationen finden Sie unter Nicht-NVMe-Festplatten auflisten.

So mounten Sie ein Instance-Store-Volume manuell

1. Wählen Sie Start, wählen Sie Computer-Verwaltung und drücken Sie dann die Eingabetaste.
2. Wählen Sie im linken Bereich die Option Datenträgerverwaltung.
3. Wenn Sie aufgefordert werden, das Volume zu initialisieren, wählen Sie das zu initialisierende Volume aus, wählen Sie je nach Anwendungsfall den erforderlichen Partitionstyp aus, und wählen Sie dann OK aus.
4. Klicken Sie in der Liste der Volumes mit der rechten Maustaste auf das zu mountende Volume und wählen Sie dann Neues einfaches Volume.

5. Wählen Sie im Assistenten Weiter.
6. Wählen Sie im Bildschirm „Volume-Größe angeben“ die Option Weiter, um die maximale Volume-Größe zu verwenden. Alternativ können Sie eine Volume-Größe wählen, die zwischen dem minimalen und dem maximalen Speicherplatz liegt.
7. Führen Sie auf dem Bildschirm „Laufwerksbuchstabe oder Pfad zuweisen“ einen der folgenden Schritte aus und wählen Sie Weiter.
   - Um das Volume mit einem Laufwerksbuchstaben zu mounten, wählen Sie Den folgenden Laufwerksbuchstaben zuweisen und anschließend den zu verwendenden Laufwerksbuchstaben aus.
   - Um das Volume als Ordner bereitzustellen, wählen Sie Im folgenden leeren NTFS-Ordner mounten und anschließend Durchsuchen aus, um den zu verwendenden Ordner zu erstellen oder auszuwählen.
   - Wenn Sie das Volume ohne Laufwerksbuchstaben oder -pfad mounten möchten, wählen Sie Keinen Laufwerksbuchstaben oder Laufwerkspfad zuweisen.
8. Geben Sie im Fenster „Partition formatieren“ an, ob das Volume formatiert werden soll. Wenn Sie das Volume formatieren möchten, wählen Sie das erforderliche Dateisystem und die Einheitengröße aus und geben Sie eine Datenträgerbezeichnung an.
9. Wählen Sie Weiter, Fertigstellen.

Das Instance-Speicher-Swap-Volume für M1- und C1-EC2-Instances aktivieren

> **Note**
>
> Dieses Thema bezieht sich nur auf `c1.medium`- und `m1.small`- Linux-Instances.

Die `c1.medium`- und die `m1.small`-Instance-Typen verfügen über eine begrenzte Menge an physischem Speicher. Daher erhalten sie zum Startzeitpunkt ein Auslagerungsvolumen von 900 MiB, das als virtueller Speicher oder Swap-Platz für das Linux-System fungiert. Unter Linux können Auslagerungsbereiche verwendet werden, wenn ein System mehr Speicherplatz benötigt, als ihm physisch zugeordnet ist. Wenn der Auslagerungsbereich aktiviert ist, können Linux-Systeme selten verwendete Speicherseiten aus dem physischen Speicher als Auslagerungsbereich kennzeichnen

(entweder eine dedizierte Partition oder eine Auslagerungsdatei in einem bestehenden Dateisystem) und diesen Speicherplatz für Speicherseiten freigeben, die schnellen Zugriff benötigen.

> **Note**
>
> - Die Verwendung des Auslagerungsbereichs für Speicherseiten ist nicht so schnell oder effizient wie die Verwendung von RAM. Wenn Ihre Workload regelmäßig Speicherplatz in den Auslagerungsbereich verschiebt, sollten Sie erwägen, zu einem größeren Instance-Typ mit mehr RAM-Speicher zu migrieren. Weitere Informationen finden Sie unter Änderungen des EC2 Amazon-Instanztyps.
> - Obwohl der Linux-Kernel diesen Auslagerungsbereich als Partition auf dem Root-Volume erkennt, ist er eigentlich ein separates Instance-Speicher-Volume, unabhängig vom Root-Volume-Typ.

Amazon Linux aktiviert und nutzt diesen Auslagerungsbereich automatisch, aber Ihr AMI benötigt möglicherweise einige zusätzliche Schritte, um diesen Bereich zu erkennen und zu nutzen. Verwenden Sie den Befehl swapon -s, um festzustellen, ob Ihre Instance den Auslagerungsbereich nutzt.

```
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
/dev/xvda3                              partition       917500  0       -1
```

Bei der obigen Instance ist ein Swap-Volume mit 900 MiB angefügt und aktiviert. Wenn nach Eingabe dieses Befehls kein Swap-Volume angezeigt wird, müssen Sie möglicherweise den Auslagerungsbereich für das Gerät aktivieren. Überprüfen Sie Ihre verfügbaren Laufwerke mit dem lsblk-Befehl.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M  0 disk
```

Hier ist das Swap-Volume `xvda3` für die Instance verfügbar, aber es ist nicht aktiviert (beachten Sie, dass das Feld `MOUNTPOINT` leer ist). Sie können das Swap-Volume mit dem Befehl swapon aktivieren.

> **Note**
>
> Sie müssen `/dev/` dem Gerätenamen voranstellen, der von lsblk aufgelistet wird. Möglicherweise hat Ihr Gerät eine andere Bezeichnung, beispielsweise `sda3`, `sde3` oder `xvde3`. Verwenden Sie im nachfolgenden Befehl den Gerätenamen für Ihr System.

```
[ec2-user ~]$ sudo swapon /dev/xvda3
```

Jetzt sollte der Auslagerungsbereich in der Ausgabe von lsblk und swapon -s angezeigt werden.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M  0 disk [SWAP]
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
/dev/xvda3                              partition       917500  0       -1
```

Sie müssen auch die Datei `/etc/fstab` bearbeiten, damit dieser Auslagerungsbereich bei jedem Starten des Systems automatisch aktiviert wird.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Hängen Sie die folgende Zeile an die Datei `/etc/fstab` an (und verwenden Sie dabei den Swap-Gerätenamen für Ihr System):

```
/dev/xvda3       none    swap    sw  0       0
```

So nutzen Sie ein Instance-Speicher-Volume als Auslagerungsbereich

Jedes Instance-Speicher-Volume kann als Auslagerungsbereich verwendet werden. Beispielsweise enthält der Instance-Typ `m3.medium` ein SSD-Instance-Speicher-Volume von 4 GB, das als Auslagerungsbereich geeignet ist. Wenn Ihr Instance-Speicher-Volume erheblich größer ist (z. B. 350 GB), können Sie das Volume in eine kleinere Auslagerungspartition von 4-8 GB und den Rest als Daten-Volume partitionieren.

> **Note**
>
> Dieses Verfahren kann nur bei Instance-Typen angewendet werden, die Instance-Speicher unterstützen. Eine Liste mit unterstützten Instance-Typen finden Sie unter Volumenlimits für den Instance-Speicher für EC2-Instances.

1. Auflisten der an Ihre Instance angefügten Blockgeräte, um den Gerätenamen für Ihr Instance-Speicher-Volume zu ermitteln.

```
[ec2-user ~]$ lsblk -p
NAME       MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
/dev/xvdb  202:16   0   4G  0 disk /media/ephemeral0
/dev/xvda1 202:1    0   8G  0 disk /
```

   In diesem Beispiel ist das Instance-Speicher-Volume `/dev/xvdb`. Da dies eine Amazon Linux-Instance ist, wird das Instance-Speicher-Volume formatiert und auf `/media/ephemeral0` gemountet; nicht alle Linux-Betriebssysteme tun dies automatisch.

2. (Optional) Wenn Ihr Instance-Speicher-Volume gemountet ist (es wird ein `MOUNTPOINT` in der lsblk-Befehlsausgabe aufgeführt), müssen Sie mit dem folgenden Befehl das Mounting aufheben.

```
[ec2-user ~]$ sudo umount /dev/xvdb
```

3. Einrichten eines Linux-Auslagerungsbereichs auf dem Gerät mit dem Befehl mkswap.

```
[ec2-user ~]$ sudo mkswap /dev/xvdb
mkswap: /dev/xvdb: warning: wiping old ext3 signature.
Setting up swapspace version 1, size = 4188668 KiB
no label, UUID=b4f63d28-67ed-46f0-b5e5-6928319e620b
```

4. Aktivieren Sie den neuen Auslagerungsbereich.

```
[ec2-user ~]$ sudo swapon /dev/xvdb
```

5. Überprüfen Sie, ob der neue Auslagerungsbereich verwendet wird.

```
[ec2-user ~]$ swapon -s
Filename    Type  Size Used Priority
/dev/xvdb                               partition 4188668 0 -1
```

6. Bearbeiten Sie die Datei `/etc/fstab` so, dass dieser Auslagerungsbereich bei jedem Starten des Systems automatisch aktiviert wird.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Wenn Ihre `/etc/fstab`-Datei einen Eintrag für `/dev/xvdb` (oder `/dev/sdb`) hat, ändern Sie ihn so, dass er mit der unten stehenden Zeile übereinstimmt. Wenn die Datei keinen Eintrag für dieses Gerät hat, hängen Sie die folgende Zeile an Ihre `/etc/fstab`-Datei an (und verwenden Sie dabei den Swap-Gerätenamen für Ihr System):

```
/dev/xvdb       none    swap    sw  0       0
```

> **Important**
>
> Instance-Speicher-Volume-Daten gehen verloren, wenn eine Instance angehalten oder in den Ruhezustand versetzt wird. Dies beinhaltet auch die Formatierung des Instance-Speicher-Auslagerungsbereichs, der in erstellt wurd Step 3. Wenn Sie eine Instance anhalten und erneut starten, die für die Verwendung eines Instance-Speicher-Auslagerungsbereichs konfiguriert wurde, müssen Sie Step 1 bis Step 5 auf dem neuen Instance-Speicher-Volume wiederholen.

Instance-Speicher-Volumes auf EC2-Instances initialisieren

Wegen der Art, wie Amazon EC2 Laufwerke virtualisiert, erfolgt der erste Schreibvorgang zu einem Speicherort bei einigen Instance-Speicher-Volumes langsamer als die nachfolgenden Schreibvorgänge. Für die meisten Anwendungen ist die Amortisierung dieser Kosten während der Nutzungsdauer der Instances akzeptabel. Wenn Sie jedoch eine höhere Laufwerksleistung benötigen, empfehlen wir, dass Sie Ihre Laufwerke initialisieren, indem Sie vor dem Einsatz in der Produktion zu jedem Laufwerksspeicherort einen Schreibvorgang ausführen.

> **Note**
>
> Einige Instance-Typen mit direkt angefügten Solid-State-Disks (SSD) und TRIM-Unterstützung stellen ohne Initialisierung die maximale Leistung zum Startzeitpunkt bereit.

Weitere Informationen über den Instance-Speicher für die einzelnen Instance-Typen finden Sie unter Volumenlimits für den Instance-Speicher für EC2-Instances.

Wenn Sie größere Flexibilität bei der Latenz oder dem Durchsatz benötigen, empfehlen wir die Verwendung von Amazon EBS.

Verwenden Sie zum Initialisieren von Instance-Speicher-Volumes die folgenden dd-Befehle, je nachdem, welchen Speicher Sie initialisieren wollen (beispielsweise `/dev/sdb` oder `/dev/nvme1n1`).

> **Note**
>
> Unmounten Sie das Laufwerk, bevor Sie diesen Befehl ausführen.
> Die Initialisierung kann lange dauern (ca. 8 Stunden bei einer sehr großen Instance).

Verwenden Sie zum Initialisieren der Instance-Speicher-Volumes die folgenden Befehle bei den Instance-Typen `m1.large`, `m1.xlarge`, `c1.xlarge`, `m2.xlarge`, `m2.2xlarge` und `m2.4xlarge`:

```
dd if=/dev/zero of=/dev/sdb bs=1M
dd if=/dev/zero of=/dev/sdc bs=1M
dd if=/dev/zero of=/dev/sdd bs=1M
dd if=/dev/zero of=/dev/sde bs=1M
```

Verwenden Sie zum gleichzeitigen Durchführen der Initialisierung bei allen Instance-Speicher-Volumes den folgenden Befehl:

```
dd if=/dev/zero bs=1M|tee /dev/sdb|tee /dev/sdc|tee /dev/sde > /dev/sdd
```

Beim Konfigurieren von Laufwerken für RAID werden diese initialisiert, indem ein Schreibvorgang zu jedem Laufwerksspeicherort durchgeführt wird. Ändern Sie beim Konfigurieren von softwarebasiertem RAID die minimale Rekonstruktionsgeschwindigkeit:

```
echo $((30*1024)) > /proc/sys/dev/raid/speed_limit_min
```

Detaillierte Leistungsstatistiken für Instance-Speicher-Volumes von Amazon EC2

Amazon EC2 bietet hochauflösende Leistungsstatistiken in Echtzeit für NVMe-Instance-Speicher-Volumes, die an Nitro-basierte Amazon-EC2-Instances angehängt sind. Diese Statistiken werden als aggregierte Zähler dargestellt, die für die Dauer der Lebensdauer der Instance beibehalten werden. Die Statistiken enthalten Details zur kumulativen Anzahl von Vorgängen, gesendeten und empfangenen Byte, zur Zeit, die für I/O-Lese- und Schreibvorgänge aufgewendet wurde, sowie Histogramme für I/O-Lese- und Schreibvorgänge. Diese Statistiken wahren zwar die Konsistenz mit den detaillierten Leistungsstatistiken von Amazon EBS, enthalten aber auch detaillierte Latenzhistogramme, aufgeschlüsselt nach I/O-Größe, die detailliertere Einblicke in Ihre Speicherleistungsmuster bieten können. Diese verbesserte Transparenz ermöglicht es Ihnen, genau zu identifizieren, bei welchen I/O-Größen Latenzprobleme auftreten, sodass Sie die Anwendungsleistung optimieren und Probleme effektiver beheben können.

Sie können diese Statistiken mit einer Genauigkeit von Intervallen von bis zu 1 Sekunde erfassen. Wenn Anfragen häufiger als 1-Sekunden-Intervalle gestellt werden, kann der NVMe-Treiber die Anfragen zusammen mit anderen Administratorbefehlen in eine Warteschlange stellen, damit sie zu einem späteren Zeitpunkt verarbeitet werden können.

Überlegungen

- Die Statistiken werden nur für NVMe-Instance-Speicher-Volumes unterstützt, die an Nitro-basierte Instances angehängt sind.
- Die Zähler sind beim Anhalten und Neustart von Instances nicht persistent.
- Die Statistiken sind ohne zusätzliche Kosten verfügbar.

Statistiken

Das NVMe-Blockgerät verkauft die folgenden Statistiken:

Name der Statistik	Vollständiger Name	Typ	Beschreibung
`total_rea d_ops`	Gesamtzahl an Lesevorgängen	Zähler	Die Gesamtzahl der abgeschlossenen Lesevorgänge.

Name der Statistik	Vollständiger Name	Typ	Beschreibung
total_wr: te_ops	Gesamtzahl an Schreibvorgängen	Zähler	Die Gesamtzahl der abgeschlossenen Schreibvorgänge.
total_re: d_bytes	Gesamtzahl der gelesenen Bytes	Zähler	Die Gesamtzahl der übertragenen und gelesenen Bytes.
total_wr: te_bytes	Gesamtzahl der Schreibbytes	Zähler	Die Gesamtzahl der übertragenen und geschriebenen Bytes.
total_re: d_time	Gesamte Lesezeit	Zähler	Die Gesamtzeit für alle abgeschlossenen Lesevorgänge in Mikrosekunden.
total_wr: te_time	Gesamte Schreibzeit	Zähler	Die Gesamtzeit für alle abgeschlossenen Schreibvorgänge in Mikrosekunden.
instance_ store_vo: ume_perf: rmance_e: ceeded_i: ps	Der gesamte Zeitbedarf hat die maximalen IOPS des Volumes überstiegen	Zähler	Die Gesamtzeit in Mikrosekunden, in der die IOPS-Anfragen die maximale Anzahl an IOPS des Volumes überschritten haben. Jeder höhere Wert als `0` weist darauf hin, dass Ihr Workload mehr IOPS benötigte, als das Volume liefern konnte. Im Idealfall sollte die inkrementelle Anzahl dieser Metrik zwischen zwei Snapshot-Zeiten minimal sein.
instance_ store_vo: ume_perf: rmance_e: ceeded_t:	Der gesamte Zeitbedarf hat den maximalen Durchsatz des Volumes überstiegen	Zähler	Die Gesamtzeit in Mikrosekunden, in der Durchsatzanfragen den maximale Durchsatz des Volumes überschritten haben. Jeder höhere Wert als `0` weist darauf hin, dass Ihr Workload mehr Durchsatz benötigte, als das Volume liefern konnte. Im Idealfall sollte die inkrementelle Anzahl dieser Metrik zwischen zwei Snapshot-Zeiten minimal sein.

Name der Statistik	Vollständiger Name	Typ	Beschreibung
`volume_queue_length`	Länge der Volume-Warteschlange	Zeitpunkt	Die Anzahl der Lese- und Schreibvorgänge, die auf Abschluss warten.
`read_io_latency_histogram`	Lese-I/O-Histogramm	Histogramm *	Die Anzahl der innerhalb der einzelnen Latenzbereiche abgeschlossenen Lesevorgänge in Mikrosekunden.
`write_io_latency_histogram`	Schreib-I/O-Histogramm	Histogramm *	Die Anzahl der innerhalb der einzelnen Latenzbereiche abgeschlossenen Schreibvorgänge in Mikrosekunden.

> **Note**
>
> * Histogrammstatistiken stellen nur I/O-Vorgänge dar, die erfolgreich abgeschlossen wurden. Blockierte oder beeinträchtigte I/O-Vorgänge sind nicht enthalten, werden aber in der Statistik `volume_queue_length` deutlich, die als Point-in-Time-Statistik dargestellt wird.

Auf die Statistiken zugreifen

Auf die Statistiken muss direkt von der Instance aus zugegriffen werden, an die die Instance-Speicher-Volumes angehängt sind. Sie können mit einer der folgenden Methoden auf die Statistik zugreifen.

Linux-Instances

Amazon CloudWatch

Sie können den Amazon-CloudWatch-Agent so konfigurieren, dass er die Statistiken von Ihrer Instance erfasst und als benutzerdefinierte Metriken in CloudWatch verfügbar macht. Anschließend können Sie die Metriken in CloudWatch verwenden, um I/O-Muster zu analysieren, Leistungstrends zu verfolgen, benutzerdefinierte Dashboards zu erstellen und automatisierte Alarme auf der Grundlage von Leistungsschwellenwerten einzurichten.

Weitere Informationen zur Konfiguration des CloudWatch-Agenten finden Sie unter Volume-Metriken für Amazon-EC2-Instance-Speicher erfassen.

nvme-cli tool

So greifen Sie auf die Statistiken zu

1. Stellen Sie eine Verbindung zu der Instance her, der das Volume angehängt ist.
2. Amazon-Linux-2023-AMIs, die nach dem 15. September 2025 veröffentlicht wurden, enthalten die neueste Version des `nvme-cli`-Tools. Wenn Sie ein älteres Amazon Linux AMI verwenden, aktualisieren Sie das `nvme-cli`-Tool.

   ```
   sudo yum install nvme-cli
   ```

3. Führen Sie den folgenden Befehl aus und geben Sie den Gerätenamen für das Volume an.

   ```
   sudo nvme amzn stats /dev/nvme0n1
   ```

Die Statistiken enthalten auch detaillierte Latenzhistogramme, aufgeschlüsselt nach I/O-Größe. Um Statistiken nach I/O-Größe aufgeschlüsselt anzuzeigen, fügen Sie die Option `--details` hinzu. Zum Beispiel:

```
sudo nvme amzn stats --details /dev/nvme0n1
```

Weitere Informationen zur Verwendung des Tools erhalten Sie, indem Sie die Option `--help` angeben. Zum Beispiel:

```
sudo nvme amzn stats --help
```

Windows-Instances

nvme_amzn.exe tool

So greifen Sie auf die Statistiken zu

1. Stellen Sie eine Verbindung zu der Instance her, der das Volume angehängt ist.

2. Stellen Sie sicher, dass Sie die AWSNVMe-Treiberversion `1.7.0` oder höher verwenden. Weitere Informationen zur Aktualisierung des AWSNVMe-Treibers finden Sie unter AWS-NVMe-Treiber.
3. Rufen Sie die Festplattennummer für das Volume ab. Weitere Informationen finden Sie unter Zuweisen von NVMe-Festplatten zu Volumes in einer Windows-Instance von Amazon EC2
4. Führen Sie den folgenden Befehl als Administrator aus und geben Sie die Festplattennummer für das Volume an.

```
.\nvme_amzn.exe stats disk_number
```

Die Statistiken enthalten auch detaillierte Latenzhistogramme, aufgeschlüsselt nach I/O-Größe. Um Statistiken nach I/O-Größe aufgeschlüsselt anzuzeigen, fügen Sie die Option `--details` hinzu. Zum Beispiel:

```
.\nvme_amzn.exe stats --details disk_number
```

Root-Volumes für Ihre Amazon-EC2-Instances

Beim Starten einer Instance erstellen wir ein Root-Volume für die Instance. Beim Starten einer Instance enthält das Root-Volume das Image, das zum Starten der Instance verwendet wird. Jede Instance hat ein einzelnes Root-Volume. Sie können Ihren Instances während oder nach dem Start Speicher-Volumes hinzufügen.

Anhand des AMI, das Sie beim Starten Ihrer Instance angeben, wird der Typ des Root-Volumes ermittelt. Sie können eine Instance entweder über ein Amazon-EBS-gestütztes AMI (Linux- und Windows-Instances) oder ein Amazon-S3-gestütztes AMI (nur Linux-Instances) starten. Es gibt erhebliche Unterschiede zwischen den Möglichkeiten der einzelnen AMI-Typen. Weitere Informationen zu diesen Unterschieden erhalten Sie unter Root-Volume-Typ.

Wir empfehlen Ihnen die Verwendung von Amazon EBS-gestützten AMIs, da diese Instances schneller gestartet werden und persistenten Speicher nutzen.

Wir behalten uns bestimmte Gerätenamen für Root-Volumes vor. Weitere Informationen finden Sie unter Gerätenamen für Volumes auf Amazon-EC2-Instances.

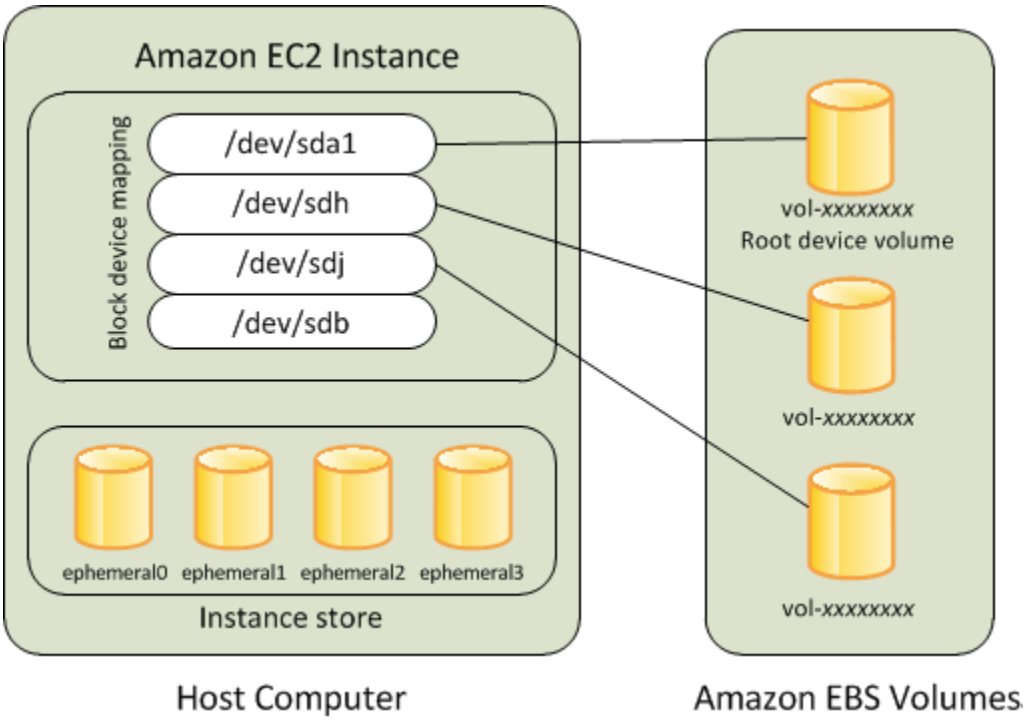
Inhalt

- Instances mit einem Amazon-EBS-Root-Volume
- Instances mit einem Instance-Speicher-Root-Volume (nur Linux-Instances)
- Behalten Sie ein Amazon-EBS-Root-Volume nach dem Beenden einer Amazon-EC2-Instance
- Ersetzen des Root-Volumes für eine Amazon-EC2-Instance, ohne sie anzuhalten

Instances mit einem Amazon-EBS-Root-Volume

An Instances, die Amazon EBS für das Root-Volume verwenden, wird automatisch ein Amazon EBS-Volume angefügt. Wenn Sie eine Instance mit einem Amazon-EBS-AMI starten, erstellen wir ein Amazon-EBS-Volume für jeden Amazon-EBS-Snapshot, auf den das AMI verweist. Optional können Sie je nach Instance-Typ weitere Amazon EBS-Volumes oder Instance-Speicher-Volumes nutzen.

Eine Instance mit einem EBS-Root-Volume kann angehalten und später neu gestartet werden, ohne dass sich dies auf die Daten auswirkt, die in den angehängten Volumes gespeichert sind. Sie können verschiedene Aufgaben für Instances und Volumes ausführen, wenn sich eine Instance mit einem EBS-Root-Volume im angehaltenen Status befindet. Sie können beispielsweise die Eigenschaften der Instance ändern, ihre Größe ändern oder den verwendeten Kernel aktualisieren oder Sie können ihr Root-Volume an eine andere laufende Instance anhängen, z. B. zum Debuggen. Weitere Informationen finden Sie unter Amazon-EBS-Volumes.



Einschränkung

Sie können `st1`- oder `sc1`-EBS-Volumes nicht als Root-Volumes verwenden.

Instance-Ausfall

Wenn eine Instance mit einem EBS-Root-Volume ausfällt, können Sie Ihre Sitzung mit einer der folgenden Methoden wiederherstellen:

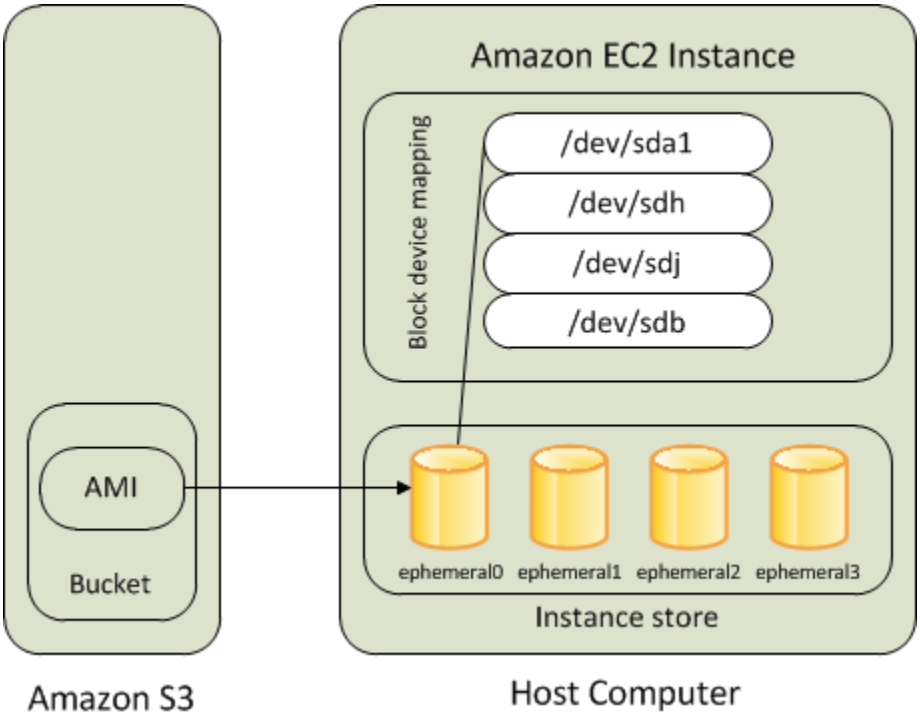
- Führen Sie das Anhalten und anschließend das erneute Starten durch. (Probieren Sie es zuerst mit dieser Methode.)
- Erstellen Sie einen automatischen Snapshot aller relevanten Volumes und erstellen Sie ein neues AMI. Weitere Informationen finden Sie unter Ein Amazon-EBS-gestütztes AMI erstellen.
- Fügen Sie das Volume an die neue Instance an, indem Sie die folgenden Schritte ausführen:
  1. Erstellen Sie einen Snapshot des Stamm-Volumes.
  2. Registrieren Sie ein neues AMI, indem Sie den Snapshot verwenden.
  3. Starten Sie über das neue AMI eine neue Instance.
  4. Trennen Sie die restlichen Amazon EBS-Volumes von der alten Instance.
  5. Fügen Sie die Amazon EBS-Volumes wieder an die neue Instance an.

Instances mit einem Instance-Speicher-Root-Volume (nur Linux-Instances)

> **Note**
>
> Windows-Instances unterstützen keine Instance-Speicher-Root-Volumes.

Instances, die Instance-Speicher für das Root-Volume verwenden, verfügen automatisch über mindestens ein Instance-Speicher-Volume, wobei ein Volume als Root-Volume dient. Wenn eine Instance von einem Amazon-S3-gestützten AMI aus gestartet wird, wird das AMI auf das Root-Volume kopiert. Beachten Sie, dass sie je nach Instance-Typ optional weitere Instance-Speicher-Volumes nutzen können.

Alle Daten auf den Instance-Speicher-Volumes werden so lange beibehalten, wie die Instance ausgeführt wird. Diese Daten werden jedoch gelöscht, wenn die Instance beendet wird (Instances mit einem Instance-Speicher-Root-Volume unterstützen die Aktion zum Anhalten nicht) oder ausfällt (z. B. bei Problemen auf einem zugrunde liegenden Laufwerk). Weitere Informationen finden Sie unter Instance-Speicher temporärer Speicher auf Blockebene für EC2-Instances.



Unterstützte Instance-Typen

Nur die folgenden Instance-Typen unterstützen ein Instance-Speichervolume als Root-Volume: C1, C3, D2, I2, M1, M2, M3, R3, und X1.

Instance-Ausfall

Nachdem eine Instance mit einem Instance-Speicher-Root-Volume ausfällt oder beendet wird, kann sie nicht wiederhergestellt werden. Wenn Sie planen, eine Instance mit einem Instance-Speicher-Root-Volume zu verwenden, empfehlen wir Ihnen dringend, die Daten auf Ihren Instance-Speicher-Volumes auf mehrere Availability Zones zu verteilen. Außerdem sollten Sie regelmäßig kritische Daten von Ihren Instance-Speicher-Volumes auf persistenten Speicher sichern.

Behalten Sie ein Amazon-EBS-Root-Volume nach dem Beenden einer Amazon-EC2-Instance

Standardmäßig wird das Amazon-EBS-Root-Volume für eine Instance gelöscht, wenn die Instance beendet wird. Sie können das Standardverhalten ändern, um sicherzustellen, dass das Amazon-EBS-Root-Volume nach dem Beenden der Instance weiterhin besteht. Legen Sie das Attribut `DeleteOnTermination` auf `false` fest, um das Standardverhalten zu ändern. Sie können dies entweder beim Start der Instance oder zu einem späteren Zeitpunkt tun.

Aufgaben

- Konfigurieren des Root-Volumes für Persistenz während des Instance-Starts
- Konfigurieren des Root-Volumes für Persistenz für eine vorhandene Instance
- Bestätigen, dass ein Root-Volume für Persistenz konfiguriert ist

Konfigurieren des Root-Volumes für Persistenz während des Instance-Starts

Sie können das Root-Volume so konfigurieren, dass es bestehen bleibt, wenn Sie eine Instance starten.

Console

So konfigurieren Sie das Root-Volume, dass es beim Starten einer Instance bestehen bleibt

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und Instances starten aus.
3. Wählen Sie ein Amazon Machine Image (AMI) aus, klicken Sie auf einen Instance-Typ, wählen Sie ein Schlüsselpaar und konfigurieren Sie Ihre Netzwerkeinstellungen.
4. Wählen Sie unter Speicher konfigurieren die Option Erweitert aus.
5. Erweitern Sie das Root-Volume.
6. Für Beim Beenden löschen wählen Sie Nein aus.
7. Wenn Sie die Konfiguration Ihrer Instance abgeschlossen haben, wählen Sie Instance starten.

AWS CLI

So konfigurieren Sie das Root-Volume, dass es beim Starten einer Instance bestehen bleibt

Verwenden Sie den Befehl run-instances und fügen Sie die folgende Option hinzu.

```
--block-device-mappings file://mapping.json
```

Geben Sie unter `mapping.json` eine Blockgerät-Zuweisung an, die das Attribut `DeleteOnTermination` auf `false` festlegt.

```
[
```

```
    {
        "DeviceName": "/dev/sda1",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
]
```

PowerShell

So konfigurieren Sie das Root-Volume, dass es beim Starten einer Instance bestehen bleibt

Verwenden Sie das cmdlet New-EC2Instance und fügen Sie den folgenden Parameter hinzu.

```
-BlockDeviceMapping $bdm
```

Erstellen Sie eine Blockgerät-Zuweisung, die das Attribut `DeleteOnTermination` auf `$false` festlegt.

```
$ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
$ebs.DeleteOnTermination = $false
$bdm = New-Object Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "dev/xvda"
$bdm.Ebs = $ebs
```

Konfigurieren des Root-Volumes für Persistenz für eine vorhandene Instance

Sie können das Root-Volume so konfigurieren, dass es für eine laufende Instance bestehen bleibt. Beachten Sie, dass Sie diese Aufgabe nicht mit der Amazon-EC2-Konsole vervollständigen können.

AWS CLI

So konfigurieren Sie das Root-Volume, damit es für eine vorhandene Instance bestehen bleibt

Verwenden Sie den Befehl modify-instance-attribute mit einer Blockgerät-Zuweisung, mit der das `DeleteOnTermination`-Attribut auf `false` festgelegt wird.

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --block-device-mappings file://mapping.json
```

Geben Sie in Folgendes a `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
]
```

PowerShell

So konfigurieren Sie das Root-Volume, damit es für eine vorhandene Instance bestehen bleibt

Verwenden Sie das cmdlet Edit-EC2InstanceAttribute mit einer Blockgerät-Zuweisung, mit der das Attribut `DeleteOnTermination` auf `$false` festgelegt wird.

```
$ebs = New-Object Amazon.EC2.Model.EbsInstanceBlockDeviceSpecification
$ebs.DeleteOnTermination = $false
$bdm = New-Object Amazon.EC2.Model.InstanceBlockDeviceMappingSpecification
$bdm.DeviceName = "/dev/xvda"
$bdm.Ebs = $ebs
Edit-EC2InstanceAttribute `
    -InstanceId i-1234567890abcdef0 `
    -BlockDeviceMapping $bdm
```

Bestätigen, dass ein Root-Volume für Persistenz konfiguriert ist

Sie können bestätigen, dass ein Root-Volume für Persistenz konfiguriert ist

Console

So bestätigen Sie, dass ein Root-Volume für Persistenz konfiguriert ist

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und wählen Sie dann die Instance aus.
3. Suchen Sie auf der Registerkarte Speicher unter Blockgeräte den Eintrag für das Stammvolume. Wenn Bei Beendigung löschen auf No gesetzt ist, wird das Volume so konfiguriert, dass es bestehen bleibt.

AWS CLI

So bestätigen Sie, dass ein Root-Volume für Persistenz konfiguriert ist

Verwenden Sie den Befehl describe-instances und stellen Sie sicher, dass das Attribut `DeleteOnTermination` auf `false` festgelegt ist.

```
aws ec2 describe-instances \
    --instance-id i-1234567890abcdef0 \
    --query "Reservations[].Instances[].BlockDeviceMappings"
```

Es folgt eine Beispielausgabe.

```
[
    [
        {
            "DeviceName": "/dev/xvda",
            "Ebs": {
                "AttachTime": "2024-07-12T04:05:33.000Z",
                "DeleteOnTermination": false,
                "Status": "attached",
                "VolumeId": "vol-1234567890abcdef0"

        }
    ]
]
```

PowerShell

So bestätigen Sie, dass ein Root-Volume für Persistenz konfiguriert ist

Verwenden Sie das cmdlet Get-EC2Instance und stellen Sie sicher, dass das Attribut `DeleteOnTermination` auf `False` festgelegt ist.

```
(Get-EC2Instance -InstanceId i-
i-1234567890abcdef0).Instances.BlockDeviceMappings.Ebs
```

Es folgt eine Beispielausgabe.

```
AssociatedResource  :
AttachTime          : 7/12/2024 4:05:33 AM
```

```
DeleteOnTermination : False
Operator            :
Status              : attached
VolumeId            : vol-1234567890abcdef0
```

Ersetzen des Root-Volumes für eine Amazon-EC2-Instance, ohne sie anzuhalten

Amazon EC2 ermöglicht es Ihnen, das Stamm-Amazon-EBS-Volume für eine ausgeführte Instance zu ersetzen und dabei Folgendes beizubehalten:

- In Instance-Speicher-Volumes gespeicherte Daten – Instance-Speicher-Volumes bleiben der Instance zugeordnet, nachdem das Root-Volume wiederhergestellt wurde.
- Auf Amazon-EBS-Daten-Volumes (Nicht-Stamm-Volumes) gespeicherte Daten – Nicht-Stamm-Volumes von Amazon EBS bleiben an die Instance angefügt, nachdem das Stamm-Volume wiederhergestellt worden ist.
- Netzwerkkonfiguration — Alle Netzwerkschnittstellen bleiben mit der Instance verbunden und behalten ihre IP-Adressen, Kennungen und Anhangs-IDs bei. Wenn die Instance verfügbar wird, wird der gesamte ausstehende Netzwerkverkehr gelöscht. Darüber hinaus bleibt die Instance auf demselben physischen Host, so dass sie ihre öffentlichen und privaten IP-Adressen und ihren DNS-Namen beibehält.
- IAM-Richtlinien — IAM-Profile und -richtlinien (wie Tag (Markierung)-basierte Richtlinien), die mit der Instance verknüpft sind, werden beibehalten und durchgesetzt.

Inhalt

- Wie der Ersatz des Root-Volumes funktioniert
- Überlegungen
- Ersetzen eines Stammvolumen

Wie der Ersatz des Root-Volumes funktioniert

Wenn Sie das Root-Volume für eine Instance ersetzen, wird eine Aufgabe zum Ersetzen des Root-Volumes erstellt. Das ursprüngliche Stamm-Volume wird von der Instance abgetrennt und das neue Stamm-Volume wird an seiner Stelle an die Instance angefügt. Die Blockgerät-Zuweisung der Instance wird aktualisiert, sodass sie die ID des Ersatz-Stamm-Volumes wiedergibt.

Wenn Sie das Root-Volume für eine Instance ersetzen, müssen Sie die Quelle des Snapshots für das neue Volume angeben. Es sind folgende Optionen möglich.

Startzustand eines Root-Volumes wiederherstellen

Diese Option ersetzt das aktuelle Root-Volume durch ein Volume, das auf dem Snapshot basiert, mit dem es erstellt wurde.

Überlegungen zur Verwendung des Startstatus

Das Ersatz-Stamm-Volume erhält denselben Typ, dieselbe Größe und dieselben Attribute zum Löschen bei Beendigung wie das ursprüngliche Stamm-Volume.

Das Root-Volume mithilfe eines Snapshots ersetzen

Diese Option ersetzt das aktuelle Root-Volume durch ein Ersatz-Volume, das auf dem von Ihnen angegebenen Snapshot basiert. Zum Beispiel ein bestimmter Snapshot, den Sie zuvor von diesem Root-Volume erstellt haben. Dies ist nützlich, wenn Sie Probleme beheben müssen, die durch eine Beschädigung des Root-Volumes oder durch Netzwerkkonfigurationsfehler im Gastbetriebssystem verursacht wurden.

Das Ersatz-Stamm-Volume erhält denselben Typ, dieselbe Größe und dieselben Attribute zum Löschen bei Beendigung wie das ursprüngliche Stamm-Volume.

Überlegungen zur Verwendung eines Snapshots

- Sie können nur Snapshots verwenden, die direkt aus den aktuellen oder früheren Root-Volumes der Instance erstellt wurden.
- Sie können keine Snapshot-Kopien verwenden, die aus Snapshots erstellt wurden, die vom Stammvolume entnommen wurden.
- Nachdem Sie das Root-Volume erfolgreich ersetzt haben, können Sie immer noch Snapshots des ursprünglichen Root-Volumes verwenden, um das neue (Ersatz-)Root-Volume zu ersetzen.

Ersetzen eines Root-Volumes unter Verwendung eines AMIs

Diese Option ersetzt das aktuelle Root-Volume mithilfe eines von Ihnen angegebenen AMIs. Dies ist nützlich, wenn Sie Patches oder Upgrades für das Betriebssystem und die Anwendungen durchführen müssen. Das AMI muss denselben Produktcode, dieselben Rechnungsinformationen, denselben Architekturtyp und denselben Virtualisierungstyp haben wie die Instance.

Wenn die Instance für ENA oder sriov-net aktiviert ist, müssen Sie ein AMI verwenden, das diese Features unterstützt. Wenn die Instance nicht für ENA oder sriov-net aktiviert ist, können Sie entweder ein AMI auswählen, das diese Features nicht unterstützt, oder Sie können automatisch die Unterstützung hinzufügen, wenn Sie ein AMI auswählen, das ENA oder sriov-net unterstützt.

Wenn die Instance für NitroTPM aktiviert ist, müssen Sie ein AMI verwenden, für das NitroTPM aktiviert ist. Die NitroTPM-Unterstützung ist nicht aktiviert, wenn die Instance nicht dafür konfiguriert wurde, unabhängig vom ausgewählten AMI.

Sie können ein AMI mit einem anderen Start-Modus als dem der Instance auswählen, solange die Instance den Start-Modus des AMI unterstützt. Wenn die Instance den Start-Modus nicht unterstützt, schlägt die Anforderung fehl. Wenn die Instance den Start-Modus unterstützt, wird der neue Start-Modus an die Instance weitergegeben und ihre UEFI-Daten werden entsprechend aktualisiert. Wenn Sie die Start-Reihenfolge manuell geändert oder einen privaten UEFI-Sicherheits-Start-Schlüssel zum Laden privater Kernel-Module hinzugefügt haben, gehen die Änderungen beim Ersetzen des Stamm-Volumes verloren.

Das Ersatz-Stamm-Volume erhält denselben Volume-Typ und dasselbe Löschen-bei-Beendigung-Attribut wie das ursprüngliche Stamm-Volume und erhält die Größe der AMI-Stamm-Volume-Blockgerät-Zuweisung.

> **Note**
>
> Die Größe der AMI-Stamm-Volume-Blockgerät-Zuweisung muss der Größe des ursprünglichen Stamm-Volumes entsprechen. Wenn die Größe der Blockgerät-Zuweisung des AMI Stamm-Volumes kleiner als die Größe des ursprünglichen Stamm-Volumes ist, schlägt die Anforderung fehl.

Nachdem die Stamm-Volume-Ersetzungsaufgabe abgeschlossen ist, werden die folgenden neuen und aktualisierten Informationen widergespiegelt, wenn Sie die Instance mithilfe der Konsole, AWS CLI oder AWS-SDKs beschreiben:

- Neue AMI-ID
- Neue Volume-ID für das Stamm-Volume
- Aktualisierte Start-Modus-Konfiguration (sofern vom AMI geändert)
- Aktualisierte NitroTPM-Konfiguration (sofern vom AMI aktiviert)

- Aktualisierte ENA-Konfiguration (sofern vom AMI aktiviert)
- Aktualisierte sriov-net-Konfiguration (sofern vom AMI aktiviert)

Die neue AMI-ID spiegelt sich auch in den Instance-Metadaten wider.

Überlegungen zur Verwendung eines AMI:

- Wenn Sie ein AMI verwenden, das über mehrere Blockgerät-Zuweisungen verfügt, wird nur das Stamm-Volume des AMI verwendet. Die anderen (Nicht-Stamm-)Volumes werden ignoriert.
- Sie können dieses Feature nur verwenden, wenn Sie über Berechtigungen für das AMI und den zugehörigen Root-Volume-Snapshot verfügen. Sie können dieses Feature nicht mit AWS Marketplace-AMIs verwenden.
- Sie können ein AMI ohne Produktcode nur verwenden, wenn die Instance über keinen Produktcode verfügt.
- Die Größe der AMI-Stamm-Volume-Blockgerät-Zuweisung muss der Größe des ursprünglichen Stamm-Volumes entsprechen. Wenn die Größe der Blockgerät-Zuweisung des AMI Stamm-Volumes kleiner als die Größe des ursprünglichen Stamm-Volumes ist, schlägt die Anforderung fehl.
- Die Instance-Identitätsdokumente für die Instance werden automatisch aktualisiert.
- Wenn die Instance NitroTPM unterstützt, werden die NitroTPM-Daten für die Instance zurückgesetzt und neue Schlüssel generiert.

Sie können wählen, ob das ursprüngliche Root-Volume nach Abschluss des Root-Volume-Ersetzungsprozesses erhalten bleiben soll. Wenn Sie nach Abschluss des Ersetzungsvorgangs das ursprüngliche Stamm-Volume löschen, wird das ursprüngliche Stamm-Volume automatisch gelöscht und ist nicht mehr wiederherstellbar. Wenn Sie sich dafür entscheiden, das ursprüngliche Root-Volume nach Abschluss des Vorgangs beizubehalten, bleibt das Volume in Ihrem Konto bereitgestellt. Sie müssen das Volume manuell löschen, wenn Sie es nicht mehr benötigen.

Die Aufgabe zum Ersetzen des Root-Volumes wechselt während des Vorgangs durch die folgenden Status:

- `pending` – das Ersatzvolume wird erstellt.
- `in-progress` – das ursprüngliche Volume wird abgelöst und das Ersatzvolume wird angehängt.
- `succeeded` – das Ersatzvolume wurde erfolgreich an die Instance angehängt und die Instance ist verfügbar.

- `failing` – Die Ersetzungsaufgabe ist im Begriff fehlzuschlagen.
- `failed` – Die Ersetzungsaufgabe ist fehlgeschlagen, aber das Root-Volume ist immer noch angefügt.
- `failing-detached` – Die Ersetzungsaufgabe ist im Begriff fehlzuschlagen und der Instance ist möglicherweise kein Root-Volume angefügt.
- `failed-detached` – Die Ersetzungsaufgabe ist fehlgeschlagen und der Instance ist kein Root-Volume angefügt.

Wenn die Aufgabe zum Ersetzen des Stamm-Volumes fehlschlägt, wird die Instance neu gestartet und das ursprüngliche Stamm-Volume bleibt mit der Instance verbunden.

Überlegungen

Bevor Sie beginnen, überlegen Sie folgendes.

Voraussetzungen

- Die Instance muss sich im Status `running` befinden.
- Die Instance wird während des Vorgangs automatisch neu gestartet. Der Inhalt des Arbeitsspeichers (RAM) wird während des Neustarts gelöscht. Es sind keine manuellen Neustarts erforderlich.
- Sie können das Stamm-Volume nicht ersetzen, wenn es sich um ein Instance-Speicher-Volume handelt. Nur Instances mit Amazon-EBS-Stamm-Volumes werden unterstützt.
- Sie können das Stamm-Volume für alle virtualisierten Instance-Typen und Bare-Metal-Instances von EC2 Mac ersetzen. Alle anderen Bare-Metal-Instance-Typen werden nicht unterstützt.
- Sie können nur Snapshots verwenden, die direkt aus den aktuellen oder früheren Root-Volumes der Instance erstellt wurden.
- Wenn Ihr Konto in der aktuellen Region standardmäßig für die Amazon-EBS-Verschlüsselung aktiviert ist, wird das Ersatz-Root-Volume, das durch die Aufgabe zum Ersetzen des Root-Volumes erstellt wird, immer verschlüsselt, unabhängig vom Verschlüsselungsstatus des angegebenen Snapshots oder des Root-Volumes des angegebenen AMI.

Verschlüsselungsergebnisse

In der folgenden Tabelle werden die möglichen Verschlüsselungsergebnisse zusammengefasst.

	Ursprüngliches Stamm-Volume	Angegebener Snapshot oder AMI	Standardmäßige Verschlüsselung	Stamm-Volume-Ersatz	Verschlüsselungsschlüssel, der für das Ersatz-Root-Volume verwendet wird
Wiederherstellen des Startstatus des Ersatz-Root-Volumes	Encrypted	Nicht zutreffend	Nicht berücksichtigt	Encrypted	Derselbe KMS-Schlüssel wie das ursprüngliche Root-Volume
	Unverschlüsselt	Nicht zutreffend	Disabled	Unverschlüsselt	Nicht zutreffend
	Unverschlüsselt	Nicht zutreffend	Aktiviert	Encrypted	Der Standard-KMS-Schlüssel des Kontos für die Amazon-EBS-Verschlüsselung
Wiederherstellen des Ersatz-Root-Volumes aus Snapshot oder AMI	Encrypted	Unverschlüsselt	Nicht berücksichtigt	Encrypted	Derselbe KMS-Schlüssel wie das ursprüngliche Root-Volume
	Encrypted	Encrypted	Nicht berücksichtigt	Encrypted	Derselbe KMS-Schlüssel wie das ursprüngliche Root-Volume

	Ursprüngliches Stamm-Volume	Angegebener Snapshot oder AMI	Standardmäßige Verschlüsselung	Stamm-Volume-Ersatz	Verschlüsselungsschlüssel, der für das Ersatz-Root-Volume verwendet wird
	Unverschlüsselt	Unverschlüsselt	Disabled	Unverschlüsselt	Nicht zutreffend
	Unverschlüsselt	Unverschlüsselt	Aktiviert	Encrypted	Der Standard-KMS-Schlüssel des Kontos für die Amazon-EBS-Verschlüsselung

	Ursprüngliches Stamm-Volume	Angegebener Snapshot oder AMI	Standardmäßige Verschlüsselung	Stamm-Volume-Ersatz	Verschlüsselungsschlüssel, der für das Ersatz-Root-Volume verwendet wird
	Unverschlüsselt	Encrypted	Nicht berücksichtigt	Encrypted	Wenn das AMI oder der Snapshot Eigentum des Kontos ist, wird das Ersatz-Volume mit dem KMS-Schlüssel des AMI oder Snapshots verschlüsselt. Wenn AMI oder Snapshot für das Konto freigegeben werden, wird das Ersatz-Volume mit dem Standard-KMS-Schlüssel des Kontos für die Amazon-EBS-Verschl

	Ursprüngliches Stamm-Volume	Angegebener Snapshot oder AMI	Standardmäßige Verschlüsselung	Stamm-Volume-Ersatz	Verschlüsselungsschlüssel, der für das Ersatz-Root-Volume verwendet wird
					üsselung verschlüselt.

Ersetzen eines Stammvolumen

Wenn Sie das Stamm-Volume für eine Instance ersetzen, wird eine Aufgabe zum Ersetzen des Stamm-Volumes erstellt. Sie können die Aufgabe zum Ersetzen des Stamm-Volumes verwenden, um den Fortschritt und das Ergebnis des Ersetzungsvorgangs zu überwachen.

Console

So ersetzen Sie das Stamm-Volume

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus, für die das Stamm-Volume ersetzt werden soll, und wählen Sie Actions (Aktionen), Monitor and troubleshoot (Überwachen und Fehlerbehebung) und Replace root volume (Stamm-Volume ersetzen).

   > **Note**
   >
   > Die Replace root volume (Ersetzen des Root-Volumes)-Aktion ist deaktiviert, wenn sich die ausgewählte Instance nicht im Zustand `running` befindet.

4. Wählen Sie für Wiederherstellen eine der folgenden Optionen aus:

   - Startstatus – Das Root-Volume Ersatz aus dem Snapshot wiederherstellen, der zum Erstellen des aktuellen Root-Volumes verwendet wurde.

- Snapshot – Das Ersatz-Root-Volume auf dem von Ihnen angegebenen Snapshot wiederherstellen. Wählen Sie für Snapshot den zu verwendenden Snapshot aus.
- Image – Stellen Sie das Ersatz-Root-Volume mithilfe des von Ihnen angegebenen AMI wieder her. Wählen Sie für Image das zu verwendende AMI aus.

5. (Optional) Für die Volume-Initialisierungsrate können Sie die Rate für die von Amazon EBS bereitgestellte Volume-Initialisierung (Volume-Initialisierungsrate) in MiB/s angeben, mit der die Snapshot-Blöcke von Amazon S3 auf das Volume heruntergeladen werden sollen. Weitere Informationen finden Sie unter Verwendung einer von Amazon EBS bereitgestellte Rate für die Volume-Initialisierung. Um die Standard-Initialisierungsrate oder die schnelle Snapshot-Wiederherstellung zu verwenden (sofern sie für den ausgewählten Snapshot aktiviert ist), geben Sie keine Rate an.
6. (Optional) Um das Root-Volume zu löschen, das Sie ersetzen, wählen Sie Ersetztes Root-Volume löschen aus.
7. Wählen Sie Ersatzaufgabe erstellen aus.
8. Um die Ersatzaufgabe zu überwachen, wählen Sie die Registerkarte Speicher für die Instance und erweitern Sie Aktuelle Aufgaben zum Ersatz des Root-Volumes.

AWS CLI

So stellen Sie den Start-Status des Ersatz-Stamm-Volumes wieder her

Verwenden Sie den Befehl create-replace-root-volume-task. Geben Sie für `--instance-id` die ID der Instance an, für die das Stamm-Volume ersetzt werden soll. Lassen Sie die Parameter `--snapshot-id` und `--image-id` aus. Um das ursprüngliche Stamm-Volume zu löschen, nachdem es ersetzt wurde, schließen Sie `--delete-replaced-root-volume` ein und geben Sie `true` an. Um die Volume-Initialisierungsrate anzugeben, mit der die Snapshot-Blöcke von Amazon S3 auf das Volume heruntergeladen werden, geben Sie für `--volume-initialization-rate` einen Wert zwischen `100` und `300` MiB/s an.

```
aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--delete-replaced-root-volume \
--volume-initialization-rate 150
```

So stellen Sie das Ersatz-Stamm-Volume auf einem bestimmten Snapshot wieder her

Verwenden Sie den Befehl create-replace-root-volume-task . Geben Sie für `--instance-id` die ID der Instance an, für die das Stamm-Volume ersetzt werden soll. Geben Sie für `--snapshot-id` die ID des zu verwendenden Snapshots an. Um das ursprüngliche Stamm-Volume zu löschen, nachdem es ersetzt wurde, schließen Sie `--delete-replaced-root-volume` ein und geben Sie `true` an. Um die Volume-Initialisierungsrate anzugeben, mit der die Snapshot-Blöcke von Amazon S3 auf das Volume heruntergeladen werden, geben Sie für `--volume-initialization-rate` einen Wert zwischen `100` und `300` MiB/s an.

```
aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--snapshot-id snap-9876543210abcdef0 \
--delete-replaced-root-volume \
--volume-initialization-rate 150
```

So stellen Sie das Ersatz-Stamm-Volume mithilfe eines AMI wieder her

Verwenden Sie den Befehl create-replace-root-volume-task. Geben Sie für `--instance-id` die ID der Instance an, für die das Stamm-Volume ersetzt werden soll. Geben Sie für `--image-id` die ID des zu verwendenden AMI an. Um das ursprüngliche Stamm-Volume zu löschen, nachdem es ersetzt wurde, schließen Sie `--delete-replaced-root-volume` ein und geben Sie `true` an. Um die Volume-Initialisierungsrate anzugeben, mit der die Snapshot-Blöcke von Amazon S3 auf das Volume heruntergeladen werden, geben Sie für `--volume-initialization-rate` einen Wert zwischen `100` und `300` MiB/s an.

```
aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--image-id ami-09876543210abcdef \
--delete-replaced-root-volume \
--volume-initialization-rate 150
```

So zeigen Sie den Status einer Aufgabe zum Stammvolumenersatz an

Verwenden Sie den Befehl describe-replace-root-volume-tasks und geben Sie die IDs der Aufgaben zum Stammvolumenersatz an, die angezeigt werden sollen.

```
aws ec2 describe-replace-root-volume-tasks \
    --replace-root-volume-task-ids replacevol-1234567890abcdef0 \
    --query ReplaceRootVolumeTasks[].TaskState
```

Es folgt eine Beispielausgabe.

```
[
    "succeeded"
]
```

Geben Sie alternativ den `instance-id`-Filter an, um die Ergebnisse nach Instances zu filtern.

```
$ aws ec2 describe-replace-root-volume-tasks \
    --filters Name=instance-id,Values=i-1234567890abcdef0
```

PowerShell

So stellen Sie den Start-Status des Ersatz-Stamm-Volumes wieder her

Verwenden Sie den Befehl New-EC2ReplaceRootVolumeTask. Geben Sie für `-InstanceId` die ID der Instance an, für die das Stamm-Volume ersetzt werden soll. Lassen Sie die Parameter `-SnapshotId` und `-ImageId` aus. Um das ursprüngliche Stamm-Volume zu löschen, nachdem es ersetzt wurde, schließen Sie `-DeleteReplacedRootVolume` ein und geben Sie `$true` an. Um die Volume-Initialisierungsrate anzugeben, mit der die Snapshot-Blöcke von Amazon S3 auf das Volume heruntergeladen werden, geben Sie für `-VolumeInitializationRate` einen Wert zwischen `100` und `300` MiB/s an.

```
New-EC2ReplaceRootVolumeTask `
    -InstanceId i-1234567890abcdef0 `
    -VolumeInitializationRate 150 `
    -DeleteReplacedRootVolume $true
```

So stellen Sie das Ersatz-Stamm-Volume auf einem bestimmten Snapshot wieder her

Verwenden Sie den Befehl New-EC2ReplaceRootVolumeTask. Geben Sie für `--InstanceId` die ID der Instance an, für die das Stamm-Volume ersetzt werden soll. Geben Sie für `-SnapshotId` die ID des zu verwendenden Snapshots an. Um das ursprüngliche Stamm-Volume zu löschen, nachdem es ersetzt wurde, schließen Sie `-DeleteReplacedRootVolume` ein und geben Sie `$true` an. Um die Volume-Initialisierungsrate anzugeben, mit der die Snapshot-Blöcke von Amazon S3 auf das Volume heruntergeladen werden, geben Sie für `-VolumeInitializationRate` einen Wert zwischen `100` und `300` MiB/s an.

```
New-EC2ReplaceRootVolumeTask `
    -InstanceId i-1234567890abcdef0 `
    -SnapshotId snap-9876543210abcdef0 `
    -VolumeInitializationRate 150 `
```

```
    -DeleteReplacedRootVolume $true
```

So stellen Sie das Ersatz-Stamm-Volume mithilfe eines AMI wieder her

Verwenden Sie den Befehl New-EC2ReplaceRootVolumeTask. Geben Sie für `-InstanceId` die ID der Instance an, für die das Stamm-Volume ersetzt werden soll. Geben Sie für `-ImageId` die ID des zu verwendenden AMI an. Um das ursprüngliche Stamm-Volume zu löschen, nachdem es ersetzt wurde, schließen Sie `-DeleteReplacedRootVolume` ein und geben Sie `$true` an. Um die Volume-Initialisierungsrate anzugeben, mit der die Snapshot-Blöcke von Amazon S3 auf das Volume heruntergeladen werden, geben Sie für `-VolumeInitializationRate` einen Wert zwischen `100` und `300` MiB/s an.

```
New-EC2ReplaceRootVolumeTask `
    -InstanceId i-1234567890abcdef0 `
    -ImageId ami-0abcdef1234567890 `
    -VolumeInitializationRate 150 `
    -DeleteReplacedRootVolume $true
```

So zeigen Sie den Status einer Aufgabe zum Stammvolumenersatz an

Verwenden Sie den Befehl Get-EC2ReplaceRootVolumeTask und geben Sie die IDs der Aufgaben zum Ersetzen des Root-Volumes an, die angezeigt werden sollen.

```
(Get-EC2ReplaceRootVolumeTask `
    -ReplaceRootVolumeTaskIds replacevol-1234567890abcdef0).TaskState.Value
```

Es folgt eine Beispielausgabe.

```
Succeeded
```

Geben Sie alternativ den `instance-id`-Filter an, um die Ergebnisse nach Instances zu filtern.

```
PS C:\> Get-EC2ReplaceRootVolumeTask -Filters @{Name = 'instance-id'; Values =
 'i-1234567890abcdef0'} | Format-Table
```

Gerätenamen für Volumes auf Amazon-EC2-Instances

Wenn Sie an Ihre Instance ein Volume anfügen, vergeben Sie einen Gerätenamen für das Volume. Dieser Gerätename wird von Amazon EC2 verwendet. Der Blockgeräte-Treiber für die Instance weist

beim Mounten des Volumes den tatsächlichen Volume-Namen zu. Dieser zugewiesene Name kann sich von dem Namen unterscheiden, den Amazon EC2 verwendet.

Die Anzahl der Volumes, die Sie Ihre Instance unterstützen kann, wird vom Betriebssystem bestimmt. Weitere Informationen finden Sie unter Amazon EBS-Volumenlimits für Amazon-Instances EC2 .

Inhalt

- Verfügbare Gerätenamen
- Überlegungen zu Gerätenamen

Verfügbare Gerätenamen

Linux-Instances

Für Linux-Instances sind zwei Virtualisierungtypen verfügbar: Paravirtual (PV) und Hardware Virtual Machine (HVM). Der Virtualisierungtyp einer Instance wird durch das AMI bestimmt, das zum Starten der Instance verwendet wird. Alle Instance-Typen unterstützen HVM-AMIs. Einige Instance-Typen früherer Generationen unterstützen PV-AMIs. Notieren Sie sich den Virtualisierungstyp Ihres AMI, weil die empfohlenen und verfügbaren Gerätenamen, die Sie verwenden können, vom Virtualisierungstyp Ihrer Instance abhängig sind. Weitere Informationen finden Sie unter Virtualisierungstypen.

Die folgende Tabelle führt die verfügbaren Gerätenamen auf, die Sie in einer Blockgerätezuordnung oder beim Anhängen eines EBS-Volumes verwenden können.

Virtualisierungstyp	Verfügbar	Reserviert für Stamm-Volume	Empfohlen für EBS-Daten-Volumes	Instance-Speicher-Volumes
Paravirtual	/dev/sd[a-z] /dev/sd[a-z][1-15] /dev/hd[a-z] /dev/hd[a-z][1-15]	/dev/sda1	/dev/sd[f-p] /dev/sd[f-p][1-6]	/dev/sd[b-e]

Virtualisierungstyp	Verfügbar	Reserviert für Stamm-Volume	Empfohlen für EBS-Daten-Volumes	Instance-Speicher-Volumes
HVM (Hardware gestützte virtuelle Maschine)	/dev/sd[a-z] /dev/xvd[a-c][a-z] /dev/xvdd[a-x]	Unterschiedlich nach AMI /dev/sda1 or /dev/xvda	/dev/sd[b-z] /dev/xvdb[b-z] *	/dev/sd[b-e] /dev/sd[b-h] (h1.16xlarge) /dev/sd[b-y] (d2.8xlarge) /dev/sd[b-i] (i2.8xlarge) **

*Die Gerätenamen, die Sie in einer Blockgerätezuordnung für NVMe-EBS-Volumes angeben, werden durch NVMe-Gerätenamen ersetzt (`/dev/nvme[0-26]n1`). Der Blockgerät-Treiber kann NVMe-Gerätenamen in einer anderen Reihenfolge zuweisen, als Sie es für die Volumes in der Blockgerät-Zuweisung angegeben haben.

** NVMe-Instance-Speicher-Volumes werden automatisch aufgezählt und ihnen wird ein NVMe-Gerätename zugeordnet.

Windows-Instances

AWS Windows AMIs verwenden eine der folgenden Treibergruppen, um Zugriff auf virtualisierte Hardware zu erlauben:

- AWS PV: Paravirtual-Treiber für Windows-Instances
- AWS NVMe: AWS NVMe-Treiber

Gerätenamen für Nitro-basierte Instances

Die folgende Tabelle führt die verfügbaren Gerätenamen auf, die Sie in einer Blockgerät-Zuweisung oder beim Anhängen eines EBS-Volumes an eine Nitro-basierte Instance verwenden können.

Treibertyp	Verfügbar	Reserviert für Stamm-Volume	Empfohlen für EBS-Volumes	Instance-Speicher-Volumes
AWS NVMe	xvd[a-z] xvd[a-c][a-z] xvdd[a-x] /dev/sda1	/dev/sda1	xvd[b-z] xvdb[b-z]	*

* NVMe-Instance-Speicher-Volumes werden automatisch aufgezählt und ihnen wird ein Windows-Laufwerksbuchstabe zugeordnet.

Gerätenamen für Xen-basierte Instances

Die folgende Tabelle führt die verfügbaren Gerätenamen auf, die Sie in einer Blockgerät-Zuweisung oder beim Anhängen eines EBS-Volumes an eine Xen-basierte Instance verwenden können.

Treibertyp	Verfügbar	Reserviert für Stamm-Volume	Empfohlen für EBS-Volumes	Instance-Speicher-Volumes
AWS PV	xvd[b-z] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd[f-z]	xvdc[a-x] xvd[a-e]
Citrix PV (nicht mehr unterstützt)	xvd[b-z] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd[f-z]	xvdc[a-x] xvd[a-e]

Treibertyp	Verfügbar	Reserviert für Stamm-Volume	Empfohlen für EBS-Volumes	Instance-Speicher-Volumes
Red Hat PV (nicht mehr unterstützt)	xvd[a-z] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd[f-p]	xvdc[a-x] xvd[a-e]

Weitere Informationen zu Instance-Speicher-Volumes finden Sie unter Instance-Speicher temporärer Speicher auf Blockebene für EC2-Instances. Weitere Informationen zu NVMe EBS-Volumes (nitrobasierte Instances), einschließlich der Identifizierung des EBS-Geräts, finden Sie unter Amazon EBS und NVMe im Benutzerhandbuch für Amazon EBS.

Überlegungen zu Gerätenamen

Bei der Auswahl eines Gerätenamens sollten Sie Folgendes beachten:

- Der letzte Teil der von Ihnen verwendeten Gerätenamen sollte sich nicht überschneiden, da dies zu Problemen beim Starten Ihrer Instance führen kann. Vermeiden Sie es beispielsweise, Kombinationen wie `/dev/xvdf` und `xvdf` für Volumes zu verwenden, die an dieselbe Instance angehängt sind.
- Obwohl Sie EBS-Volumes mit dem Gerätenamen anfügen können, der zum Anfügen von Instance-Speicher-Volumes verwendet wird, empfehlen wir dringend, dies nichts zu tun, da das Verhalten unberechenbar sein kann.
- Die Anzahl der NVMe-Instance-Speicher-Volumes für eine Instance ist abhängig von der Größe der Instance. NVMe-Instance-Speicher-Volumes werden automatisch aufgezählt und ihnen wird ein NVMe-Gerätename (Linux-Instances) oder ein Windows-Laufwerksbuchstabe (Windows-Instances) zugeordnet.
- (Windows-Instances) AWS-Windows-AMIs werden mit zusätzlicher Software geliefert, die eine Instance vorbereitet, wenn sie zum ersten Mal gestartet wird. Dies ist entweder der EC2Config-Service (Windows-AMIs vor Windows Server 2016) oder EC2Launch (Windows Server 2016 und höher). Nachdem den Geräten Laufwerksbuchstaben zugeordnet worden sind, werden sie initialisiert und gemountet. Das Stammlaufwerk wird als initialisiert und gemounte `C:`

\. Wenn ein EBS-Volume an eine Windows-Instance angefügt wird, kann es als beliebiger Laufwerksbuchstabe auf der Instance angezeigt werden. Sie können die Einstellungen ändern, um die Laufwerksbuchstaben der Volumes nach Ihren Spezifikationen anzupassen. Die Standardeinstellung für Instance-Speicher-Volumes hängt vom Treiber ab. AWS PV-Treiber und Citrix-PV-Treiber ordnen die Instance-Speicher-Volumes den Laufwerkbuchstaben von Z: nach A: zu. Red Hat-Treiber ordnen die Instance-Speicher-Volumes den Laufwerkbuchstaben von D: nach Z: zu. Weitere Informationen finden Sie unter Windows-Start-Agenten auf Amazon-EC2-Windows-Instances und Volumes für Amazon-EC2-Windows-Instances anhängen und zuordnen.

- (Linux-Instances) Je nach Blockgeräte-Treiber des Kernels kann das Gerät einem anderen als dem von Ihnen angegeben Namen zugeordnet werden. Beispiel: Falls Sie einen Gerätenamen von `/dev/sdh` angeben, könnte Ihr Gerät in `/dev/xvdh` oder `/dev/hdh` umbenannt werden. In den meisten Fällen bleibt der abschließende Buchstabe gleich. In einigen Versionen von Red Hat Enterprise Linux (und deren Varianten wie z. B. CentOS) kann der abschließende Buchstabe geändert werden (`/dev/sda` kann in `/dev/xvde` geändert werden). In diesen Fällen wird jeder abschließende Buchstabe entsprechend fortgeschrieben. Beispiel: Wenn `/dev/sdb` in `/dev/xvdf` umbenannt wird, dann wird `/dev/sdc` in `/dev/xvdg` umbenannt. Amazon Linux erstellt einen symbolischen Link für den Namen, den Sie für das umbenannte Gerät angegeben haben. Andere Betriebssysteme könnten sich anders verhalten.
- (Linux-Instances) HVM-AMIs unterstützen nicht die Nutzung von nachfolgenden Zahlen bei Gerätenamen, mit Ausnahme von `/dev/sda1`, das für das Root-Gerät reserviert ist, und `/dev/sda2`. Obwohl es möglich ist, `/dev/sda2` zu verwenden, wird die Nutzung dieser Gerätezuweisung mit HVM-Instances nicht empfohlen.
- (Linux-Instances) Wenn Sie PV-AMIs verwenden, können Sie keine Volumes anfügen, die dieselben Gerätebuchstaben mit und ohne nachfolgende Stellen haben. Wenn Sie beispielsweise ein Volume als `/dev/sdc` und ein anderes als `/dev/sdc1` anfügen, ist nur `/dev/sdc` für die Instance sichtbar. Um nachfolgende Stellen in Gerätenamen zu verwenden, müssen Sie bei allen Gerätenamen nachfolgende Stellen verwenden, die dieselben Grundbuchstaben haben (beispielsweise `/dev/sdc1`, `/dev/sdc2`, `/dev/sdc3`).
- (Linux-Instances) Bei einigen benutzerdefinierten Kernels ist die Verwendung möglicherweise auf `/dev/sd[f-p]` oder `/dev/sd[f-p][1-6]` beschränkt. Wenn Probleme bei der Verwendung von `/dev/sd[q-z]` oder `/dev/sd[q-z][1-6]` auftreten, versuchen Sie es mit `/dev/sd[f-p]` oder `/dev/sd[f-p][1-6]`.

Bevor Sie den Gerätenamen angeben, den Sie ausgewählt haben, vergewissern Sie sich, dass er verfügbar ist. Andernfalls erhalten Sie eine Fehlermeldung, dass der Gerätename bereits verwendet

wird. Um die Festplattengeräte und ihre Bereitstellungspunkte anzuzeigen, verwenden Sie den lsblk-Befehl (Linux-Instances), das Festplattenverwaltungsprogramm oder den diskpart-Befehl (Windows-Instances).

Blockgerät-Zuweisungen auf Amazon-EC2-Instances blockieren

Jede gestartete Instance hat ein zugeordnetes Root-Volume, entweder ein Amazon-EBS-Volume oder ein Instance-Speicher-Volume. Sie können mit der Blockgerät-Zuweisung zusätzliche EBS-Volumes oder Instance-Speicher-Volumes an eine Instance anhängen, wenn diese gestartet wird. Sie können ebenfalls zusätzliche EBS-Volumes an eine ausgeführte Instance anfügen. Die einzige Möglichkeit zum Anhängen von Instance-Speicher-Volumes an eine Instance ist die Blockgerät-Zuweisung, um die Volumes beim Start der Instance anzuhängen.

Inhalt

- Konzepte der Blockgerät-Zuweisung
- Blockgerät-Zuweisungen zu einem AMI hinzufügen
- Blockgerät-Zuweisungen zu Amazon-EC2-Instance hinzufügen

Konzepte der Blockgerät-Zuweisung

Ein Blockgerät ist ein Speichergerät, das Daten in Byte- bzw. Bit-Blöcken verschiebt. Diese Geräte unterstützen zufälligen Zugriff und verwenden im Allgemeinen I/O-Puffer. Beispiele sind Festplatten, CD-ROM-Laufwerke und Flashlaufwerke. Ein Blockgerät kann physisch mit einem Computer verbunden oder per Remotezugriff verwendet werden, so als ob es physikalisch mit dem Computer verbunden wäre.

Amazon EC2 unterstützt zwei Arten von Blockgeräten:

- Instance-Speicher-Volumes (virtuelle Geräte, deren physikalische Hardware mit dem Host-Computer für die Instance verbunden ist)
- EBS-Volumes (Remotespeichergeräte)

Eine Blockgerät-Zuweisung definiert die Blockgeräte (Instance-Speicher-Volumes und EBS-Volumes) zum Anfügen an eine Instance. Sie können eine Blockgerät-Zuweisung als Teil der Erstellung eines AMI angeben, sodass die Zuweisung von allen Instances verwendet wird, die vom AMI gestartet werden. Alternativ können Sie eine Blockgerät-Zuweisung zum Starten einer Instance angeben.

Diese Zuweisung gilt dann statt der im AMI angegebenen, von der aus die Instance gestartet wurde. Beachten Sie, dass alle von einem Instance-Typ unterstützen NVMe-Instance-Speicher-Volumes automatisch aufgezählt und beim Starten der Instance einem Gerätenamen zugeordnet werden. Die Aufnahme in Ihre Blockgerät-Zuweisung hat keine Auswirkung.

Inhalt

- Blockgerät-Zuweisungseinträge
- Blockgerät-Zuweisung – Instance-Speicher-Einschränkungen
- Beispiel einer Blockgerät-Zuweisung
- Bereitstellung von Geräten im Betriebssystem

Blockgerät-Zuweisungseinträge

Wenn Sie eine Blockgerät-Zuweisung erstellen, geben Sie die folgenden Informationen für jedes Blockgerät an, das der Instance angefügt werden soll:

- Der in Amazon EC2 verwendete Gerätename. Der Blockgerätetreiber für die Instance weist den tatsächlichen Volume-Namen beim Einbinden des Volumes zu. Der zugewiesene Name kann vom Namen abweichen, der von Amazon EC2 empfohlen wird. Weitere Informationen finden Sie unter Gerätenamen für Volumes auf Amazon-EC2-Instances.

Für Instance-Speichervolumes können Sie auch die folgenden Informationen angeben:

- Das virtuelle Gerät: `ephemeral[0-23]`. Die Anzahl und Größe der verfügbaren Instance-Speicher-Volumes für die Instance hängt vom Instance-Typ ab.

Für NVMe-Instance-Speichervolumes gelten auch die folgenden Informationen:

- Diese Volumes werden automatisch aufgezählt und beim Starten der Instance einem Gerätenamen zugeordnet. Die Aufnahme in Ihre Blockgerät-Zuweisung hat keine Auswirkung.

Für EBS-Volumes geben Sie auch die folgenden Informationen an:

- Die ID des zu verwendenden Snapshots zur Erstellung des Blockgeräts (snap-xxxxxxxx). Der Wert ist optional, sofern eine Volumengröße angegeben wird. Sie können die ID eines archivierten Snapshots nicht angeben.

- Die Größe des Volumes in GiB Die angegebene Größe muss größer oder genauso groß wie der angegebene Snapshot sein.
- Ob das Volume bei Beendigung der Instance gelöscht wird (`true` oder `false`). Der Standardwert ist `true` für das Root-Volume und `false` für angehängte Volumes. Wenn Sie ein AMI erstellen, erbt die Blockgerät-Zuweisung die Einstellung von der Instance. Wenn Sie eine Instance starten, erbt sie die Einstellung vom AMI.
- Der Volume-Typ. Dieser kann bei Allzweck-SSD `gp2` und `gp3`, bei SSD mit bereitgestellten IOPS `io1` und `io2`, bei durchsatzoptimierten HDD `st1`, bei Cold-HDD `sc1` und bei Magnetfestplatten `standard` sein.
- Die Anzahl der Ein/Ausgangs-Vorgänge pro Sekunde (IOPS), die das Volume unterstützt. (Wird nur mit `io1`- und `io2`-Volumes verwendet.)

Blockgerät-Zuweisung – Instance-Speicher-Einschränkungen

Beim Starten von Instances mit AMIs mit Instance-Speicher-Volumes in ihren Blockgerät-Zuweisungen müssen einige Einschränkungen beachtet werden.

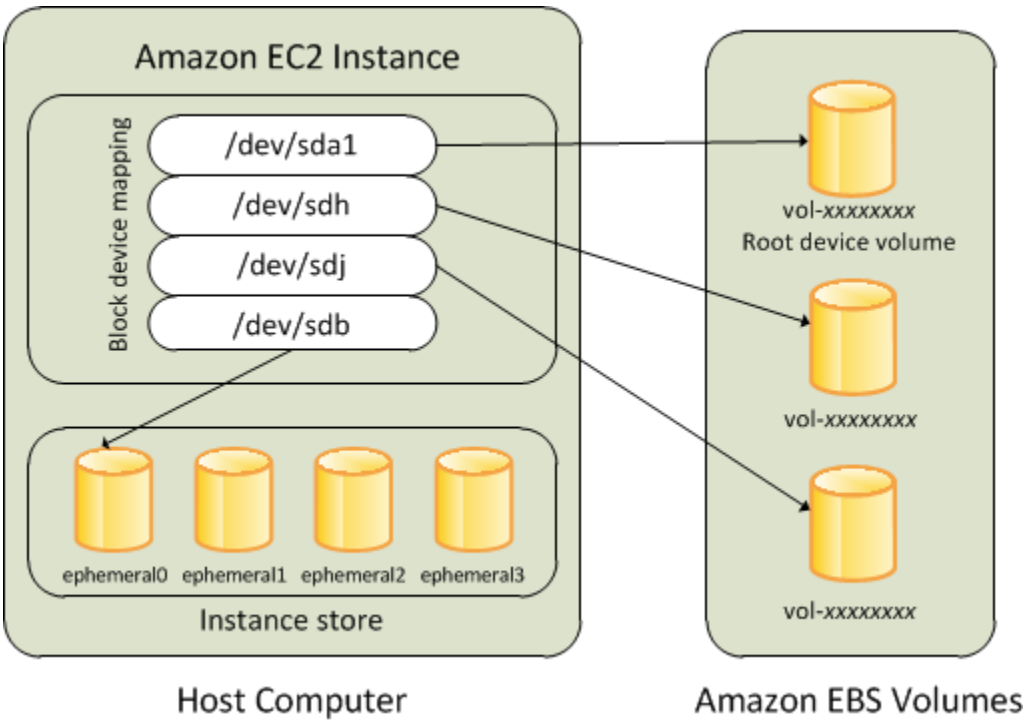
- Einige Instance-Typen enthalten mehr Instance-Speicher-Volumes als andere und bestimmte Instance-Typen enthalten überhaupt keine Instance-Speicher-Volumes. Wenn der Instance-Typ ein Instance-Speicher-Volume unterstützt und das AMI Zuweisungen für zwei Instance-Speicher-Volumes aufweist, wird die Instance mit einem Instance-Speicher-Volume gestartet.
- Instance-Speicher-Volumes können ausschließlich zum Startzeitpunkt zugewiesen werden. Sie können Instances nicht ohne Instance-Speicher-Volumes anhalten (z. B. `t2.micro`), die Instance zu einem Typ ändern, der Instance-Speicher-Volumes unterstützt, und anschließend die Instance mit Instance-Speicher-Volumes neustarten. Allerdings können Sie ein AMI aus der Instance erstellen, dieses mit einem Instance-Typ starten, der Instance-Speicher-Volumes unterstützt, und anschließend die Instance-Speicher-Volumes der Instance zuweisen.
- Wenn Sie eine Instance mit zugewiesenen Instance-Speicher-Volumes starten, anschließend die Instance anhalten und zu einem Instance-Typ mit weniger Instance-Speicher-Volumes ändern und neustarten, werden die Instance-Speicher-Volume-Zuweisungen in den Instance-Metadaten angezeigt. Allerdings ist nur die Höchstanzahl der unterstützten Instance-Speicher-Volumes für den Instance-Typ für die Instance verfügbar.

> **Note**
>
> Wenn eine Instance angehalten wird, gehen alle Daten auf den Instance-Speicher-Volumes verloren.

- Je nach Instance-Speicher-Kapazität zum Startzeitpunkt können M3-Instances AMI-Instance-Speicher-Blockgerät-Zuweisungen beim Start ignorieren, sofern sie nicht beim Start angegeben werden. Geben Sie Instance-Speicher-Blockgerät-Zuweisungen zum Startzeitpunkt an, selbst wenn beim gestarteten AMI die Instance-Speicher-Volumes im AMI zugewiesen sind, um sicherzustellen, dass die Instance-Speicher-Volumes beim Starten der Instance verfügbar sind.

Beispiel einer Blockgerät-Zuweisung

Diese Abbildung zeigt ein Beispiel für eine Blockgerät-Zuweisung für eine EBS-Backed-Instance. Sie weist `/dev/sdb` zu `ephemeral0` und zwei EBS-Volumes zu: eines zu `/dev/sdh` und ein weiteres zu `/dev/sdj`. Dieser Wert zeigt außerdem das EBS-Volume, das das Root-Volume ist: `/dev/sda1`.



Hinweis: Dieses Beispiel für Blockgerät-Zuweisung wird in den Beispielbefehlen und APIs in diesem Thema verwendet. Beispielbefehle und APIs zur Erstellung von Blockgerät-Zuweisungen finden Sie in Angeben einer Blockgerät-Zuweisung für ein AMI und Aktualisieren der Blockgerät-Zuweisung beim Starten einer Instance.

Bereitstellung von Geräten im Betriebssystem

Gerätenamen wie `/dev/sdh` und `xvdh` werden von Amazon EC2 zum Beschreiben von Blockgeräten verwendet. Die Blockgerät-Zuweisung dient in Amazon EC2 zum Angeben der Blockgeräte zum Hinzufügen zu einer EC2 Instance. Nach dem Anfügen eines Blockgeräts zu einer Instance muss es vom Betriebssystem aufgespielt werden, bevor Sie auf das Speichergerät zugreifen können. Wenn ein Blockgerät von einer Instance getrennt wird, wird die Bereitstellung vom Betriebssystem aufgehoben und Sie können nicht mehr auf das Speichergerät zugreifen.

Linux-Instances – Die in der Blockgerät-Zuweisung angegebenen Namen werden den entsprechenden Blockgeräten beim ersten Hochfahren der Instance zugewiesen. Die Instance-Typen bestimmen, welche Instance-Speicher-Volumes standardmäßig formatiert und aufgespielt werden. Sie können zusätzliche Instance-Speicher-Volumes zum Startzeitpunkt aufspielen, sofern die Anzahl der für den Instance-Typ verfügbaren Instance-Speicher-Volumes nicht überschritten wird. Weitere Informationen finden Sie unter Instance-Speicher temporärer Speicher auf Blockebene für EC2-Instances. Der Blockgerät-Treiber für die Instance bestimmt, welche Geräte beim Formatieren und Aufspielen der Volumes verwendet werden.

Windows-Instances – Die in der Blockgerät-Zuweisung angegebenen Namen werden den entsprechenden Blockgeräten beim ersten Hochfahren der Instance zugewiesen. Anschließend startet der Ec2Config-Service die Laufwerke und spielt sie auf. Der Root-Volume wird als `C:\` aufgespielt. Die Instance-Speicher-Volumes werden als `Z:\`, `Y:\` aufgespielt usw. Zum Aufspielen eines EBS-Volume kann ein beliebiger verfügbarer Laufwerkbuchstabe verwendet werden. Sie können die Art der Zuweisung von Laufwerkbuchstaben zu EBS-Volumes jedoch konfigurieren. Weitere Informationen finden Sie unter the section called “Windows-Start-Agenten”.

Blockgerät-Zuweisungen zu einem AMI hinzufügen

Jedes AMI weist eine Blockgerät-Zuweisung auf, die die Blockgeräte angibt, die einer Instance beim Start des AMI angefügt werden sollen. Um einem AMI mehr Blockgeräte hinzuzufügen, müssen Sie Ihr eigenes AMI erstellen.

Inhalt

- Angeben einer Blockgerät-Zuweisung für ein AMI
- Anzeigen der EBS-Volumes in einer AMI-Blockgerät-Zuweisung

Angeben einer Blockgerät-Zuweisung für ein AMI

Beim Erstellen eines AMI können Volumes zusätzlich zum Root-Volume auf zwei Arten angegeben werden. Wenn Sie bereits Volumes einer ausgeführten Instance vor dem Erstellen eines AMI von der Instance angefügt haben, enthält die Blockgerät-Zuweisung für das AMI dieselben Volumes. Im Fall von EBS-Volumes werden die bestehenden Daten in einem neuen Snapshot gespeichert. Dieser neue Snapshot wird dann in der Blockgerät-Zuweisung angegeben. Im Fall von Instance-Speicher-Volumes werden die Daten nicht gespeichert.

Im Fall von EBS-Backed AMIs können Sie EBS-Volumes und Instance-Speicher-Volumes mit Blockgerät-Zuweisung hinzufügen. Im Fall von Amazon-S3-gestützten AMIs können Sie Instance-Speicher-Volumes nur durch Änderung der Blockgerät-Zuweisungs-Einträge in der Image-Manifestdatei beim Registrieren des Images hinzufügen.

> **Note**
>
> Geben Sie für M3-Instances die Instance-Speicher-Volumes in der Blockgerät-Zuweisung für die Instance an, wenn Sie diese starten. Wenn Sie eine M3-Instance starten, werden in der Blockgerät-Zuweisung für das AMI angegebene Instance-Speicher-Volumes möglicherweise ignoriert, wenn sie nicht als Teil der Instance-Blockgerät-Zuweisung angegeben werden.

Console

So fügen Sie Volumes zu einem AMI hinzu

1. Öffnen Sie die Amazon EC2-Konsole.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie eine Instance und anschließend Actions (Aktionen), Image and templates (Image und Vorlagen), Create Image (Image erstellen) aus.
4. Geben Sie einen Namen und eine Beschreibung für das neue Image ein.
5. Die Instance-Volumes werden unter Instance volumes (Instance-Volumes) angezeigt. Um ein weiteres Volume hinzuzufügen, wählen Sie Add volume (Volume hinzufügen).
6. Wählen Sie unter Volume type (Volume-Type) den Volume-Typen aus. Wählen Sie für Device (Gerät) den Gerätenamen aus. Für ein EBS-Volume können Sie zusätzliche Details wie einen Snapshot, eine Volume-Größe, einen Volume-Typ, IOPS und einen Verschlüsselungsstatus angeben.

7. Wählen Sie Create Image (Image erstellen) aus.

AWS CLI

So fügen Sie Volumes zu einem AMI hinzu

Verwenden Sie den Befehl create-image zum Angeben einer Blockgerät-Zuweisung für ein EBS-gestütztes AMI. Verwenden Sie den Befehl register-image zum Angeben einer Blockgerät-Zuweisung für ein Amazon-S3-gestütztes AMI.

Geben Sie die Blockgerät-Zuweisung mit dem `--block-device-mappings`-Parameter an. Sie können in JSON kodierte Argumente direkt in der Befehlszeile oder durch Verweisen auf eine JSON-Datei festlegen, wie hier gezeigt.

```
--block-device-mappings file://mapping.json
```

Verwenden Sie das folgende Mapping, um ein Instance-Speicher-Volume hinzuzufügen. Beachten Sie, dass NVMe-Instance-Speicher-Volumes automatisch hinzugefügt werden.

```
{
    "DeviceName": "device_name",
    "VirtualName": "ephemeral0"
}
```

Verwenden Sie das folgende Mapping, um ein leeres 100 GiB--Volume hinzuzufügen:

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

Verwenden Sie das folgende Mapping, um ein EBS-Volume basierend auf einem Snapshot hinzuzufügen.

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "SnapshotId": "snap-1234567890abcdef0"
```

```
    }
}
```

Um das Mapping für ein Gerät auszulassen, verwenden Sie das folgende Mapping.

```
{
    "DeviceName": "device_name",
    "NoDevice": ""
}
```

PowerShell

Verwenden Sie das cmdlet New-EC2Image zum Angeben einer Blockgerät-Zuweisung für ein EBS-gestütztes AMI. Verwenden Sie das cmdlet Register-EC2Image zum Angeben einer Blockgerät-Zuweisung für ein Amazon-S3-gestütztes AMI.

Fügen Sie die Option `-BlockDeviceMapping` hinzu und geben Sie die Updates in `bdm` an:

```
-BlockDeviceMapping $bdm
```

Die folgende Zuordnung fügt ein Volume basierend auf einem Snapshot hinzu.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.SnapshotId = "snap-1234567890abcdef0"
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "device_name"
$bdm.Ebs = $ebd
```

Die folgende Zuordnung fügt ein leeres 100-GiB-Volume hinzu.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.VolumeSize = 100
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "device_name"
$bdm.Ebs = $ebd
```

Anzeigen der EBS-Volumes in einer AMI-Blockgerät-Zuweisung

Sie können die EBS-Volumes in der Blockgerät-Zuweisung für ein AMI leicht aufzählen.

Console

So zeigen Sie die EBS-Volumes für ein AMI an

1. Öffnen Sie die Amazon EC2-Konsole.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie EBS images (EBS-Images) in der Liste Filter aus, um eine Liste der EBS-Backed AMIs abzurufen.
4. Wählen Sie das gewünschte AMI aus und rufen Sie die Registerkarte Details auf. Für das Root-Volume (wobei der Begriff Root-Gerät dem Root-Volume entspricht) sind mindestens die folgenden Informationen verfügbar:

   - Root Device Type (Root-Gerätetyp (`ebs`)
   - Root Device Name (Root-Gerätename) (Beispiel: `/dev/sda1`)
   - Block Devices (Blockgeräte) (z. B. `/dev/sda1=snap-1234567890abcdef0:8:true`)

   Wenn das AMI mit zusätzlichen EBS-Volumes mit einer Blockgerät-Zuweisung erstellt wurde, wird im Feld Block Devices (Blockgeräte) ebenfalls die Zuweisung für diese zusätzlichen Volumes angezeigt. (Dieser Bildschirm zeigt keine Instance-Speicher-Volumes an.)

AWS CLI

So zeigen Sie die EBS-Volumes für ein AMI an

Verwenden Sie den Befehl describe-images.

```
aws ec2 describe-images \
    --image-ids ami-0abcdef1234567890 \
    --query Image[0].BlockDeviceMappings
```

PowerShell

So zeigen Sie die EBS-Volumes für ein AMI an

Verwenden Sie das cmdlet Get-EC2Image.

```
(Get-EC2Image -ImageId ami-0abcdef1234567890).BlockDeviceMappings
```

Blockgerät-Zuweisungen zu Amazon-EC2-Instance hinzufügen

Standardmäßig enthält eine gestartete Instance ein in der Blockgerät-Zuweisung der AMI, in der die Instance gestartet wurde, angegebenes Speichergerät. Alternativ können Sie Änderungen an der Blockgerät-Zuweisung für eine Instance bei deren Start angeben. Diese Aktualisierungen überschreiben dann die Blockgerät-Zuweisung der AMI bzw. werden in diese integriert.

Einschränkungen

- Im Fall des Root-Volumes kann ausschließlich Folgendes geändert werden: Volume-Größe, Volume-Typ und das Bei Beendigung löschen-Flag.
- Wenn Sie ein EBS-Volume ändern, können Sie dessen Größe verringern. Geben Sie deshalb einen Snapshot an, dessen Größe der in der Blockgerät-Zuweisung des AMI angegebenen entspricht bzw. größer als diese ist.

Aufgaben

- Aktualisieren der Blockgerät-Zuweisung beim Starten einer Instance
- Aktualisieren der Blockgerät-Zuweisung einer ausgeführten Instance
- Anzeigen der EBS-Volumes in einer Instance-Blockgerät-Zuweisung
- Anzeigen der Instance-Blockgerät-Zuweisung für Instance-Speicher-Volumes

Aktualisieren der Blockgerät-Zuweisung beim Starten einer Instance

Sie können EBS-Volumes und Instance-Speicher-Volumes beim Starten zu einer Instance hinzufügen. Hinweis: Durch das Aktualisieren der Blockgerät-Zuweisung für eine Instance wird die Blockgerät-Zuweisung des AMI, von der sie gestartet wurde, nicht dauerhaft geändert.

Console

So aktualisieren Sie die Volumes für eine Instance beim Start

1. Befolgen Sie den Schritten zum Starten einer Instance, aber starten Sie die Instance erst, nachdem Sie die folgenden Schritte durchgeführt haben, um die Volumes zu ändern.
2. (Optional) Um ein Volume hinzuzufügen, wählen Sie Speicher konfigurieren, Neues Volume hinzufügen. Wählen Sie die Volume-Größe und den Volume-Typ aus.
3. (Optional) Um ein Volume zu unterdrücken, das durch die Blockgerät-Zuweisung des AMI angegeben wurde, wählen Sie Speicher konfigurieren, Entfernen aus.

4. (Optional) Um die Konfiguration eines EBS-Volumes zu ändern, wählen Sie im Bereich Speicher konfigurieren die Option Erweitert aus. Erweitern Sie die Informationen für das Volume und nehmen Sie die gewünschten Änderungen vor.
5. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten.

AWS CLI

So aktualisieren Sie die Volumes für eine Instance beim Start

Verwenden den Befehl run-instances mit der Option `--block-device-mappings`.

```
--block-device-mappings file://mapping.json
```

Beispiel: Angenommen eine AMI-Blockgerät-Zuweisung gibt Folgendes an:

- `/dev/xvda` – EBS-Root-Volume
- `/dev/sdh` – EBS-Volume erstellt von `snap-1234567890abcdef0`
- `/dev/sdj` – Leeres EBS-Volume mit einer Größe von `100`
- `/dev/sdb` – Instance-Speicher-Volume `ephemeral0`

Nehmen wir an, die Instance-Blockgerät-Zuweisung in `mapping.json` ist wie folgt.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 100
        }
    },
    {
        "DeviceName": "/dev/sdj",
        "NoDevice": ""
    },
    {
        "DeviceName": "/dev/sdh",
        "Ebs": {
            "VolumeSize": 300
```

```
        }
    },
    {
        "DeviceName": "/dev/sdc",
        "VirtualName": "ephemeral1"
    }
]
```

Die Instance-Blockgerät-Zuweisung bewirkt Folgendes:

- Überschreibt die Größe des Root-Volumes `/dev/xvda` und erhöht sie auf 100 GiB.
- Verhindert, dass `/dev/sdj` an die Instance angehängt wird.
- Überschreibt die Größe von `/dev/sdh` und erhöht sie auf 300 GiB. Beachten Sie, dass Sie die Snapshot-ID nicht erneut festlegen müssen.
- Fügt ein flüchtiges Volume `/dev/sdc` hinzu. Wenn der Instance-Typ nicht mehrere Instance-Speicher-Volumes unterstützt, hat dies keine Wirkung. Wenn der Instance-Typ NVMe-Instance-Speicher-Volumes unterstützt, werden diese automatisch aufgelistet und in die Instance-Blockgerät-Zuweisung aufgenommen, und können nicht überschrieben werden.

PowerShell

So aktualisieren Sie die Volumes für eine Instance beim Start

Verwenden Sie den Parameter `-BlockDeviceMapping` mit dem cmdlet New-EC2Instance mit dem Parameter `-BlockDeviceMapping`.

```
-BlockDeviceMapping $bdm
```

Nehmen wir an, die Instance-Blockgerät-Zuweisung in `$bdm` ist wie folgt.

```
$bdm = @()

$root = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$root.DeviceName = "/dev/xvda"
$ebs1 = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebs1.VolumeSize = 100
$root.Ebs = $ebs1
$bdm += $root

$sdj = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
```

```
$sdj.DeviceName = "/dev/sdj"
$sdj.NoDevice = ""
$bdm += $sdj

$sdh = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdh.DeviceName = "/dev/sdh"
$ebs2 = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebs2.VolumeSize = 300
$sdh.Ebs = $ebs2
$bdm += $sdh

$sdc = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$sdc.DeviceName = "/dev/sdc"
$sdc.VirtualName = "ephemeral1"
$bdm += $sdc
```

Die Instance-Blockgerät-Zuweisung bewirkt Folgendes:

- Überschreibt die Größe des Root-Volumes `/dev/xvda` und erhöht sie auf 100 GiB.
- Verhindert, dass `/dev/sdj` an die Instance angehängt wird.
- Überschreibt die Größe von `/dev/sdh` und erhöht sie auf 300 GiB. Beachten Sie, dass Sie die Snapshot-ID nicht erneut festlegen müssen.
- Fügt ein flüchtiges Volume `/dev/sdc` hinzu. Wenn der Instance-Typ nicht mehrere Instance-Speicher-Volumes unterstützt, hat dies keine Wirkung. Wenn der Instance-Typ NVMe-Instance-Speicher-Volumes unterstützt, werden diese automatisch aufgelistet und in die Instance-Blockgerät-Zuweisung aufgenommen, und können nicht überschrieben werden.

Aktualisieren der Blockgerät-Zuweisung einer ausgeführten Instance

Die Instance muss vor Änderung dieses Attributs nicht angehalten werden.

AWS CLI

So aktualisieren Sie die Blockgerät-Zuweisung einer ausgeführten Instance

Verwenden Sie den Befehl modify-instance-attribute.

Fügen Sie die Option `--block-device-mappings` hinzu:

```
--block-device-mappings file://mapping.json
```

Geben Sie unter `mapping.json` die Updates an. Das folgende Update ändert beispielsweise das Root-Volume, dass es bestehen bleibt.

```
[
  {
    "DeviceName": "/dev/sda1",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

PowerShell

So aktualisieren Sie die Blockgerät-Zuweisung einer ausgeführten Instance

Verwenden Sie das cmdlet Edit-EC2InstanceAttribute.

Fügen Sie die Option `-BlockDeviceMapping` hinzu:

```
-BlockDeviceMapping $bdm
```

Geben Sie unter `bdm` die Updates an. Das folgende Update ändert beispielsweise das Root-Volume, dass es bestehen bleibt.

```
$ebd = New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice
$ebd.DeleteOnTermination = false
$bdm = New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping
$bdm.DeviceName = "/dev/sda1"
$bdm.Ebs = $ebd
```

Anzeigen der EBS-Volumes in einer Instance-Blockgerät-Zuweisung

Sie können die EBS-Volumes, die einer Instance zugewiesen sind, leicht aufzählen.

Console

So zeigen Sie die EBS-Volumes für eine Instance an

1. Öffnen Sie die Amazon EC2-Konsole.

2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und sehen Sie sich Details auf der Registerkarte Speicher an. Für das Root-Volume (wobei der Begriff Root-Gerät dem Root-Volume entspricht) sind mindestens die folgenden Informationen verfügbar:

   - Root device type (Root-Gerätetyp) (zum Beispiel EBS)
   - Root device name (Root-Gerätename) (Beispiel: `/dev/xvda`)
   - Blockgeräte (z. B. `/dev/xvda`, `/dev/sdf` und `/dev/sdj`)

   Wenn die Instance mit zusätzlichen EBS-Volumes unter Verwendung einer Blockgeräte-Zuweisung gestartet wurde, werden diese unter Block devices (Blockgeräte) angezeigt. Auf dieser Registerkarte werden keine Instance-Speicher-Volumes angezeigt.
4. Um zusätzliche Informationen zu einem EBS-Volume anzuzeigen, wählen Sie seine Volume-ID aus, um zur Volume-Seite zu gelangen.

AWS CLI

So zeigen Sie die EBS-Volumes für eine Instance an

Verwenden Sie den Befehl describe-instances.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[*].Instances[0].BlockDeviceMappings
```

PowerShell

So zeigen Sie die EBS-Volumes für eine Instance an

Verwenden Sie das cmdlet Get-EC2Instance.

```
(Get-EC2Instance -InstanceId i-0bac57d7472c89bac).Instances.BlockDeviceMappings
```

Anzeigen der Instance-Blockgerät-Zuweisung für Instance-Speicher-Volumes

Der Instance-Typ bestimmt die Anzahl und Typ der Instance-Speicher-Volumes, die für die Instance verfügbar sind. Wenn die Anzahl der Instance-Speicher-Volumes in einer Blockgerät-Zuweisung

die für eine Instance verfügbare Anzahl an Instance-Speicher-Volumes übersteigt, werden die überzähligen Volumes ignoriert. Führen Sie zum Anzeigen der Instance-Speicher-Volumes für die Instance den lsblk-Befehl aus (Linux-Instances) oder öffnen Sie Windows Disk Management (Windows-Instances). Für Informationen zum Ermitteln der Anzahl an Instance-Speicher-Volumes, die von jedem Instance-Typ unterstützt werden, siehe Typspezifikationen für Amazon-EC2-Instances.

Wenn Sie die Blockgerät-Zuweisung für die Instance anzeigen, werden ausschließlich die EBS-Volumes und nicht die Instance-Speicher-Volumes angezeigt. Welche Methode Sie verwenden, um die Instance-Speicher-Volumes für die Instance anzuzeigen, hängt vom Volume-Typ ab.

NVMe-Instance-Speicher-Volumes

Linux-Instances

Sie können das NVMe-Befehlszeilenpaket nvme-cli verwenden, um die Speichervolumes der NVMe-Instance in der Blockgerätezuordnung abzufragen. Laden Sie das Paket herunter, installieren Sie es auf Ihrer Instance und führen Sie dann den folgenden Befehl aus.

```
[ec2-user ~]$ sudo nvme list
```

Nachstehend finden Sie eine Beispielausgabe für eine Instance. Der Text in der Spalte Modell gibt an, ob das Volume ein EBS-Volume oder ein Instance-Speicher-Volume ist. In diesem Beispiel sind sowohl `/dev/nvme1n1` als auch `/dev/nvme2n1` Instance-Speicher-Volumes.

```
Node             SN                   Model
 Namespace
---------------- -------------------- ----------------------------------------
 ---------
/dev/nvme0n1     vol06afc3f8715b7a597 Amazon Elastic Block Store               1

/dev/nvme1n1     AWS2C1436F5159EB6614 Amazon EC2 NVMe Instance Storage         1

/dev/nvme2n1     AWSB1F4FF0C0A6C281EA Amazon EC2 NVMe Instance Storage         1
  ...
```

Windows-Instances

Sie können Disk Management oder PowerShell verwenden, um sowohl EBS- als auch Instance-Speicher-NVMe-Volumes aufzulisten. Weitere Informationen finden Sie unter the section called “Zuweisen von NVMe-Festplatten zu Volumes”.

HDD- oder SSD-Instance-Speicher-Volumes

Sie können Instance-Metadaten verwenden, um HDD- oder SSD-Instance-Speicher-Volumes in der Blockgerät-Zuweisung abzufragen. NVMe-Instance-Speicher-Volumes sind in der Blockgerät-Zuweisung nicht enthalten.

Die Basis-URI für alle Instance-Metadaten-Anfragen ist `http://169.254.169.254/latest/`. Weitere Informationen finden Sie unter Verwenden Sie Instanz-Metadaten, um Ihre EC2 Instanz zu verwalten.

Linux-Instances

Stellen Sie zunächst eine Verbindung mit der ausgeführten Instance her. Rufen Sie von dieser Instance aus mithilfe der Abfrage die Blockgerät-Zuweisung ab.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/
```

Die Antwort enthält die Namen der Blockgeräte für die Instance. Die Ausgabe für eine Instance–Speicher basierte `m1.small`-Instance sieht beispielsweise folgendermaßen aus.

```
ami
ephemeral0
root
swap
```

Das `ami`-Gerät ist das Root-Volume wie es von der Instance erfasst wird. Die Instance-Speicher-Volumes werden nach dem Schema benann `ephemeral[0-23]`. Das `swap`-Gerät ist für die Seitendatei. Wenn Sie ebenfalls EBS-Volumes zugewiesen haben, werden sie als `ebs1`, `ebs2` usw. aufgeführt.

Um Details zu einzelnen Blockgeräten in der Blockgerät-Zuweisung abzurufen, hängen Sie den Namen wie hier gezeigt an die vorherige Abfrage an.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

Windows-Instances

Stellen Sie zunächst eine Verbindung mit der ausgeführten Instance her. Rufen Sie von dieser Instance aus mithilfe der Abfrage die Blockgerät-Zuweisung ab.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-mapping/
```

Die Antwort enthält die Namen der Blockgeräte für die Instance. Die Ausgabe für eine Instance–Speicher basierte `m1.small`-Instance sieht beispielsweise folgendermaßen aus.

```
ami
ephemeral0
root
swap
```

Das `ami`-Gerät ist das Root-Volume wie es von der Instance erfasst wird. Die Instance-Speicher-Volumes werden nach dem Schema benann `ephemeral[0-23]`. Das `swap`-Gerät ist für die Seitendatei. Wenn Sie ebenfalls EBS-Volumes zugewiesen haben, werden sie als `ebs1`, `ebs2` usw. aufgeführt.

Um Details zu einzelnen Blockgeräten in der Blockgerät-Zuweisung abzurufen, hängen Sie den Namen wie hier gezeigt an die vorherige Abfrage an.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

Volumes für Amazon-EC2-Windows-Instances anhängen und zuordnen

> **Note**
>
> Dieses Thema bezieht sich ausschließlich auf Windows-Instances.

Ihre Windows-Instance verfügt über ein EBS-Volume, das als Root-Volume dient. Wenn die Windows-Instance AWS PV- oder Citrix PV-Treiber verwendet, können Sie noch 25 weitere Volumes hinzufügen, sodass insgesamt 26 Volumes zugeordnet sind. Weitere Informationen finden Sie unter Amazon EBS-Volumenlimits für Amazon-Instances EC2 .

Je nach dem vorliegenden Instance-Typ können Sie Ihrer Instance zwischen 0 und 24 Instance-Speicher-Volumes zuordnen. Sie können die in einer Instance verfügbaren Instance-Speicher-Volumes verwenden, wenn Sie sie bei der Erstellung des entsprechenden AMIs oder beim Start der Instance angeben. Außerdem können Sie bei der Erstellung des entsprechenden AMIs oder beim Start der Instance weitere EBS-Volumes hinzufügen oder Sie ordnen sie zu, während die Instance ausgeführt wird.

Wenn Sie einer Instance ein Volume hinzufügen, geben Sie den Gerätenamen an, den Amazon EC2 verwendet. Weitere Informationen finden Sie unter Gerätenamen für Volumes auf Amazon-EC2-Instances. AWS Windows Amazon Machine Images (AMIs) enthalten eine Reihe von Treibern, mit denen Amazon EC2 dem Instance-Speicher und den EBS-Volumes Windows-Datenträger und -Laufwerkbuchstaben zuweist.

Methoden zum Zuordnen von Festplatten zu EBS-Volumes

- Zuweisen von NVMe-Festplatten zu Volumes in Ihrer Amazon-EC2-Windows-Instance
- Nicht-NVME-Festplatten auf Amazon-EC2-Windows-Instance Volumes zuordnen

Zuweisen von NVMe-Festplatten zu Volumes in Ihrer Amazon-EC2-Windows-Instance

Mit Nitro-basierenden Instances werden EBS-Volumes als NVMe-Blockgeräte angezeigt. In diesem Thema wird erklärt, wie Sie die NVMe-Festplatten anzeigen, die für das Windows-Betriebssystem in Ihrer Instance verfügbar sind. Außerdem wird gezeigt, wie diese NVMe-Festplatten den zugrunde liegenden Amazon-EBS-Volumes und den Gerätenamen zugeordnet werden, die für die von Amazon EC2 verwendeten Blockgerät-Zuweisungen angegeben wurden.

Themen

- NVMe-Festplatten auflisten
- NVMe-Festplatten zu Volumes zuweisen

NVMe-Festplatten auflisten

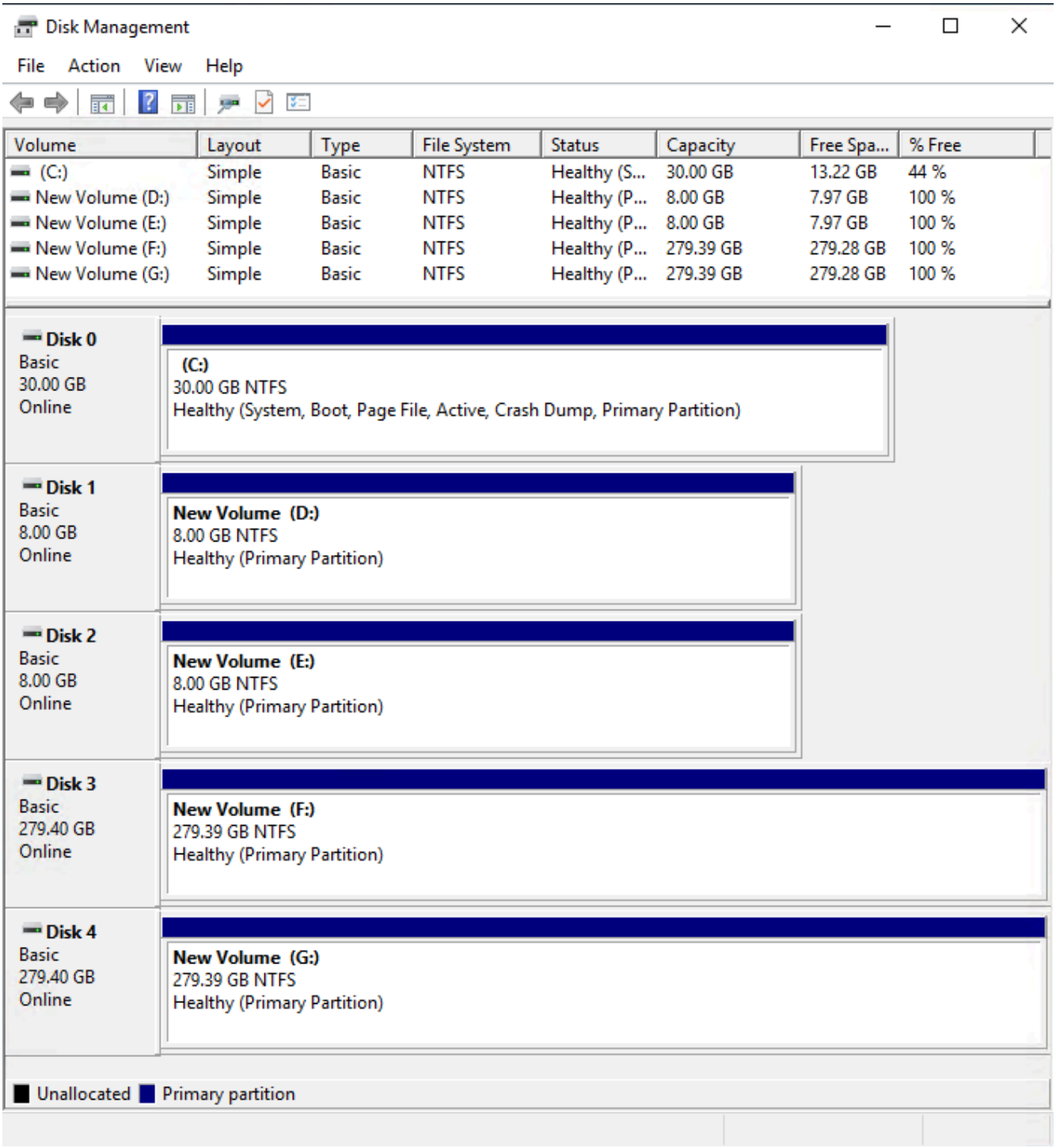
Sie können die Datenträger in Ihrer Windows-Instances auch mithilfe der Datenträgerverwaltung oder Powershell anzeigen.

Disk Management

So zeigen Sie die Datenträger in Ihrer Windows-Instance an

1. Melden Sie sich per Remotedesktop an Ihrer Windows-Instance an. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von RDP.
2. Starten Sie das Dienstprogramm für die Datenträgerverwaltung.
3. Überprüfen Sie die Datenträger. Das Root-Volume ist ein EBS-Volume, das unter gemountet is `C:\`. Wenn keine weiteren Datenträger angezeigt werden, haben Sie keine zusätzlichen Volumes angegeben, als Sie das AMI erstellt bzw. die Instance gestartet haben.

   Das folgende Beispiel zeigt die verfügbaren Datenträger beim Start einer `r5d.4xlarge`-Instance mit zwei zusätzlichen EBS-Volumes.



PowerShell

Das folgende PowerShell-Skript listet alle Datenträger und die entsprechenden Gerätenamen und Volumes auf. Es ist für die Verwendung mit Nitro-basierten Instances vorgesehen, die NVMe-EBS- und Instance-Speicher-Volumes verwenden.

Stellen Sie eine Verbindung mit Ihrer Windows-Instance her und führen Sie den folgenden Befehl aus, um die Ausführung von PowerShell-Skripts zu aktivieren.

```
Set-ExecutionPolicy RemoteSigned
```

Kopieren Sie das folgende Skript und speichern Sie es unter Ihrer Windows-Instance als `mapping.ps1`.

```
# List the disks for NVMe volumes

function Get-EC2InstanceMetadata {
    param([string]$Path)
    (Invoke-WebRequest -Uri "http://169.254.169.254/latest/$Path").Content
}

function GetEBSVolumeId {
    param($Path)
    $SerialNumber = (Get-Disk -Path $Path).SerialNumber
    if($SerialNumber -clike 'vol*'){
        $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("vol","vol-")
    }
    else {
       $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("AWS","AWS-")
    }
    return $EbsVolumeId
}

function GetDeviceName{
    param($EbsVolumeId)
    if($EbsVolumeId -clike 'vol*'){

        $Device  = ((Get-EC2Volume -VolumeId $EbsVolumeId ).Attachment).Device
        $VolumeName = ""
    }
     else {
        $Device = "Ephemeral"
        $VolumeName = "Temporary Storage"
    }
    Return $Device,$VolumeName
}

function GetDriveLetter{
    param($Path)
```

```
    $DiskNumber =  (Get-Disk -Path $Path).Number
    if($DiskNumber -eq 0){
        $VirtualDevice = "root"
        $DriveLetter = "C"
        $PartitionNumber = (Get-Partition -DriveLetter C).PartitionNumber
    }
    else
    {
        $VirtualDevice = "N/A"
        $DriveLetter = (Get-Partition -DiskNumber $DiskNumber).DriveLetter
        if(!$DriveLetter)
        {
            $DriveLetter = ((Get-Partition -DiskId $Path).AccessPaths).Split(",")[0]
        }
        $PartitionNumber = (Get-Partition -DiskId $Path).PartitionNumber
    }

    return $DriveLetter,$VirtualDevice,$PartitionNumber

}

$Report = @()
foreach($Path in (Get-Disk).Path)
{
    $Disk_ID = ( Get-Partition -DiskId $Path).DiskId
    $Disk = ( Get-Disk -Path $Path).Number
    $EbsVolumeId  = GetEBSVolumeId($Path)
    $Size =(Get-Disk -Path $Path).Size
    $DriveLetter,$VirtualDevice, $Partition = (GetDriveLetter($Path))
    $Device,$VolumeName = GetDeviceName($EbsVolumeId)
    $Disk = New-Object PSObject -Property @{
      Disk          = $Disk
      Partitions    = $Partition
      DriveLetter   = $DriveLetter
      EbsVolumeId   = $EbsVolumeId
      Device        = $Device
      VirtualDevice = $VirtualDevice
      VolumeName= $VolumeName
    }
 $Report += $Disk
}
```

```
$Report | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions,
 DriveLetter, EbsVolumeId, Device, VirtualDevice, VolumeName
```

Führen Sie das Skript wie folgt aus:

```
PS C:\> .\mapping.ps1
```

Im Folgenden finden Sie eine Beispielausgabe für eine Instance mit einem Root-Volume, zwei EBS-Volumes und zwei Instance-Speicher-Volumes.

```
Disk Partitions DriveLetter EbsVolumeId           Device    VirtualDevice VolumeName
---- ---------- ----------- -----------           ------    ------------- ----------
   0          1 C           vol-03683f1d861744bc7 /dev/sda1 root
   1          1 D           vol-082b07051043174b9 xvdb      N/A
   2          1 E           vol-0a4064b39e5f534a2 xvdc      N/A
   3          1 F           AWS-6AAD8C2AEEE1193F0 Ephemeral N/A           Temporary
 Storage
   4          1 G           AWS-13E7299C2BD031A28 Ephemeral N/A           Temporary
 Storage
```

Wenn Sie Ihre Anmeldeinformationen für Tools für Windows PowerShell für die Windows-Instance nicht konfiguriert haben, kann das Skript die EBS-Volume-ID nicht erhalten und verwendet N/A in der `EbsVolumeId`-Spalte.

NVMe-Festplatten zu Volumes zuweisen

Mit dem Befehl Get-Disk können Sie Windows-Festplattennummern an Amazon-EBS-Volumes und Instance-Speicher-Volumes von Amazon EC2 zuordnen.

```
PS C:\> Get-Disk
Number Friendly Name Serial Number                    HealthStatus
 OperationalStatus      Total Size Partition

                      Style
------ ------------ -------------                    ------------
 -----------------      ---------- ----------
3      NVMe Amazo... AWS6AAD8C2AEEE1193F0_00000001.   Healthy              Online
              279.4 GB MBR
4      NVMe Amazo... AWS13E7299C2BD031A28_00000001.   Healthy              Online
              279.4 GB MBR
```

```
2      NVMe Amazo... vol0a4064b39e5f534a2_00000001.   Healthy            Online
                8 GB MBR
0      NVMe Amazo... vol03683f1d861744bc7_00000001.   Healthy            Online
               30 GB MBR
1      NVMe Amazo... vol082b07051043174b9_00000001.   Healthy            Online
                8 GB MBR
```

Sie können auch den Befehl ebsnvme-id ausführen, um die NVMe-Datenträgernummern EBS-Volume-IDs und Gerätenamen zuzuordnen.

```
PS C:\> C:\PROGRAMDATA\Amazon\Tools\ebsnvme-id.exe
Disk Number: 0
Volume ID: vol-03683f1d861744bc7
Device Name: sda1

Disk Number: 1
Volume ID: vol-082b07051043174b9
Device Name: xvdb

Disk Number: 2
Volume ID: vol-0a4064b39e5f534a2
Device Name: xvdc
```

Nicht-NVME-Festplatten auf Amazon-EC2-Windows-Instance Volumes zuordnen

Wenn Sie eine Instance aus einem Windows-AMI starten, das AWS-PV- oder Citrix-PV-Treiber verwendet, können Sie die auf dieser Seite beschriebenen Beziehungen verwenden, um Ihre Windows-Datenträger Ihrem Instance-Speicher und Ihren EBS-Volumes zuzuweisen. In diesem Thema wird erklärt, wie Sie die Nicht-NVMe-Festplatten anzeigen, die für das Windows-Betriebssystem auf Ihrer Instance verfügbar sind. Außerdem wird gezeigt, wie diese Nicht-NVME-Festplatten den zugrunde liegenden Amazon-EBS-Volumes und den Gerätenamen zugeordnet werden, die für die von Amazon EC2 verwendeten Blockgerät-Zuweisungen angegeben wurden.

> **Note**
>
> Wenn das Windows-AMI Red-Hat-PV-Treiber verwendet, können Sie ein Upgrade Ihrer Instance für die Verwendung von Citrix-Treibern durchführen. Weitere Informationen finden Sie unter the section called “Upgrade für PV-Treiber”.

Themen

- Nicht-NVMe-Festplatten auflisten
- Nicht-NVME-Festplatten Volumes zuordnen

Nicht-NVMe-Festplatten auflisten

Sie können die Datenträger in Ihrer Windows-Instances auch mithilfe der Datenträgerverwaltung oder Powershell finden.

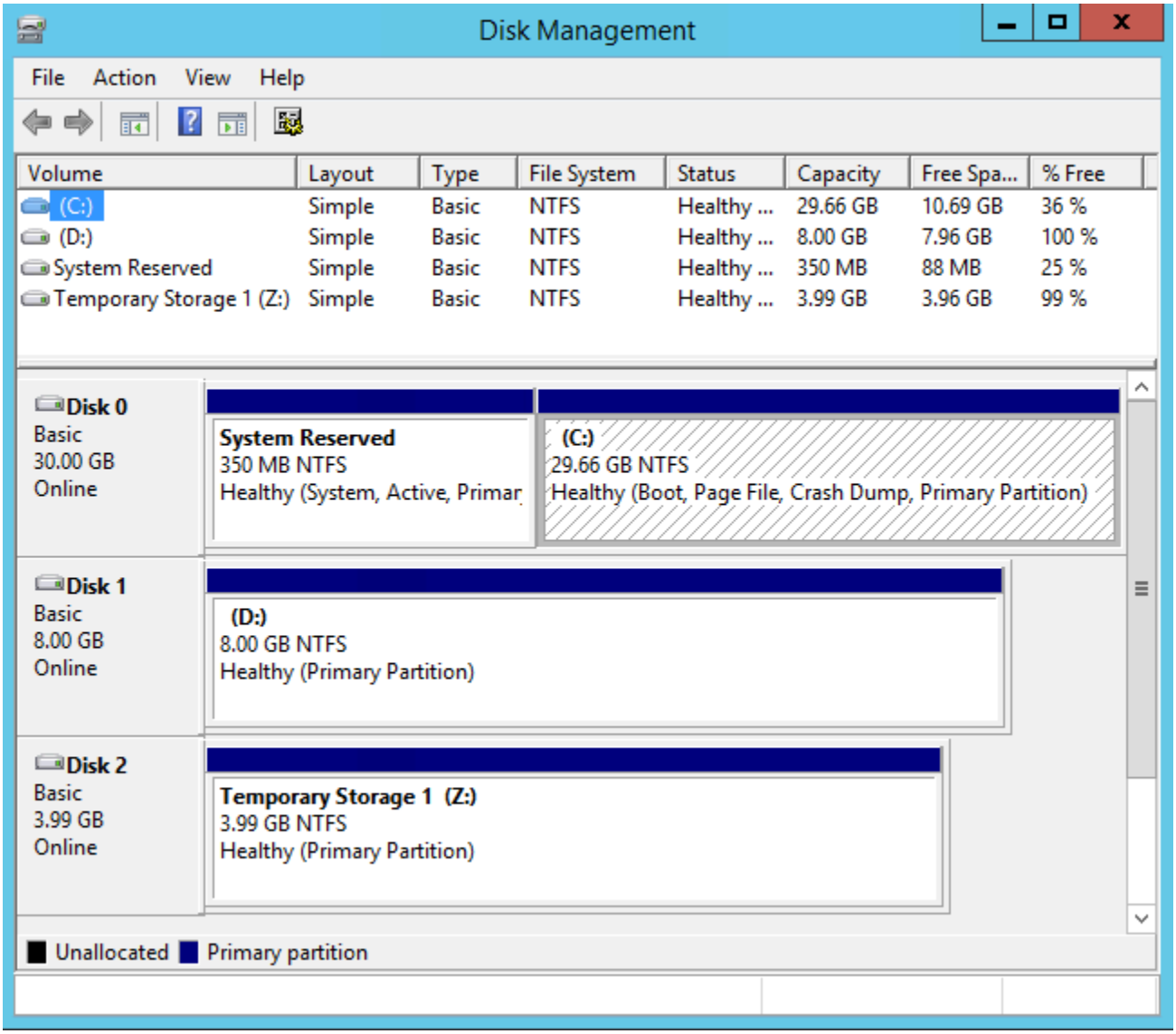
Disk Management

So zeigen Sie die Datenträger in Ihrer Windows-Instance an

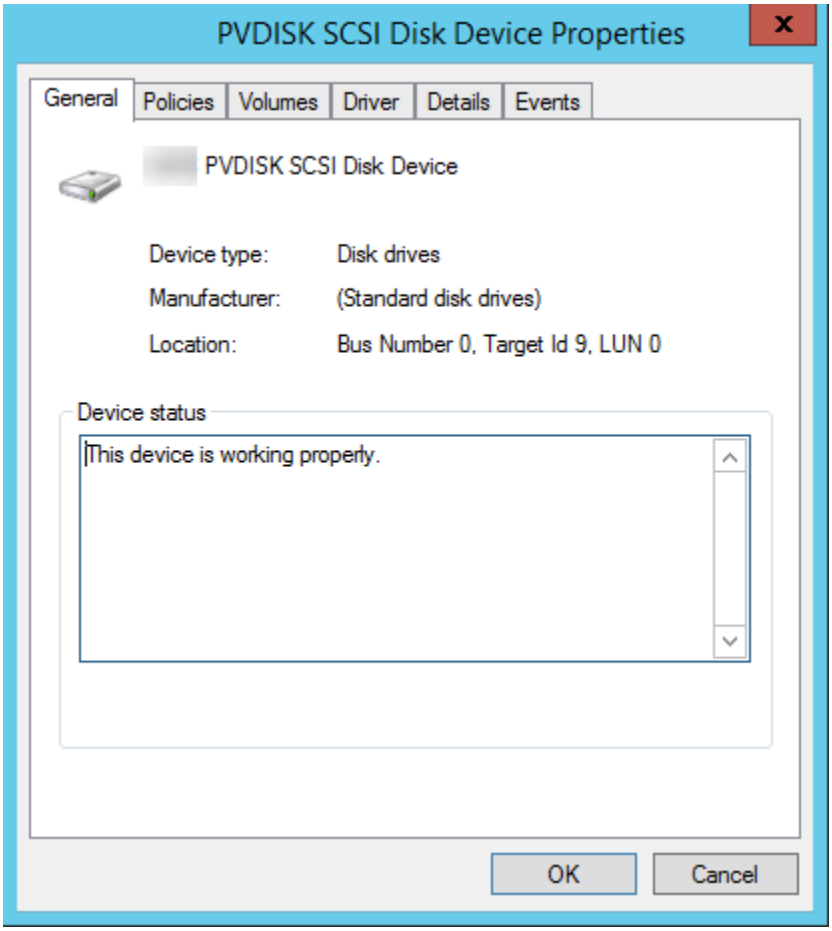
1. Melden Sie sich per Remotedesktop an Ihrer Windows-Instance an. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von RDP.
2. Starten Sie das Dienstprogramm für die Datenträgerverwaltung.

   Klicken Sie in der Aufgabenleiste mit der rechten Maustaste auf das Windows-Logo und wählen Sie anschließend Datenträgerverwaltung aus.
3. Überprüfen Sie die Datenträger. Das Root-Volume ist ein EBS-Volume, das unter gemountet is `C:\`. Wenn keine weiteren Datenträger angezeigt werden, haben Sie keine zusätzlichen Volumes angegeben, als Sie das AMI erstellt bzw. die Instance gestartet haben.

   Das folgende Beispiel zeigt die verfügbaren Datenträger beim Start einer `m3.medium`-Instance mit einem Instance-Speicher-Volume (Disk 2) und einem zusätzlichen EBS Volume (Disk 1).



4. Klicken Sie mit der rechten Maustaste auf den grauen Bereich mit der Bezeichnung "Datenträger 1" und wählen Sie dann die Option Eigenschaften. Notieren Sie sich den Wert unter Location (Speicherort) und schlagen Sie ihn in den Tabellen unter Nicht-NVME-Festplatten Volumes zuordnen nach. Für den folgenden Datenträger wird als Speicherort z. B. der Wert„Bus Number 0, Target Id 9, LUN 0” angezeigt. Laut der Tabelle für EBS-Volumes lautet der Gerätename für diesen Speicherort `xvdj`.



PowerShell

Das folgende PowerShell-Skript listet alle Datenträger und die entsprechenden Gerätenamen und Volumes auf.

Anforderungen und Einschränkungen

- Erfordert Windows Server 2012 oder höher.
- Erfordert Anmeldedaten, um die EBS-Volume-ID zu erhalten Sie können ein Profil mit Tools for PowerShell konfigurieren oder eine IAM-Rolle an die Instance anhängen.
- Unterstützt keine NVMe-Volumes.
- Unterstützt keine dynamischen Festplatten.

Stellen Sie eine Verbindung mit Ihrer Windows-Instance her und führen Sie den folgenden Befehl aus, um die Ausführung von PowerShell-Skripts zu aktivieren.

```
Set-ExecutionPolicy RemoteSigned
```

Kopieren Sie das folgende Skript und speichern Sie es unter Ihrer Windows-Instance als `mapping.ps1`.

```
# List the disks
function Convert-SCSITargetIdToDeviceName {
  param([int]$SCSITargetId)
  If ($SCSITargetId -eq 0) {
    return "sda1"
  }
  $deviceName = "xvd"
  If ($SCSITargetId -gt 25) {
    $deviceName += [char](0x60 + [int]($SCSITargetId / 26))
  }
  $deviceName += [char](0x61 + $SCSITargetId % 26)
  return $deviceName
}

[string[]]$array1 = @()
[string[]]$array2 = @()
[string[]]$array3 = @()
[string[]]$array4 = @()

Get-WmiObject Win32_Volume | Select-Object Name, DeviceID | ForEach-Object {
  $array1 += $_.Name
  $array2 += $_.DeviceID
}

$i = 0
While ($i -ne ($array2.Count)) {
  $array3 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-
Disk).SerialNumber) -replace "_[^ ]*$" -replace "vol", "vol-"
  $array4 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-
Disk).FriendlyName)
  $i ++
}

[array[]]$array = $array1, $array2, $array3, $array4

Try {
  $InstanceId = Get-EC2InstanceMetadata -Category "InstanceId"
```

```
  $Region = Get-EC2InstanceMetadata -Category "Region" | Select-Object -
ExpandProperty SystemName
}
Catch {
  Write-Host "Could not access the instance Metadata using AWS Get-
EC2InstanceMetadata CMDLet.
Verify you have AWSPowershell SDK version '3.1.73.0' or greater installed and
 Metadata is enabled for this instance." -ForegroundColor Yellow
}
Try {
  $BlockDeviceMappings = (Get-EC2Instance -Region $Region -Instance
 $InstanceId).Instances.BlockDeviceMappings
  $VirtualDeviceMap = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping").GetEnumerator() | Where-Object { $_.Key -ne "ami" }
}
Catch {
  Write-Host "Could not access the AWS API, therefore, VolumeId is not available.
Verify that you provided your access keys or assigned an IAM role with adequate
 permissions." -ForegroundColor Yellow
}

Get-disk | ForEach-Object {
  $DriveLetter = $null
  $VolumeName = $null
  $VirtualDevice = $null
  $DeviceName = $_.FriendlyName

  $DiskDrive = $_
  $Disk = $_.Number
  $Partitions = $_.NumberOfPartitions
  $EbsVolumeID = $_.SerialNumber -replace "_[^ ]*$" -replace "vol", "vol-"
  if ($Partitions -ge 1) {
    $PartitionsData = Get-Partition -DiskId $_.Path
    $DriveLetter = $PartitionsData.DriveLetter | Where-object { $_ -notin @("",
 $null) }
    $VolumeName = (Get-PSDrive | Where-Object { $_.Name -in
 @($DriveLetter) }).Description | Where-object { $_ -notin @("", $null) }
  }
  If ($DiskDrive.path -like "*PROD_PVDISK*") {
    $BlockDeviceName = Convert-SCSITargetIdToDeviceName((Get-WmiObject -Class
 Win32_Diskdrive | Where-Object { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" +
 $DiskDrive.Number) }).SCSITargetId)
    $BlockDeviceName = "/dev/" + $BlockDeviceName
```

```
    $BlockDevice = $BlockDeviceMappings | Where-Object { $BlockDeviceName -like "*"
 + $_.DeviceName + "*" }
    $EbsVolumeID = $BlockDevice.Ebs.VolumeId
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -
eq $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON_EC2_NVME*") {
    $BlockDeviceName = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping")."ephemeral$((Get-WmiObject -Class Win32_Diskdrive | Where-
Object { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" + $DiskDrive.Number) }).SCSIPort - 2)"
    $BlockDevice = $null
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -
eq $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
        $i ++
      }
    }
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
 $EbsVolumeID }).DeviceName
  }
  ElseIf ($DiskDrive.path -like "*NETAPP*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
        $i ++
      }
    }
    $EbsVolumeID = "FSxN Volume"
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
 $EbsVolumeID }).DeviceName
```

```
  }
  Else {
    $BlockDeviceName = $null
    $BlockDevice = $null
  }
  New-Object PSObject -Property @{
    Disk          = $Disk;
    Partitions    = $Partitions;
    DriveLetter   = If ($DriveLetter -eq $null) { "N/A" } Else { $DriveLetter };
    EbsVolumeId   = If ($EbsVolumeID -eq $null) { "N/A" } Else { $EbsVolumeID };
    Device        = If ($BlockDeviceName -eq $null) { "N/A" } Else
 { $BlockDeviceName };
    VirtualDevice = If ($VirtualDevice -eq $null) { "N/A" } Else { $VirtualDevice };
    VolumeName    = If ($VolumeName -eq $null) { "N/A" } Else { $VolumeName };
    DeviceName    = If ($DeviceName -eq $null) { "N/A" } Else { $DeviceName };
  }
} | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions,
 DriveLetter, EbsVolumeId, Device, VirtualDevice, DeviceName, VolumeName
```

Führen Sie das Skript wie folgt aus:

```
PS C:\> .\mapping.ps1
```

Es folgt eine Beispielausgabe.

```
Disk  Partitions  DriveLetter   EbsVolumeId            Device      VirtualDevice
 DeviceName              VolumeName
----  ----------  -----------   -----------            ------      -------------
 ----------              ----------
   0           1            C   vol-0561f1783298efedd   /dev/sda1   N/A
 NVMe Amazon Elastic B   N/A
   1           1            D   vol-002a9488504c5e35a   xvdb        N/A
 NVMe Amazon Elastic B   N/A
   2           1            E   vol-0de9d46fcc907925d   xvdc        N/A
 NVMe Amazon Elastic B   N/A
```

Wenn Sie Ihre Anmeldeinformationen für die Windows-Instance nicht angegeben haben, kann das Skript die EBS-Volume-ID nicht erhalten und verwendet N/A in der `EbsVolumeId`-Spalte.

Nicht-NVME-Festplatten Volumes zuordnen

Der Blockgerät-Treiber für die Instance weist die tatsächlichen Volume-Namen beim Aufspielen der Volumes zu.

Mappings

- Instance-Speicher-Volumes
- EBS-Datenträger

Instance-Speicher-Volumes

In der folgenden Tabelle wird beschrieben, wie die Citrix PV- und AWS PV-Treiber nicht-NVMe-Instance-Speicher-Volumes zu Windows-Volumes zuweisen. Die Anzahl der verfügbaren Instance-Speicher-Volumes wird von dem jeweiligen Instance-Typ bestimmt. Weitere Informationen finden Sie unter Volumenlimits für den Instance-Speicher für EC2-Instances.

Ort	Gerätename
Bus Number 0, Target ID 78, LUN 0	xvdca
Bus Number 0, Target ID 79, LUN 0	xvdcb
Bus Number 0, Target ID 80, LUN 0	xvdcc
Bus Number 0, Target ID 81, LUN 0	xvdcd
Bus Number 0, Target ID 82, LUN 0	xvdce
Bus Number 0, Target ID 83, LUN 0	xvdcf
Bus Number 0, Target ID 84, LUN 0	xvdcg
Bus Number 0, Target ID 85, LUN 0	xvdch
Bus Number 0, Target ID 86, LUN 0	xvdci
Bus Number 0, Target ID 87, LUN 0	xvdcj
Bus Number 0, Target ID 88, LUN 0	xvdck

Ort	Gerätename
Bus Number 0, Target ID 89, LUN 0	xvdcl

EBS-Datenträger

In der folgenden Tabelle wird beschrieben, wie die Citrix PV- und AWS PV-Treiber nicht-NVME EBS-Volumes zu Windows-Volumes zuweisen.

Ort	Gerätename
Bus Number 0, Target ID 0, LUN 0	/dev/sda1
Bus Number 0, Target ID 1, LUN 0	xvdb
Bus Number 0, Target ID 2, LUN 0	xvdc
Bus Number 0, Target ID 3, LUN 0	xvdd
Bus Number 0, Target ID 4, LUN 0	xvde
Bus Number 0, Target ID 5, LUN 0	xvdf
Bus Number 0, Target ID 6, LUN 0	xvdg
Bus Number 0, Target ID 7, LUN 0	xvdh
Bus Number 0, Target ID 8, LUN 0	xvdi
Bus Number 0, Target ID 9, LUN 0	xvdj
Bus Number 0, Target ID 10, LUN 0	xvdk
Bus Number 0, Target ID 11, LUN 0	xvdl
Bus Number 0, Target ID 12, LUN 0	xvdm
Bus Number 0, Target ID 13, LUN 0	xvdn
Bus Number 0, Target ID 14, LUN 0	xvdo

Ort	Gerätename
Bus Number 0, Target ID 15, LUN 0	xvdp
Bus Number 0, Target ID 16, LUN 0	xvdq
Bus Number 0, Target ID 17, LUN 0	xvdr
Bus Number 0, Target ID 18, LUN 0	xvds
Bus Number 0, Target ID 19, LUN 0	xvdt
Bus Number 0, Target ID 20, LUN 0	xvdu
Bus Number 0, Target ID 21, LUN 0	xvdv
Bus Number 0, Target ID 22, LUN 0	xvdw
Bus Number 0, Target ID 23, LUN 0	xvdx
Bus Number 0, Target ID 24, LUN 0	xvdy
Bus Number 0, Target ID 25, LUN 0	xvdz

Torn Write Prevention in Amazon-EC2-Linux Instances

> **Note**
>
> Torn Write Prevention wird nur für Linux-Instances unterstützt.

Verbessern Sie die Leistung Ihrer I/O-intensiven relationalen Datenbank-Workloads und reduzieren Sie die Latenz, ohne die Datenstabilität zu beeinträchtigen, indem Sie das Blockspeicherfeature Torn-Write-Prävention verwenden, die von AWS entwickelt wurde. Relationale Datenbanken, die InnoDB oder XtraDB als Datenbank-Engine verwenden, wie MySQL und MariaDB, profitieren von Torn-Write-Prävention.

In der Regel verwenden relationale Datenbanken, die Seiten verwenden, die größer sind als die Stromausfall-Atomizität des Speichergeräts, Datenprotokollierungsmechanismen, um

sich vor fehlerhaften Schreibvorgängen zu schützen. MariaDB und MySQL verwenden einen Doublewrite-Puffer, um Daten zu protokollieren, bevor sie in Datentabellen geschrieben werden. Bei unvollständigen oder unterbrochenen Schreibvorgängen aufgrund von Betriebssystemabstürzen oder Stromausfällen während Schreibtransaktionen kann die Datenbank die Daten aus dem Doublewrite-Puffer wiederherstellen. Der zusätzliche I/O-Overhead, der mit dem Schreiben in den Doublewrite-Puffer verbunden ist, wirkt sich auf die Datenbankleistung und die Anwendungslatenz aus und reduziert die Anzahl der Transaktionen, die pro Sekunde verarbeitet werden können. Weitere Informationen zu Doublewrite Buffer finden Sie in der Dokumentation zu MariaDB und MySQL.

Mit Torn-Write-Prävention werden Daten in Alles-oder-Nichts-Schreibtransaktionen in den Speicher geschrieben, sodass der Doublewrite-Puffer nicht mehr verwendet werden muss. Dadurch wird verhindert, dass bei Betriebssystemabstürzen oder Stromausfällen während Schreibtransaktionen teilweise oder aufgespaltete Daten in den Speicher geschrieben werden. Die Anzahl der pro Sekunde verarbeiteten Transaktionen kann um bis zu 30 Prozent erhöht und die Schreiblatenz um bis zu 50 Prozent verringert werden, ohne die Resilienz Ihrer Workloads zu beeinträchtigen.

Preisgestaltung

Für die Verwendung von Torn-Write-Prävention fallen keine zusätzlichen Kosten an.

Inhalt

- Blockgrößen für Torn Write Prevention auf Amazon EC2
- Anforderungen für die Verwendung von Torn Write Prevention auf Amazon EC2
- Überprüfen Sie die Unterstützung von Amazon-EC2-Instances für Torn Write Prevention
- Ihren Workload in Amazon EC2 für Torn Write Prevention konfigurieren

Blockgrößen für Torn Write Prevention auf Amazon EC2

Torn-Write-Prävention unterstützt Schreiboperationen für Datenblöcke von 4 KiB, 8 KiB und 16 KiB. Die Startadresse des Datenblocks (Logical Block Address, LBA) muss auf die jeweilige Blockgrenzengröße von 4 KiB, 8 KiB oder 16 KiB ausgerichtet sein. Beispielsweise muss für 16-KiB-Schreibvorgänge der Datenblockstart LBA auf eine Blockgrenzgröße von 16 KiB ausgerichtet werden.

Die folgende Tabelle zeigt die Unterstützung für verschiedene Speicher- und Instance-Typen.

	4-KiB-Blöcke	8-KiB-Blöcke	16-KiB-Blöcke
Instance-Speicher-Volumes	Alle NVMe-Instance-Speichervolumes, die an Instances der I-Familie der aktuellen Generation angefügt sind.	Von AWS Nitro SSD unterstützte I4i-, Im4gn-, Is4gen-, I7i-, I7ie-, I8g- und I8ge-Instances.	
Amazon-EBS-Volumes	Alle Amazon-EBS-Volumes, die Nitro-basierten Instances zugeordnet sind.		

Um zu überprüfen, ob Ihre Instance und Ihr Volume Torn-Write-Prävention unterstützen, prüfen Sie, ob die Instance Torn-Write-Prävention unterstützt und überprüfen Sie weitere Details wie unterstützte Block- und Grenzgrößen. Weitere Informationen finden Sie unter Überprüfen Sie die Unterstützung von Amazon-EC2-Instances für Torn Write Prevention.

Anforderungen für die Verwendung von Torn Write Prevention auf Amazon EC2

Damit Torn-Write-Prävention ordnungsgemäß funktioniert, muss ein I/O-Vorgang die Anforderungen an Größe, Ausrichtung und Grenzen erfüllen, wie in den Feldern `NTWPU`, `NTWGU` und `NTWBU` angegeben. Sie müssen Ihr Betriebssystem so konfigurieren, dass das spezifische Speichersubsystem (Dateisystem, LVM, RAID usw.) keine I/O-Eigenschaften im Speicherstapel verändert, einschließlich Blockzusammenführungen, Splits oder Blockadressverschiebungen, bevor sie an das Gerät übermittelt werden.

Torn-Write-Prävention wurde mit der folgenden Konfiguration getestet:

- Ein Instance-Typ und ein Speichertyp, der die erforderliche Blockgröße unterstützt.
- Amazon Linux 2 mit Kernel-Version 5.10 oder höher.
- ext4 mit `bigalloc` aktiviert und einer Clustergröße von 16 KiB sowie die neuesten ext4-Hilfsprogramme (e2fsprogs 1.46.5 oder höher).
- `O_DIRECT`-Dateizugriffsmodus zur Umgehung des Linux-Kernel-Puffercaches.

> **Note**
>
> Sie müssen die I/O-Zusammenführung für MySQL- und MariaDB-Workloads nicht deaktivieren.

Überprüfen Sie die Unterstützung von Amazon-EC2-Instances für Torn Write Prevention

Verwenden Sie den folgenden Befehl, um zu überprüfen, ob Ihre Instance und Ihr Volume Torn-Write-Prävention unterstützen, und um die herstellerspezifischen NVMe-Namespace-Daten einzusehen, die Informationen zur Verhinderung von Torn-Write-Prävention enthalten.

```
$ sudo nvme id-ns -v device_name
```

> **Note**
>
> Der Befehl gibt die herstellerspezifischen Informationen in Hexadezimalform mit ASCII-Interpretation zurück. Möglicherweise müssen Sie ein ähnliches Tool wie `ebsnvme-id` in Ihre Anwendungen einbauen, das die Ausgabe lesen und analysieren kann.

Der folgende Befehl gibt beispielsweise die herstellerspezifischen NVMe-Namespace-Daten zurück, die Informationen zu Torn-Write-Prävention für `/dev/nvme1n1` enthalten.

```
$ sudo nvme id-ns -v /dev/nvme1n1
```

Wenn Ihre Instance und Ihr Volume Torn-Write-Prävention unterstützen, werden die folgenden Informationen zur AWS-Torn-Write-Prävention in den herstellerspezifischen NVMe-Namespace-Daten zurückgegeben.

> **Note**
>
> Die Bytes in der folgenden Tabelle stellen den Abstand in Bytes vom Anfang der herstellerspezifischen NVMe-Namespace-Daten dar.

Bytes	Beschreibung
0:31	Der Name des Befestigungspunkts des Geräts, z. B. /dev/xvda . Sie geben dies bei der Anforderung eines Volumenanhangs an und es kann von der Amazon-EC2-Instance verwendet werden, um einen Symlink zum NVMe-Blockgerät (nvmeXn1) zu erstellen.
32:63	Die Volume-ID. Beispiel, vol01234567890abcdef . Dieses Feld kann verwendet werden, um das NVMe-Gerät dem angeschlossenen Volume zuzuordnen.
64:255	Für die spätere Verwendung reserviert.
256:257	Größe der Namespace-Torn-Write-Prävention-Einheit (NTWPU, Namespace Torn Write Prevention Unit). Dieses Feld gibt die namespace-spezifischen Größe des Schreibvorgangs an, die bei einem Stromausfall oder einer Fehlerbedingung garantiert automatsch in den NVM geschrieben werden. Dieses Feld ist in logischen Blöcken angegeben, die in Nullwerten dargestellt werden.
258:259	Granularitätsgröße von Namespace Torn Write Prevention (NTWPG). Dieses Feld gibt die namespace-spezifischen Größeninkremente unter NTWPU des Schreibvorgangs an, die bei einem Stromausfall oder einer Fehlerbedingung garantiert atomar in den NVM geschrieben werden. Das heißt, die Größe sollte bei NTWPG * n <= NTWPU liegen, wobei n eine positive Ganzzahl ist. Der Schreibvorgang „LBA-Offset“ muss ebenfalls an dieses Feld angepasst werden. Dieses Feld ist in logischen Blöcken angegeben, die in Nullwerten dargestellt werden.
260:263	Größe der Namespace-Torn-Write-Prävention-Grenze (NTWPB, Namespace Torn Write Prevention Boundary). Dieses Feld gibt die atomare Grenzgröße für diesen Namespace für den Wert NTWPU an. Es ist nicht garantiert, dass Schreibvorgänge in diesen Namespace , die atomare Grenzen überschreiten, bei einem Stromausfall oder einem Fehler automatsch auf die NVM geschrieben werden. Ein Wert von 0h gibt an, dass es keine atomaren Grenzen für Stromausfall- oder Fehlerbedingungen gibt. Alle anderen Werte geben eine Größe in

Bytes	Beschreibung
	Form logischer Blöcke an, die dieselbe Kodierung wie das NTWPU-Feld verwenden.

Ihren Workload in Amazon EC2 für Torn Write Prevention konfigurieren

Torn-Write-Prävention ist standardmäßig auf unterstützten Instance-Typen mit unterstützten Volumes aktiviert. Sie müssen keine zusätzlichen Einstellungen aktivieren, um Ihr Volume oder Ihre Instance für Torn-Write-Prävention zu aktivieren.

> **Note**
>
> Es gibt keine Auswirkungen auf die Leistung von Workloads, die Torn-Write-Prävention nicht unterstützen. Sie müssen keine Änderungen für diese Workloads vornehmen. Workloads, die Torn-Write-Prävention unterstützen, aber nicht dafür konfiguriert sind, verwenden weiterhin den Doublewrite-Puffer und erhalten keine Leistungsvorteile.

Gehen Sie wie folgt vor, um Ihren MySQL- oder MariaDB-Softwarestack so zu konfigurieren, dass der Doublewrite-Puffer deaktiviert und Torn-Write-Prävention verwendet wird:

1. Konfigurieren Sie Ihr Volume so, dass es das ext4-Dateisystem mit der Option BigAlloc verwendet, und legen Sie die Clustergröße auf 4 KiB, 8 KiB oder 16 KiB fest. Die Verwendung von BigAlloc mit einer Clustergröße von 4 KiB, 8 KiB oder 16 KiB stellt sicher, dass das Dateisystem Dateien zuweist, die an der jeweiligen Grenze ausgerichtet sind.

   ```
   $  mkfs.ext4 -O bigalloc -C 4096|8192|16384 device_name
   ```

   > **Note**
   >
   > Für MySQL und MariaDB müssen Sie `-C 16384` verwenden, um die Seitengröße der Datenbank anpassen. Wenn Sie die Zuweisungsgranularität auf einen anderen Wert als ein Vielfaches der Seitengröße festlegen, kann dies zu Zuordnungen führen, die möglicherweise nicht mit den Grenzen des Speichergeräts zur Verhinderung von fehlerhaften Schreibvorgängen übereinstimmen.

Zum Beispiel:

```
$  mkfs.ext4 -O bigalloc -C 16384 /dev/nvme1n1
```

2. Konfigurieren Sie InnoDB so, dass es die `O_DIRECT`-Flushing-Methode verwendet, und schalten Sie InnoDB-Doublewrite aus. Verwenden Sie Ihren bevorzugten Texteditor, um `/etc/my.cnf` zu öffnen und die `innodb_flush_method`- und `innodb_doublewrite`-Parameter wie folgt zu aktualisieren:

```
innodb_flush_method=O_DIRECT
innodb_doublewrite=0
```

> **Important**
>
> Wenn Sie den Logical Volume Manager (LVM) oder eine andere Speichervirtualisierungsschicht verwenden, stellen Sie sicher, dass die Startoffsets der Volumes auf ein Vielfaches von 16 KiB ausgerichtet sind. Dies bezieht sich auf den zugrunde liegenden NVMe-Speicher, um die von der Speichervirtualisierungsebene verwendeten Metadaten-Header und Superblöcke zu berücksichtigen. Wenn Sie dem physischen LVM-Volume einen Offset hinzufügen, kann dies zu einer Fehlausrichtung zwischen den Dateisystemzuordnungen und den Offsets des NVMe-Geräts führen, was die Verhinderung von fehlerhaften Schreibvorgängen zunichte machen würde. Weitere Informationen finden Sie unter `--dataalignmentoffset` in der Linux-Handbuchseite.

Anwendungskonsistente Windows-VSS-basierte Amazon-EBS-Snapshots

Sie können anwendungskonsistente Snapshots aller Amazon-EBS-Volumes erstellen, die Ihren Amazon-EC2-Windows-Instances angefügt sind, indem Sie AWS Systems Manager-Befehl ausführen verwenden. Der Snapshot-Vorgang erstellt mit dem Windows Volume Shadow Copy Service (VSS) Backups VSS-fähiger Anwendungen auf EBS-Volume-Ebene. Dazu gehören auch Daten von schwebenden Transaktionen zwischen diesen Anwendungen und dem Datenträger. Sie müssen Ihre Instances nicht herunterfahren oder trennen, wenn Sie ein Backup aller angefügten Volumes durchführen möchten.

Für die Verwendung von VSS-basierten EBS-Snapshots fallen keine zusätzlichen Kosten an. Sie zahlen nur für die EBS-Snapshots, die durch den Backup-Vorgang erstellt werden. Weitere Informationen finden Sie unter Wie werden mir meine Amazon-EBS-Snapshots in Rechnung gestellt?

> **Note**
>
> Anwendungskonsistente Windows-VSS-basierte Snapshots werden nur mit Windows-Instances unterstützt.

Inhalt

- Was ist -VSS?
- So funktioniert die VSS-basierte Amazon-EBS-Snapshot-Lösung
- Voraussetzungen für die Erstellung von Windows-VSS-basierten EBS-Snapshots
- Auf VSS basierende EBS-Snapshots für Ihre EC2-Windows-Instance erstellen
- Problembehandlung bei Windows-VSS-basierten EBS-Snapshots
- Verwenden Sie die AWS-VSS-Lösung, um Daten für Ihre Instance wiederherzustellen.
- Versionsverlauf der AWS VSS-Lösung

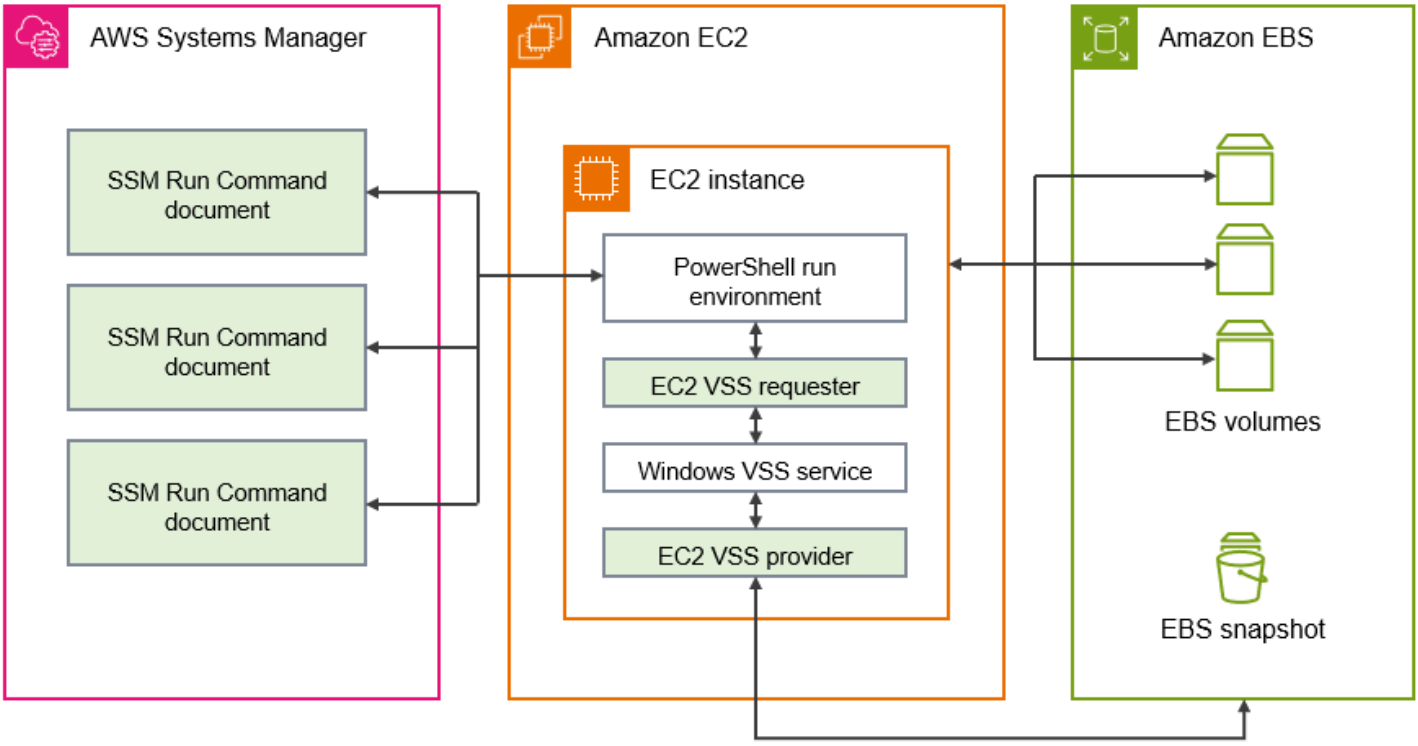
Was ist -VSS?

Volume Shadow Copy Service (VSS) ist eine Backup- und Wiederherstellungstechnologie, die in Microsoft Windows enthalten ist. Es kann Backup-Kopien oder Snapshots von Computerdateien oder Volumes erstellen, während diese verwendet werden. Weitere Informationen finden Sie unter Volume Shadow Copy Service.

Die folgenden Softwarekomponenten sind an der Erstellung eines anwendungskonsistenten Snapshots beteiligt.

- VSS-Service – Teil des Windows-Betriebssystems
- VSS-Anforderer – Die Software, die die Erstellung von Schattenkopien anfordert
- VSS-Writer – Wird in der Regel als Teil einer Anwendung, wie z. B. SQL Server, bereitgestellt, um einen konsistenten Datensatz für das Backup sicherzustellen
- VSS-Anbieter – Die Komponente, die die Schattenkopien der zugrunde liegenden Volumes erstellt

Die Windows VSS-basierte Amazon EBS-Snapshot-Lösung besteht aus mehreren Systems Manager (SSM)-Ausführungsbefehlsdokumenten, welche die Erstellung von Backups erleichtern, und einem Systems-Manager-Distributor-Paket namens `AwsVssComponents`, das einen EC2-VSS-Requester und einen EC2-VSS-Provider enthält. Das Paket `AwsVssComponents` muss auf EC2-Windows-Instances installiert werden, um anwendungskonsistente Snapshots von EBS-Volumes erstellen zu können. Die folgende Abbildung zeigt die Beziehung zwischen diesen Softwarekomponenten.



So funktioniert die VSS-basierte Amazon-EBS-Snapshot-Lösung

Für die Erstellung anwendungskonsistenter, VSS-basierter EBS-Snapshots sind folgende Schritte erforderlich.

1. Sie müssen die für erfüllen Voraussetzungen für die Erstellung von Windows-VSS-basierten EBS-Snapshots.
2. Geben Sie Parameter für das SSM-Dokument `AWSEC2-VssInstallAndSnapshot` ein und führen Sie dieses Dokument mit Run Command aus. Weitere Informationen finden Sie unter AWSEC2-VssInstallAndSnapshot-Befehlsdokument ausführen (empfohlen).
3. Der Windows VSS-Service auf Ihrer Instance koordiniert alle laufenden I/O-Vorgänge für laufende Anwendungen.

4. Das System bereinigt alle I/O-Puffer und hält alle I/O-Vorgänge vorübergehend an. Die Unterbrechung dauert maximal zehn Sekunden.
5. Während der Unterbrechung erstellt das System Snapshots aller Volumes, die an die Instance angehängt sind.
6. Die Unterbrechung wird aufgehoben und der I/O-Vorgang fortgesetzt.
7. Das System fügt alle neu erstellten Snapshots zu der Liste der EBS-Snapshots hinzu. Das System markiert alle durch diesen Vorgang erstellten VSS-fähigen EBS-Snapshots mit dem Tag AppConsistent:true.
8. Falls Sie eine Wiederherstellung von einem Snapshot aus vornehmen müssen, können Sie hierfür den EBS-Standardvorgang zum Erstellen eines Volumes aus einem Snapshot verwenden oder alle Volumes in einer Instance wiederherstellen, indem Sie ein Beispielskript verwenden. Dieses Verfahren wird in Verwenden Sie die AWS-VSS-Lösung, um Daten für Ihre Instance wiederherzustellen. beschrieben.

Voraussetzungen für die Erstellung von Windows-VSS-basierten EBS-Snapshots

Sie können VSS-basierte EBS-Snapshots mit Systems Manager Run Command, AWS Backup oder Amazon Data Lifecycle Manager erstellen. Die folgenden Voraussetzungen gelten für alle Lösungen.

Systemanforderungen

Stellen Sie sicher, dass Ihre EC2-Windows-Instance alle Systemanforderungen für die Erstellung von VSS-basierten Snapshots erfüllt, einschließlich unterstützter Versionen des Windows-Betriebssystems, .NET Framework, PowerShell AWS Tools for Windows PowerShell und des AWS Systems Manager-Agenten.

IAM-Berechtigungen

Die Ihrer Amazon-EC2-Windows-Instance zugewiesenen IAM-Rolle muss über die Berechtigung zum Erstellen anwendungskonsistenter Snapshots mit VSS verfügen. Um die erforderlichen Berechtigungen zu gewähren, können Sie die `AWSEC2VssSnapshotPolicy`-verwaltete Richtlinie an Ihr Instance-Profil anhängen.

VSS-Komponenten

Um anwendungskonsistente Snapshots auf Windows-Betriebssystemen zu erstellen, muss das Paket `AwsVssComponents` auf der Instance installiert sein. Das Paket enthält einen On-Instance-EC2-VSS-Agent, der als VSS-Anforderer und EC2-VSS-Anbieter für EBS-Volumes fungiert.

Systemanforderungen

Den Systems Manager Agent installieren

VSS wird vom Systems Manager Agent mithilfe von PowerShell orchestriert. Auf Ihrer EC2-Instance muss die SSM-Agent-Version `3.0.502.0` oder höher installiert sein. Wenn Sie bereits eine ältere Version von SSM-Agent verwenden, aktualisieren Sie diese mithilfe von Run Command. Weitere Informationen finden Sie unter Einrichtung von Systems Manager für Amazon EC2-Instances und Arbeiten mit SSM-Agent auf Amazon-EC2-Instances für Windows Server im AWS Systems Manager-Benutzerhandbuch.

Amazon EC2-Windows Instance-Anforderungen

VSS-basierte EBS-Snapshots werden für Instances mit Windows Server 2016 oder höher unterstützt.

.NET Framework-Version

Das `AwsVssComponents`-Paket erfordert .NET Framework der Version `4.6` oder höher. Windows-Betriebssystemversionen vor Windows Server 2016 verwenden standardmäßig eine frühere Version von.NET Framework. Wenn Ihre Instance eine frühere Version von.NET Framework verwendet, müssen Sie Version `4.6` oder höher mit Windows Update installieren.

AWS Tools for Windows PowerShell-Version

Stellen Sie sicher, dass Ihre Instance Version `3.3.48.0` oder höher von AWS Tools for Windows PowerShell ausführt. Um Ihre Version zu überprüfen, führen Sie den folgenden Befehl im PowerShell-Terminal auf der Instance aus.

```
C:\> Get-AWSPowerShellVersion
```

Wenn Sie AWS Tools for Windows PowerShell auf Ihrer Instance aktualisieren müssen, lesen Sie bitte den Abschnitt Installieren der AWS Tools for Windows PowerShell im AWS -Tools für PowerShell-Benutzerhandbuch.

Windows-Powershell-Version

Stellen Sie sicher, dass auf Ihrer Instance die Hauptversion von Windows PowerShell 3, 4 oder 5 ausgeführt wird. Um Ihre Version zu überprüfen, führen Sie den folgenden Befehl in einem PowerShell-Terminal auf der Instance aus.

```
C:\> $PSVersionTable.PSVersion
```

PowerShell-Sprachmodus

Stellen Sie sicher, dass für Ihre Instance der PowerShell-Sprachmodus auf `FullLanguage` eingestellt ist. Weitere Informationen finden Sie unter about_Language_Modes in der Microsoft-Dokumentation.

Verwenden Sie eine IAM-verwaltete Richtlinie, um Berechtigungen für VSS-basierte Snapshots zu gewähren

Die AWSEC2VssSnapshotPolicy-verwaltete Richtlinie ermöglicht es Systems Manager, die folgenden Aktionen auf Ihrer Windows-Instance auszuführen:

- EBS-Snapshots erstellen und markieren
- Amazon Machine Images (AMIs) erstellen und markieren
- Fügen Sie Metadaten wie die Geräte-ID an die von VSS erstellten Snapshot-Standard-Tags an.

Dieses Thema behandelt die Berechtigungsdetails für die VSS-verwaltete Richtlinie und wie Sie sie an die IAM-Rolle Ihres EC2-Instance-Profils anhängen können.

Inhalt

- AWSEC2VssSnapshotPolicy Details zur verwalteten Richtlinie
- Fügen Sie die verwaltete VSS-Snapshot-Richtlinie Ihrer Instance-Profilrolle hinzu

AWSEC2VssSnapshotPolicy Details zur verwalteten Richtlinie

Bei einer von AWS-verwalteten Richtlinie handelt es sich um eine eigenständige Richtlinie, die Amazon AWS seinen Kunden anbietet. Die von AWS verwalteten Richtlinien stellen Berechtigungen für häufige Anwendungsfälle bereit. Die Berechtigungen, die in den von AWS verwalteten Richtlinien

definiert sind, können nicht geändert werden. Sie können die Richtlinie jedoch kopieren und als Grundlage für eine vom Kunden verwaltete Richtlinie verwenden, die speziell auf Ihren Anwendungsfall zugeschnitten ist.

Weitere Informationen zu verwalteten AWS-Richtlinien finden Sie unter Verwaltete AWS-Richtlinien im IAM-Leitfaden.

Um die AWSEC2VssSnapshotPolicy-verwaltete Richtlinie zu verwenden, können Sie sie der IAM-Rolle zuordnen, die Ihren EC2-Windows-Instances zugewiesen ist. Diese Richtlinie ermöglicht es der EC2-VSS-Lösung, Tags für Amazon Machine Images (AMIs) und EBS-Snapshots zu erstellen und hinzuzufügen. Informationen zum Anfügen der Richtlinie finden Sie unter Fügen Sie die verwaltete VSS-Snapshot-Richtlinie Ihrer Instance-Profilrolle hinzu.

Berechtigungen von AWSEC2VssSnapshotPolicy

Die AWSEC2VssSnapshotPolicy-Richtlinie umfasst die folgenden Amazon-EC2-Berechtigungen, die es Amazon EC2 ermöglichen, VSS-Snapshots in Ihrem Namen zu erstellen und zu verwalten. Sie können diese verwaltete Richtlinie an die IAM-Instance-Profilrolle anhängen, die Sie für Ihre EC2-Windows-Instances verwenden.

- ec2:CreateTags – Fügen Sie Tags zu EBS-Snapshots und AMIs hinzu, um die Ressourcen zu identifizieren und zu kategorisieren.
- ec2:DescribeInstanceAttribute – Ruft die EBS-Volumes und die entsprechenden Blockgerätezuordnungen ab, die an die Ziel-Instance angefügt sind.
- ec2:CreateSnapshots – Erstellt Snapshots von EBS-Volumes.
- ec2:CreateImage – Erstellen Sie ein AMI aus einer ausgeführten EC2-Instance.
- ec2:DescribeImages – Ruft die Informationen für EC2-AMIs und -Snapshots ab.
- ec2:DescribeSnapshots – Ermittelt die Erstellungszeit und den Status von Snapshots, um die Anwendungskonsistenz zu überprüfen.

> **Note**
>
> Informationen zu den Berechtigungsdetails für diese Richtlinie finden Sie unter AWSEC2VssSnapshotPolicy in der Referenz zu von AWS verwalteten Richtlinien.

Optimieren Sie die Berechtigungen für bestimmte Anwendungsfälle – für Fortgeschrittene

Die `AWSEC2VssSnapshotPolicy`-verwaltete Richtlinie umfasst Berechtigungen für alle Arten, wie Sie VSS-basierte Snapshots erstellen können. Sie können eine benutzerdefinierte Richtlinie erstellen, die nur die Berechtigungen enthält, die Sie benötigen.

Anwendungsfall: AMI erstellen, Anwendungsfall: AWS Backup-Service verwenden

Wenn Sie ausschließlich die `CreateAmi`-Option verwenden oder wenn Sie VSS-basierte Snapshots nur über den AWS Backup-Service erstellen, können Sie die Richtlinienangaben wie folgt optimieren.

- Lassen Sie die durch die folgenden Statement IDs (SIDs) identifizierten Richtlinienaussagen weg:
  - `CreateSnapshotsWithTag`
  - `CreateSnapshotsAccessInstance`
  - `CreateSnapshotsAccessVolume`
- Passen Sie die `CreateTagsOnResourceCreation` Aussage wie folgt an:
  - `arn:aws:ec2:*:*:snapshot/*` aus der Ressource entfernen.
  - `CreateSnapshots` aus dem `ec2:CreateAction` Bedingung entfernen.
- Passen Sie die `CreateTagsAfterResourceCreation` Aussage an, um sie `arn:aws:ec2:*:*:snapshot/*` aus den Ressourcen zu entfernen.
- Passen Sie die `DescribeImagesAndSnapshots` Aussage an, um sie `ec2:DescribeSnapshots` aus der Aussageaktion zu entfernen.

Anwendungsfall: Nur Snapshot

Wenn Sie die `CreateAmi`-Option nicht verwenden, können Sie die Richtlinienerklärungen wie folgt vereinfachen.

- Lassen Sie die durch die folgenden Statement IDs (SIDs) identifizierten Richtlinienaussagen weg:
  - `CreateImageAccessInstance`
  - `CreateImageWithTag`
- Passen Sie die `CreateTagsOnResourceCreation` Aussage wie folgt an:
  - `arn:aws:ec2:*:*:image/*` aus der Ressource entfernen.
  - `CreateImage` aus dem `ec2:CreateAction` Bedingung entfernen.
- Passen Sie die `CreateTagsAfterResourceCreation` Aussage an, um sie `arn:aws:ec2:*:*:image/*` aus den Ressourcen zu entfernen.

- Passen Sie die `DescribeImagesAndSnapshots` Aussage an, um sie `ec2:DescribeImages` aus der Aussageaktion zu entfernen.

> **Note**
>
> Um sicherzustellen, dass Ihre benutzerdefinierte Richtlinie erwartungsgemäß funktioniert, empfehlen wir Ihnen, die verwaltete Richtlinie regelmäßig zu überprüfen und Aktualisierungen daran vorzunehmen.

Fügen Sie die verwaltete VSS-Snapshot-Richtlinie Ihrer Instance-Profilrolle hinzu

Um Berechtigungen für VSS-basierte Snapshots für Ihre EC2-Windows-Instance zu gewähren, können Sie die AWSEC2VssSnapshotPolicy-verwaltete Richtlinie wie folgt an Ihre Instance-Profilrolle anhängen. Es ist wichtig sicherzustellen, dass Ihre Instance alle Systemanforderungen erfüllt.

> **Note**
>
> Um die verwaltete Richtlinie verwenden zu können, muss auf Ihrer Instance die `AwsVssComponents`-Paketversion `2.3.1` oder neuer installiert sein. Informationen zum Versionsverlauf finden Sie unter AwsVssComponents-Paketversionen.

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Rollen aus, um eine Liste der IAM-Rollen anzuzeigen, auf die Sie Zugriff haben.
3. Wählen Sie den Link Rollenname für die Rolle aus, die Ihrer Instance zugeordnet ist. Die Detailseite „Rollen“ wird geöffnet.
4. Um die verwaltete Richtlinie anzuhängen, wählen Sie in der oberen rechten Ecke des Listenfensters die Option Berechtigungen hinzufügen aus. Wählen Sie in der Dropdown-Liste Richtlinien anfügen aus.
5. Geben Sie den Namen der Richtlinie in die Suchleiste ein (`AWSEC2VssSnapshotPolicy`), um die Ergebnisse zu optimieren.
6. Aktivieren Sie das Kontrollkästchen neben dem Namen der anzuhängenden Richtlinie und wählen Sie anschließend Richtlinie hinzufügen aus.

VSS-Komponentenpaket für Windows VSS-basierte EBS-Snapshots verwalten

Bevor Sie VSS-basierte EBS-Snapshots erstellen, stellen Sie sicher, dass Sie die neueste Version des VSS-Komponentenpakets auf Ihrer Windows-Instance installiert haben. Es gibt mehrere Möglichkeiten, das `AwsVssComponents`-Paket auf einer bestehenden Instance zu installieren:

- (Empfohlen) AWSEC2-VssInstallAndSnapshot-Befehlsdokument ausführen (empfohlen). Dies wird bei jeder Ausführung automatisch installiert oder bei Bedarf aktualisiert.
- VSS-Komponenten manuell auf einer EC2-Windows-Instance installieren.
- Das VSS-Komponentenpaket auf Ihrer EC2-Windows-Instance aktualisieren.

Sie können auch ein AMI mit EC2 Image Builder erstellen, das die verwaltete Komponente `aws-vss-components-windows` verwendet, um das `AwsVssComponents`-Paket für das Image zu installieren. Die verwaltete Komponente verwendet AWS Systems Manager-Verteiler, um das Paket zu installieren. Nachdem Image Builder das Image erstellt hat, wird auf jeder Instance, die Sie über das zugehörige AMI starten, das VSS-Paket installiert. Weitere Informationen dazu, wie Sie ein AMI mit dem installierten VSS-Paket erstellen können, finden Sie unter Vom Verteilerpaket verwaltete Komponenten für Windows im Benutzerhandbuch für EC2 Image Builder.

Inhalt

- VSS-Komponenten manuell auf einer EC2-Windows-Instance installieren
- Das VSS-Komponentenpaket auf Ihrer EC2-Windows-Instance aktualisieren

VSS-Komponenten manuell auf einer EC2-Windows-Instance installieren

Auf Ihrer EC2-Windows-Instance müssen VSS-Komponenten installiert sein, bevor Sie mit Systems Manager anwendungskonsistente Snapshots erstellen können. Wenn Sie das `AWSEC2-VssInstallAndSnapshot`-Befehlsdokument nicht ausführen, um das Paket jedes Mal automatisch zu installieren oder zu aktualisieren, wenn Sie anwendungskonsistente Snapshots erstellen, müssen Sie das Paket manuell installieren.

Sie müssen die Installation auch manuell durchführen, wenn Sie eine der folgenden Methoden verwenden möchten, um anwendungskonsistente Snapshots von Ihrer EC2-Instance zu erstellen.

- Erstellen von VSS-Snapshots mit AWS Backup
- VSS-Snapshots mit Amazon Data Lifecycle Manager erstellen

Wenn Sie eine manuelle Installation durchführen müssen, empfehlen wir Ihnen, das neueste AWS-VSS-Komponentenpaket zu verwenden, um die Zuverlässigkeit und Leistung von anwendungskonsistenten Snapshots auf Ihren EC2-Windows-Instances zu verbessern.

> **Note**
>
> Um das Paket `AwsVssComponents` automatisch zu installieren oder zu aktualisieren, wenn Sie anwendungskonsistente Snapshots erstellen, empfehlen wir, dass Sie Systems Manager verwenden, um das Dokument `AWSEC2-VssInstallAndSnapshot` auszuführen. Weitere Informationen finden Sie unter AWSEC2-VssInstallAndSnapshot-Befehlsdokument ausführen (empfohlen).

Befolgen Sie die Schritte für Ihre bevorzugte Umgebung, um die VSS-Komponenten auf einer Amazon-EC2-Windows-Instance zu installieren.

Console

So installieren Sie die VSS-Komponenten mit SSM-Distributor

1. Öffnen Sie die AWS Systems Manager-Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich Run Command aus.
3. Wählen Sie Run Command (Befehl ausführen) aus.
4. Wählen Sie für Command document (Befehlsdokument) die Schaltfläche neben AWS-ConfigureAWSPackage aus.
5. Führen Sie unter Command parameters (Befehlsparameter) die folgenden Schritte aus:
   a. Stellen Sie sicher, dass Action (Aktion) auf Install (Installieren) festgelegt ist.
   b. Geben Sie unter Name `AwsVssComponents` ein.
   c. Geben Sie für Version eine Version ein oder lassen Sie das Feld leer, sodass Systems Manager die neueste Version installiert.
6. Identifizieren für Targets (Ziele) die Instances, in denen Sie diese Operation ausführen möchten, indem Sie Tags (Markierungen) angeben oder Instances manuell auswählen.

> **Note**
>
> Wenn Sie entscheiden, Instances manuell auszuwählen, und eine von Ihnen erwartete Instance nicht in der Liste enthalten ist, finden Sie Tipps zur Fehlerbehebung unter Einige meiner Instances fehlen im Benutzerhandbuch zu AWS Systems Manager.

7. Für Other parameters (Weitere Parameter):

   - (Optional) Geben Sie für Comment (Kommentar) Informationen zu diesem Befehl ein.
   - Geben Sie für Timeout (seconds) (Timeout (Sekunden)) in Sekunden an, wie lange gewartet werden soll, bis für die gesamte Befehlsausführung ein Fehler auftritt.

8. (Optional) Für Rate control (Ratenregelung):

   - Geben Sie unter Concurrency (Gleichzeitigkeit) entweder eine Zahl oder einen Prozentsatz für die Instances an, auf denen der Befehl gleichzeitig ausgeführt werden soll.

     > **Note**
     >
     > Wenn Sie Ziele anhand von Amazon-EC2-Tags (Markierungen) ausgewählt haben und noch nicht sicher sind, von wie vielen Instances die ausgewählten Tags (Markierungen) verwendet werden, sollten Sie die Anzahl von Instances für die gleichzeitige Ausführung des Dokuments beschränken, indem Sie einen Prozentsatz angeben.

   - Geben Sie unter Error threshold (Schwellenwert-Fehler) an, wann die Ausführung des Befehls auf anderen Instances beendet werden soll, nachdem dafür entweder auf einer bestimmten Anzahl oder einem Prozentsatz von Instances ein Fehler aufgetreten ist. Falls Sie beispielsweise drei Fehler angeben, sendet Systems Manager keinen Befehl mehr, wenn der vierte Fehler empfangen wird. Von Instances, auf denen der Befehl noch verarbeitet wird, werden unter Umständen ebenfalls Fehler gesendet.

9. (Optional) Wenn Sie im Abschnitt Ouput options (Ausgabeoptionen) die Befehlsausgabe in einer Datei speichern möchten, aktivieren Sie das Kontrollkästchen neben Enable writing to a S3 bucket (Schreiben in einen S3-Bucket aktivieren). Geben Sie den Bucket und (optional) die Präfixnamen (Ordner) an.

> **Note**
>
> Die S3-Berechtigungen zum Schreiben von Daten in einen S3-Bucket sind die Berechtigungen des der Instance zugewiesenen Instance-Profils und nicht diejenigen des -Benutzers, der diese Aufgabe ausführt. Weitere Informationen finden Sie unter EC2-Instance-Berechtigungen konfigurieren im Benutzerhandbuch für AWS Systems Manager.

10. (Optional) Geben Sie Optionen für SNS notifications (SNS-Benachrichtigungen) an.

    Weitere Informationen über das Konfigurieren von Amazon SNS-Benachrichtigungen für Run Command finden Sie unter Konfigurieren von Amazon SNS-Benachrichtigungen für AWS Systems Manager.

11. Wählen Sie Run (Ausführen) aus.

AWS CLI

Gehen Sie wie folgt vor, um mithilfe von Run Command über die `AwsVssComponents` das AWS CLI-Paket herunterzuladen und auf Ihren Instances zu installieren. Das Paket installiert zwei Komponenten: einen VSS-Anforderer und einen VSS-Anbieter. Das System kopiert diese Komponenten in ein Verzeichnis auf der Instance und registriert die Anbieter-DLL als VSS-Anbieter.

So installieren Sie das VSS-Paket

Führen Sie den folgenden Befehl aus, um die erforderlichen VSS-Komponenten für Systems Manager herunterzuladen und zu installieren.

```
aws ssm send-command \
    --document-name "AWS-ConfigureAWSPackage" \
    --instance-ids "i-1234567890abcdef0" \
    --parameters '{"action":["Install"],"name":["AwsVssComponents"]}'
```

PowerShell

Gehen Sie wie folgt vor, um mithilfe von Run Command aus den Tools for Windows PowerShell das `AwsVssComponents`-Paket herunterzuladen und auf Ihren Instances zu installieren. Das Paket installiert zwei Komponenten: einen VSS-Anforderer und einen VSS-Anbieter. Das System

kopiert diese Komponenten in ein Verzeichnis auf der Instance und registriert die Anbieter-DLL als VSS-Anbieter.

So installieren Sie das VSS-Paket

Führen Sie den folgenden Befehl aus, um die erforderlichen VSS-Komponenten für Systems Manager herunterzuladen und zu installieren.

```
Send-SSMCommand `
    -DocumentName "AWS-ConfigureAWSPackage" `
    -InstanceId "i-1234567890abcdef0" `
    -Parameter @{'action'='Install';'name'='AwsVssComponents'}
```

Überprüfen der Signatur für AWS-VSS-Komponenten

Gehen Sie wie folgt vor, um die Signatur für das `AwsVssComponents`-Paket zu überprüfen.

1. Herstellen einer Verbindung mit Ihrer Windows-Instance. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von RDP.
2. Rufen Sie C:\Programme\Amazon\AwsVssComponents auf.
3. Öffnen Sie das Kontextmenü (rechte Maustaste) für `ec2-vss-agent.exe` und wählen Sie dann Eigenschaften.
4. Navigieren Sie zur Registerkarte Digitale Signaturen und stellen Sie sicher, dass der Name des Signierers „Amazon Web Services Inc.“ lautet.
5. Überprüfen Sie mit den vorherigen Schritten auch die Signatur für `Ec2VssInstaller` und `Ec2VssProvider.dll`.

Das VSS-Komponentenpaket auf Ihrer EC2-Windows-Instance aktualisieren

Wir empfehlen, die VSS-Komponenten immer auf die neueste empfohlene Version zu aktualisieren. Es gibt verschiedene Möglichkeiten, wie Sie Komponenten aktualisieren können, wenn eine neue Version des Pakets `AwsVssComponents` veröffentlicht wird.

Update-Methoden

- Sie können die in VSS-Komponenten manuell auf einer EC2-Windows-Instance installieren beschriebenen Schritte wiederholen, wenn eine neue Version der AWS-VSS-Komponenten veröffentlicht wird.

- Sie können eine Systems-Manager-State-Manager-Zuordnung so konfigurieren, dass neue VSS-Komponenten automatisch heruntergeladen und installiert werden, sobald das Paket `AwsVssComponents` verfügbar ist.
- Sie können das Paket `AwsVssComponents` automatisch installieren oder aktualisieren, wenn Sie anwendungskonsistente Snapshots erstellen und den Systems Manager verwenden, um das Dokument `AWSEC2-VssInstallAndSnapshot` auszuführen.

> **Note**
>
> Wir empfehlen, dass Sie Systems Manager verwenden, um das Dokument mit dem Befehl `AWSEC2-VssInstallAndSnapshot` auszuführen, wodurch das Paket `AwsVssComponents` automatisch installiert oder aktualisiert wird, bevor die anwendungskonsistenten Snapshots erstellt werden. Weitere Informationen finden Sie unter AWSEC2-VssInstallAndSnapshot-Befehlsdokument ausführen (empfohlen).

Um eine Systems-Manager-State-Manager-Zuordnung zu erstellen, folgen Sie den Schritten für Ihre bevorzugte Umgebung.

Console

Wenn Sie eine Systems-Manager-State-Manager-Zuordnung erstellen, gibt es zwei Optionen für die Aktualisierung des `AwsVssComponents`-Pakets:

Deinstallieren und erneutes Installieren

Bei dieser Methode wird das Paket ohne zusätzliche Voraussetzungen heruntergeladen und installiert.

Direktes Update

Dadurch wird ein direktes Update für das Paket durchgeführt, für das die folgenden Voraussetzungen erfüllt sind:

- Die SSM-Agent-Version, die auf der Instance installiert ist, muss Version `3.3.808.0` oder höher sein. Weitere Informationen finden Sie unter Arbeiten mit dem SSM-Agent auf EC2-Instances für Windows Server im AWS Systems Manager-Benutzerhandbuch.
- Falls angegeben, muss die `AwsVssComponents`-Paketversion Version `2.5.0` oder höher sein. Frühere Versionen unterstützen kein direktes Update.

> **Note**
>
> Wenn Ihre Instance diese Voraussetzungen nicht erfüllt, schlägt das direkte Update fehl. Verwenden Sie stattdessen die Option Deinstallieren und erneutes Installieren.

So erstellen Sie eine State Manager-Zuordnung

1. Öffnen Sie die AWS Systems Manager-Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich Statusmanager aus.

   Oder, wenn die Systems Manager-Startseite zuerst geöffnet wird, öffnen Sie den Navigationsbereich und wählen Sie dann State Manager aus.
3. Wählen Sie Create association (Zuordnung erstellen) aus.
4. Geben Sie im Feld Name einen aussagekräftigen Namen ein.
5. Wählen Sie in der Liste Dokument die Option AWS-ConfigureAWSPackage aus.
6. Wählen Sie im Abschnitt Parameters (Parameter) die Option Install (Installieren) aus der Liste Action (Aktion) aus.
7. Wählen Sie für Installationstyp entweder Deinstallieren und neu installieren oder Direktes Update.
8. Geben Sie im Feld Name `AwsVssComponents` ein. Sie können die Felder Version und Additional Arguments leer lassen.
9. Wählen Sie im Abschnitt Targets (Ziele) eine Option aus.

   > **Note**
   >
   > Wenn Sie Ziel-Instances mittels Tags auswählen und Tags angeben, die Linux-Instances zugeordnet sind, ist die Zuordnung zwar auf der Windows-Instance erfolgreich, schlägt jedoch auf den Linux-Instances fehl. Der Gesamtstatus der Zuordnung zeigt Failed (Fehler) an.
10. Wählen Sie im Abschnitt Specify schedule eine Option.
11. Wählen Sie im Abschnitt Advanced options (Erweiterte Optionen) für Compliance severity (Compliance-Schweregrad) einen Schweregrad für die Zuordnung aus. Weitere Informationen finden Sie unter Erfahren Sie mehr über die Zuordnungs-Compliance. Wählen Sie für

Änderungskalender einen vorkonfigurierten Änderungskalender aus. Weitere Informationen finden Sie unter AWS Systems Manager-Change Calendar.

12. Gehen Sie für Ratenkontrolle wie folgt vor:

    - Geben Sie unter Nebenläufigkeit entweder eine Zahl oder einen Prozentsatz der verwalteten Knoten an, auf denen der Befehl gleichzeitig ausgeführt werden soll.
    - Geben Sie unter Fehlerschwellenwert an, wann die Ausführung des Befehls auf anderen verwalteten Knoten beendet werden soll, nachdem dafür entweder auf einer bestimmten Anzahl oder einem Prozentsatz von Knoten ein Fehler aufgetreten ist.

13. (Optional) Wenn Sie im Abschnitt Ausgabeoptionen die Befehlsausgabe in einer Datei speichern möchten, wählen Sie Schreiben der Ausgabe in S3 aktivieren aus. Geben Sie die Namen für den Bucket und das Präfix (Ordner) in die Textfelder ein.
14. Wählen Sie Create association (Zuordnung erstellen) und dann Close (Schließen) aus. Das System versucht, die Zuordnung auf den Instances zu erstellen und den Status sofort anzuwenden.

> **Note**
>
> Wenn EC2-Instances für Windows Server einen Fehlgeschlagen-Status anzeigen, überprüfen Sie, ob der SSM-Agent auf der Instance ausgeführt wird, und stellen Sie sicher, dass die Instance mit einer AWS Identity and Access Management (IAM)-Rolle für Systems Manager konfiguriert ist. Weitere Informationen finden Sie unter Einrichten von AWS Systems Manager.

AWS CLI

Sie können den Befehl create-association ausführen, um ein Distributor-Paket nach einem Zeitplan zu aktualisieren, ohne die zugehörige Anwendung offline zu schalten. Nur neue oder aktualisierte Dateien im Paket werden ersetzt.

So erstellen Sie eine State Manager-Zuordnung

Führen Sie den folgenden Befehl aus, um eine Zuordnung zu erstellen. Der Wert für `--name`, d. h. der Name des Dokuments, ist stets `AWS-ConfigureAWSPackage`. Der folgende Befehl verwendet den Schlüssel `InstanceIds` zur Angabe von Ziel-Instances.

```
aws ssm create-association \
```

```
    --name "AWS-ConfigureAWSPackage" \
    --parameters action=Install,installationType="Uninstall and
 reinstall",name=AwsVssComponents \
    --targets Key=InstanceIds,Values=i-1234567890abcdef0,i-000011112222abcde
```

PowerShell

So erstellen Sie eine State Manager-Zuordnung

Verwenden Sie das cmdlet New-SSMAssociation.

```
New-SSMAssociation `
    -Name "AWS-ConfigureAWSPackage" `
    -Parameter  @{
        "action" = "Install"
        "installationType" = "Uninstall and reinstall"
        "name" = "AwsVssComponents"
    } `
    -Target @{
        "Key" = "InstanceIds"
        "Values" = @("i-1234567890abcdef0", "i-000011112222abcde")
    }
```

Auf VSS basierende EBS-Snapshots für Ihre EC2-Windows-Instance erstellen

Nachdem Sie alle Voraussetzungen für die Erstellung von Windows-VSS-basierten EBS-Snapshots erfüllt haben, können Sie eine der folgenden Methoden verwenden, um VSS-basierte Snapshots von Ihrer EC2-Instance zu erstellen.

AWS Systems Manager-Befehlsdokumente

Verwenden Sie Systems-Manager-Befehlsdokumente, um VSS-basierte Snapshots zu erstellen.

Sie können Backups automatisieren, indem Sie eine AWS Systems Manager-Wartungsfenster-Aufgabe erstellen, die das Dokument `AWSEC2-VssInstallAndSnapshot` verwendet. Weitere Informationen finden Sie unter Arbeiten mit Wartungsfenstern (Konsole) im Benutzerhandbuch für AWS Systems Manager.

AWS Backup

Sie können bei der Verwendung von AWS Backup ein VSS-Backup erstellen, indem Sie VSS in der Konsole oder CLI aktivieren. Weitere Informationen finden Sie unter Creating Windows VSS backups im AWS Backup-Entwicklerhandbuch.

> **Note**
>
> AWS Backup installiert das `AwsVssComponents`-Paket nicht automatisch auf Ihrer Instance. Sie müssen in Ihrer Instance eine manuelle Installation durchführen. Weitere Informationen finden Sie unter VSS-Komponenten manuell auf einer EC2-Windows-Instance installieren.

Amazon Data Lifecycle Manager

Sie können VSS-Snapshots mit Amazon Data Lifecycle Manager erstellen, indem Sie Vor- und Nach-Skripte in Ihren Snapshot-Lebenszyklusrichtlinien aktivieren. Weitere Informationen finden Sie unter Automatisieren anwendungskonsistenter Snapshots im Amazon-EBS-Benutzerhandbuch.

> **Note**
>
> Amazon Data Lifecycle Manager installiert das `AwsVssComponents`-Paket nicht automatisch auf Ihrer Instance. Sie müssen in Ihrer Instance eine manuelle Installation durchführen. Weitere Informationen finden Sie unter VSS-Komponenten manuell auf einer EC2-Windows-Instance installieren.

Verwenden Sie die Systems-Manager-Befehlsdokumente, um VSS-aktivierte Snapshots zu erstellen

Sie können AWS Systems Manager-Befehlsdokumente verwenden, um VSS-aktivierte Snapshots zu erstellen. Im Folgenden werden die verfügbaren Befehlsdokumente und die Laufzeitparameter vorgestellt, die die Dokumente zur Erstellung Ihrer Snapshots verwenden.

Bevor Sie eines der Befehlsdokumente von Systems Manager verwenden, stellen Sie sicher, dass Sie alle Anforderungen von Voraussetzungen für die Erstellung von Windows-VSS-basierten EBS-Snapshots erfüllt haben.

Themen

- Parameter für VSS-Snapshot-Dokumente von Systems Manager
- VSS-Snapshot-Befehlsdokumente im Systems Manager ausführen

Parameter für VSS-Snapshot-Dokumente von Systems Manager

Die Systems-Manager-Dokumente, die VSS-Snapshots erstellen, verwenden alle die folgenden Parameter, sofern nicht anders angegeben:

AmiName (Zeichenfolge, optional)

Wenn die Option CreateAmi auf `True` festgelegt ist, geben Sie den Namen des AMI an, das das Backup erstellt.

description (Zeichenfolge, optional)

Geben Sie eine Beschreibung für die Snapshots oder das Image an, das dieser Prozess erstellt.

CollectDiagnosticLogs (Zeichenfolge, optional)

Um während der Schritte zur Snapshot- und AMI-Erstellung weitere Informationen zu sammeln, setzen Sie diesen Parameter auf „`True`“. Der Standardwert für diesen Parameter ist „`False`“. Konsolidierte Diagnoseprotokolle werden als `.zip`-Formatarchiv am folgenden Speicherort auf Ihrer Instance gespeichert:

`C:\ProgramData\Amazon\AwsVss\Logs\`*`timestamp`*`.zip`

CopyOnly (Zeichenfolge, optional)

Wenn Sie zusätzlich zu AWS VSS das native SQL-Server-Backup verwenden, verhindert das Ausführen eines Copy-only-Backups, dass AWS VSS die native differentielle Sicherungskette unterbricht. Um einen Copy-only-Backup-Vorgang durchzuführen, setzen Sie diesen Parameter auf `True`.

Der Standardwert für diesen Parameter ist `False`, was dazu führt, dass AWS VSS einen vollständigen Sicherungsvorgang durchführt.

CreateAmi (Zeichenfolge, optional)

Um ein VSS-fähiges Amazon Machine Image (AMI) zum Sichern Ihrer Instance zu erstellen, setzen Sie diesen Parameter auf `True`. Der Standardwert für diesen Parameter ist `False`, wodurch Ihre Instance stattdessen mit einem EBS-Snapshot gesichert wird.

Weitere Informationen zum Erstellen einer AMI von einer Instance finden Sie unter Ein Amazon-EBS-gestütztes AMI erstellen.

executionTimeout (Zeichenfolge, optional)

Geben Sie die maximale Zeit in Sekunden an, um den Snapshot-Erstellungsprozess auf der Instance auszuführen oder ein AMI aus der Instance zu erstellen. Wenn Sie dieses Timeout erhöhen, kann der Befehl länger warten, bis VSS mit dem Einfrieren beginnt und die Markierung der von ihm erstellten Ressourcen abgeschlossen hat. Dieses Timeout gilt nur für die Schritte zur Snapshot- oder AMI-Erstellung. Der erste Schritt zur Installation oder Aktualisierung des Pakets `AwsVssComponents` ist nicht im Timeout enthalten.

ExcludeBootVolume (Zeichenfolge, optional)

Mit dieser Einstellung werden Boot-Volumes aus dem Sicherungsvorgang ausgeschlossen, wenn Sie Snapshots erstellen. Um Boot-Volumes aus Ihren Snapshots auszuschließen, setzen Sie ExcludeBootVolume auf `True` und CreateAmi auf `False`.

Wenn Sie ein AMI für Ihr Backup erstellen, sollte dieser Parameter auf `False` gesetzt werden. Der Standardwert für diesen Parameter ist `False`.

NoWriters (Zeichenfolge, optional)

Um Anwendungs-VSS-Writer vom Snapshot-Vorgang auszuschließen, setzen Sie diesen Parameter auf `True`. Anwendungs-VSS-Writer auszuschließen kann Ihnen helfen, Konflikte mit VSS-Backup-Komponenten von Drittanbietern zu lösen. Der Standardwert für diesen Parameter ist `False`.

Wenn `SaveVssMetadata` `True` ist, muss dieser Parameter auf `False` gesetzt sein.

SaveVssMetadata (Zeichenfolge, optional)

Um VSS-Metadatendateien bei jedem Snapshot zu speichern, setzen Sie diesen Parameter auf `True`. Der Standardwert ist `False`. VSS-Metadatendateien geben Aufschluss darüber, welche Komponenten oder Writer in einen Backup-Vorgang einbezogen wurden und welche Dateien jeder Komponente zugeordnet sind.

Metadatendateien haben die zugehörige Snapshot-Set-ID im Namen. Sie finden sie an der folgenden Stelle auf Ihrer Instance:

```
C:\ProgramData\Amazon\AwsVss\VssMetadata\
```

> **Warning**
>
> - Das Speichern von VSS-Metadatendateien erfordert die `AwsVssComponents`-Paketversion 2.4.0 oder höher. Wenn auf Ihrer Instance eine frühere Version installiert ist, führt die Einstellung von `SaveVssMetadata` auf `True` dazu, dass die Snapshot-Erstellung fehlschlägt.
> - Die Parameter `NoWriters` und `SaveVssMetadata` schließen sich gegenseitig aus. Wenn beide auf `True` gesetzt sind, schlägt die Snapshot-Erstellung fehl.

tags (Zeichenfolge, optional)

Wir empfehlen Ihnen, Ihre Snapshots und Bilder mit Tags zu versehen, damit Sie Ihre Ressourcen leichter finden und verwalten können, z. B. um Volumes aus einer Liste von Snapshots wiederherzustellen. Das System fügt den `Name`-Schlüssel mit einem leeren Wert hinzu, in dem Sie den Namen angeben können, den Sie auf Ihre ausgegebenen Schnappschüsse oder Bilder anwenden möchten.

Wenn Sie zusätzliche Tags angeben möchten, trennen Sie die einzelnen Tags durch Semikolon. Beispiel, `Key=Environment,Value=Test;Key=User,Value=TestUser1`.

> **Note**
>
> Tag-Schlüssel und -Werte dürfen nur alphanumerische Zeichen und die folgenden Sonderzeichen enthalten: `( ) ./\-"'@_+:={}`.

Standardmäßig fügt das System die folgenden reservierten Tags für VSS-basierte Snapshots und Bilder hinzu.

- Gerät – Bei VSS-basierten Snapshots ist dies der Gerätename des EBS-Volumes, das der Snapshot erfasst.
- AppConsistent – Dieses Tag zeigt die erfolgreiche Erstellung eines VSS-basierten Snapshots oder AMIs an.
- AwsVssConfig – Identifiziert Snapshots und AMIs, die mit aktiviertem VSS erstellt wurden. Das Tag enthält Metainformationen wie die `AwsVssComponents`-Version und die Snapshot-Set-ID.

> **Warning**
>
> Die Angabe eines dieser reservierten Tags in Ihrer Parameterliste führt zu einem Fehler.

VssVersion (Zeichenfolge, optional)

Sie können nur für das `AWSEC2-VssInstallAndSnapshot`-Dokument den Parameter `VssVersion` angeben, um eine bestimmte Version des `AwsVssComponents`-Pakets auf Ihrer Instance zu installieren. Lassen Sie diesen Parameter leer, um die empfohlene Standardversion zu installieren.

Wenn die angegebene Version des Pakets `AwsVssComponents` bereits installiert ist, überspringt das Skript den Installationsschritt und fährt mit dem Backup-Schritt fort. Eine Liste der `AwsVssComponents`-Paketversionen und der Betriebsunterstützung finden Sie unter Versionsverlauf der AWS VSS-Lösung.

VSS-Snapshot-Befehlsdokumente im Systems Manager ausführen

VSS-fähige EBS-Snapshots mit AWS Systems Manager-Befehlsdokumenten können von Ihnen wie folgt erstellt werden.

AWSEC2-VssInstallAndSnapshot-Befehlsdokument ausführen (empfohlen)

Wenn Sie AWS Systems Manager verwenden, um das Dokument `AWSEC2-VssInstallAndSnapshot` auszuführen, führt das Skript die folgenden Schritte aus.

1. Das Skript installiert oder aktualisiert zuerst das Paket `AwsVssComponents` auf Ihrer Instance, je nachdem, ob es bereits installiert ist.
2. Das Skript erstellt die anwendungskonsistenten Snapshots, nachdem der erste Schritt abgeschlossen ist.

Folgen Sie den Schritten für Ihre bevorzugte Umgebung, um das Dokument `AWSEC2-VssInstallAndSnapshot` auszuführen.

Console

VSS-fähige EBS-Snapshots über die Konsole erstellen

1. Öffnen Sie die AWS Systems Manager-Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich Befehl ausführen. Hier wird gegebenenfalls eine Liste der Befehle angezeigt, die derzeit in Ihrem Konto ausgeführt werden.
3. Wählen Sie Befehl ausführen aus. Dadurch wird eine Liste von Befehlsdokumenten geöffnet, auf die Sie Zugriff haben.
4. Wählen Sie `AWSEC2-VssInstallAndSnapshot` aus der Liste der Befehlsdokumente aus. Um die Ergebnisse zu optimieren, können Sie den Dokumentnamen ganz oder teilweise eingeben. Sie können auch nach dem Eigentümer, nach Plattformtypen oder nach Tags filtern.

   Wenn Sie ein Befehlsdokument auswählen, werden die Details unter der Liste angezeigt.
5. Wählen Sie `Default version at runtime` aus der Liste der Dokumentversionen.
6. Konfigurieren Sie die Befehlsparameter, um zu definieren, wie `AWSEC2-VssInstallAndSnapshot` das Paket `AwsVssComponents` installieren und mit VSS-Snapshots oder einem AMI sichern soll. Einzelheiten zu den Parametern finden Sie unter Parameter für VSS-Snapshot-Dokumente von Systems Manager.
7. Geben Sie für Zielauswahl Tags an oder wählen Sie Instances manuell, um die Instances zu identifizieren, in denen Sie diesen Vorgang ausführen möchten.

   > **Note**
   >
   > Wenn Sie entscheiden, Instances manuell auszuwählen, und eine von Ihnen erwartete Instance nicht in der Liste enthalten ist, finden Sie Tipps zur Fehlersuche unter Wo sind meine Instances?.
8. Für zusätzliche Parameter zur Definition des Verhaltens von Systems Manager Run Command, wie z. B. die Ratensteuerung, geben Sie Werte ein, wie unter Befehle von der Konsole ausführen beschrieben.
9. Wählen Sie Run (Ausführen) aus.

   Bei Erfolg füllt der Befehl die Liste der EBS-Snapshots mit den neuen Snapshots. Sie können diese Snapshots in der Liste der EBS-Snapshots suchen, indem Sie nach den angegebenen

Tags (Markierungen) oder nach suchen `AppConsistent`. Wenn die Befehlsausführung fehlgeschlagen ist, zeigen Sie die Systems Manager-Befehlsausgabe an, um nähere Informationen zum Grund hierfür zu erfahren. Wenn der Befehl erfolgreich abgeschlossen wurde, ein bestimmtes Volume-Backup jedoch fehlgeschlagen ist, können Sie in der Liste der EBS-Volumes nach Informationen zur Problembehebung suchen.

AWS CLI

Sie können die folgenden Befehle in der AWS CLI ausführen, um VSS-basierte EBS-Snapshots zu erstellen und den Status der Snapshot-Erstellung abzurufen.

VSS-basierte Snapshots erstellen

Führen Sie den folgenden Befehl aus, um VSS-basierte EBS-Snapshots zu erstellen. Um die Snapshots zu erstellen, müssen Sie die Instances mit dem `--instance-ids`-Parameter identifizieren. Weitere Informationen zu andere Parameter, die Sie verwenden können, finden Sie unter Parameter für VSS-Snapshot-Dokumente von Systems Manager.

```
aws ssm send-command \
 --document-name "AWSEC2-VssInstallAndSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"],"VssVersion":[""]}'
```

Bei Erfolg füllt das Befehlsdokument die Liste der EBS-Snapshots mit den neuen Snapshots. Sie können diese Snapshots in der Liste der EBS-Snapshots suchen, indem Sie nach den angegebenen Tags (Markierungen) oder nach suchen `AppConsistent`. Wenn die Befehlsausführung fehlgeschlagen ist, zeigen Sie die -Befehlsausgabe an, um nähere Informationen zum Grund hierfür zu erfahren.

Abrufen des Befehlsstatus

Um den aktuellen Status der Snapshots abzurufen, führen Sie den folgenden Befehl mit der Befehls-ID aus, die von send-command zurückgegeben wurde.

```
aws ssm get-command-invocation
 --instance-ids "i-01234567890abcdef" \
 --command-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
 --plugin-name "CreateVssSnapshot"
```

PowerShell

Führen Sie die folgenden Befehle mit AWS Tools for Windows PowerShell aus, um VSS-basierte EBS-Snapshots zu erstellen und den aktuellen Laufzeitstatus bei der Erstellung Ihrer Ausgabe abzurufen. Geben Sie die in der vorherigen Liste beschriebenen Parameter an, um das Verhalten des Snapshot-Prozesses zu ändern.

VSS-fähige EBS-Snapshots mit PowerShell Tools für Windows erstellen

Führen Sie den folgenden Befehl aus, um VSS-basierte EBS-Snapshots oder AMIs zu erstellen.

```
Send-SSMCommand -DocumentName "AWSEC2-VssInstallAndSnapshot" -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
 ;'tags'='Key=key_name,Value=tag_value';'VssVersion'=''}
```

Abrufen des Befehlsstatus

Um den aktuellen Status der Snapshots abzurufen, führen Sie den folgenden Befehl mit der Befehls-ID aus, die von Send-SSMCommand zurückgegeben wurde.

```
Get-SSMCommandInvocationDetail -InstanceId "i-01234567890abcdef" -CommandId
 "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" -PluginName "CreateVssSnapshot"
```

Bei Erfolg füllt der Befehl die Liste der EBS-Snapshots mit den neuen Snapshots. Sie können diese Snapshots in der Liste der EBS-Snapshots suchen, indem Sie nach den angegebenen Tags (Markierungen) oder nach suchen `AppConsistent`. Wenn die Befehlsausführung fehlgeschlagen ist, zeigen Sie die -Befehlsausgabe an, um nähere Informationen zum Grund hierfür zu erfahren.

AWSEC2-CreateVssSnapshot-Befehlsdokument ausführen

Folgen Sie den Schritten für Ihre bevorzugte Umgebung, um das Dokument `AWSEC2-CreateVssSnapshot` auszuführen.

Console

VSS-fähige EBS-Snapshots über die Konsole erstellen

1. Öffnen Sie die AWS Systems Manager-Konsole unter https://console.aws.amazon.com/systems-manager/.

2. Wählen Sie im Navigationsbereich Befehl ausführen. Hier wird gegebenenfalls eine Liste der Befehle angezeigt, die derzeit in Ihrem Konto ausgeführt werden.
3. Wählen Sie Befehl ausführen aus. Dadurch wird eine Liste von Befehlsdokumenten geöffnet, auf die Sie Zugriff haben.
4. Wählen Sie `AWSEC2-CreateVssSnapshot` aus der Liste der Befehlsdokumente aus. Um die Ergebnisse zu optimieren, können Sie den Dokumentnamen ganz oder teilweise eingeben. Sie können auch nach dem Eigentümer, nach Plattformtypen oder nach Tags filtern.

   Wenn Sie ein Befehlsdokument auswählen, werden die Details unter der Liste angezeigt.
5. Wählen Sie `Default version at runtime` aus der Liste der Dokumentversionen.
6. Konfigurieren Sie die Befehlsparameter, um zu definieren, wie `AWSEC2-CreateVssSnapshot` mit VSS-Snapshots oder einem AMI gesichert werden soll. Einzelheiten zu den Parametern finden Sie unter Parameter für VSS-Snapshot-Dokumente von Systems Manager.
7. Geben Sie für Zielauswahl Tags an oder wählen Sie Instances manuell, um die Instances zu identifizieren, in denen Sie diesen Vorgang ausführen möchten.

   > **Note**
   >
   > Wenn Sie entscheiden, Instances manuell auszuwählen, und eine von Ihnen erwartete Instance nicht in der Liste enthalten ist, finden Sie Tipps zur Fehlersuche unter Wo sind meine Instances?.
8. Für zusätzliche Parameter zur Definition des Verhaltens von Systems Manager Run Command, wie z. B. die Ratensteuerung, geben Sie Werte ein, wie unter Befehle von der Konsole ausführen beschrieben.
9. Wählen Sie Run (Ausführen) aus.

   Bei Erfolg füllt der Befehl die Liste der EBS-Snapshots mit den neuen Snapshots. Sie können diese Snapshots in der Liste der EBS-Snapshots suchen, indem Sie nach den angegebenen Tags (Markierungen) oder nach suchen `AppConsistent`. Wenn die Befehlsausführung fehlgeschlagen ist, zeigen Sie die Systems Manager-Befehlsausgabe an, um nähere Informationen zum Grund hierfür zu erfahren. Wenn der Befehl erfolgreich abgeschlossen wurde, ein bestimmtes Volume-Backup jedoch fehlgeschlagen ist, können Sie in der Liste der EBS-Volumes nach Informationen zur Problembehebung suchen.

AWS CLI

Sie können den folgenden Befehl in der AWS CLI ausführen, um VSS-basierte EBS-Snapshots zu erstellen.

VSS-basierte Snapshots erstellen

Führen Sie den folgenden Befehl aus, um VSS-basierte EBS-Snapshots zu erstellen. Um die Snapshots zu erstellen, müssen Sie die Instances mit dem `--instance-ids`-Parameter identifizieren. Weitere Informationen zu andere Parameter, die Sie verwenden können, finden Sie unter Parameter für VSS-Snapshot-Dokumente von Systems Manager.

```
aws ssm send-command \
 --document-name "AWSEC2-CreateVssSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"]}'
```

Bei Erfolg füllt das Befehlsdokument die Liste der EBS-Snapshots mit den neuen Snapshots. Sie können diese Snapshots in der Liste der EBS-Snapshots suchen, indem Sie nach den angegebenen Tags (Markierungen) oder nach suchen `AppConsistent`. Wenn die Befehlsausführung fehlgeschlagen ist, zeigen Sie die -Befehlsausgabe an, um nähere Informationen zum Grund hierfür zu erfahren.

PowerShell

Führen Sie den folgenden Befehl mit AWS Tools for Windows PowerShell aus, um VSS-basierte EBS-Snapshots zu erstellen.

VSS-fähige EBS-Snapshots mit PowerShell Tools für Windows erstellen

Führen Sie den folgenden Befehl aus, um VSS-basierte EBS-Snapshots zu erstellen. Um die Snapshots zu erstellen, müssen Sie die Instances mit dem `InstanceId`-Parameter identifizieren. Sie können mehr als eine Instance angeben, für die Snapshots erstellt werden. Weitere Informationen zu andere Parameter, die Sie verwenden können, finden Sie unter Parameter für VSS-Snapshot-Dokumente von Systems Manager.

```
Send-SSMCommand -DocumentName AWSEC2-CreateVssSnapshot -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
```

```
;'tags'='Key=key_name,Value=tag_value'}
```

Bei Erfolg füllt der Befehl die Liste der EBS-Snapshots mit den neuen Snapshots. Sie können diese Snapshots in der Liste der EBS-Snapshots suchen, indem Sie nach den angegebenen Tags (Markierungen) oder nach suchen `AppConsistent`. Wenn die Befehlsausführung fehlgeschlagen ist, zeigen Sie die -Befehlsausgabe an, um nähere Informationen zum Grund hierfür zu erfahren. Wenn der Befehl erfolgreich abgeschlossen wurde, ein bestimmtes Volume-Backup jedoch fehlgeschlagen ist, können Sie in der Liste der EBS-Snapshots nach Informationen zur Problembehebung suchen.

Führen Sie Befehlsdokumente für einen Windows-Failover-Cluster mit gemeinsam genutztem EBS-Speicher aus

Sie können jedes der im vorherigen Abschnitt beschriebenen Befehlszeilenverfahren verwenden, um einen VSS-basierten Snapshot zu erstellen. Das Befehlsdokument (`AWSEC2-VssInstallAndSnapshot` oder `AWSEC2-CreateVssSnapshot`) muss auf dem Primärknoten in Ihrem Cluster ausgeführt werden. Das Dokument schlägt auf den sekundären Knoten fehl, da sie keinen Zugriff auf die gemeinsam genutzten Festplatten haben. Wenn sich Ihr primärer und sekundärer Knoten dynamisch ändern, können Sie das Dokument „Befehl AWS Systems Manager ausführen“ auf mehreren Knoten ausführen, in der Erwartung, dass der Befehl auf dem primären Knoten erfolgreich ist und auf sekundären Knoten fehlschlägt.

> **Note**
>
> Sie können Backups automatisieren, indem Sie in AWS Systems Manager eine Wartungsfenster-Aufgabe erstellen, die das Dokument `AWSEC2-VssInstallAndSnapshot` verwendet. Weitere Informationen finden Sie unter Arbeiten mit Wartungsfenstern (Konsole) im Benutzerhandbuch für AWS Systems Manager.

Problembehandlung bei Windows-VSS-basierten EBS-Snapshots

Bevor Sie andere Schritte zur Fehlerbehebung ausprobieren, empfehlen wir Ihnen, die folgenden Details zu überprüfen.

- Stellen Sie sicher, dass Sie alle Voraussetzungen für die Erstellung von Windows-VSS-basierten EBS-Snapshots erfüllt haben.

- Stellen Sie sicher, dass Sie das neueste Support von Windows-Betriebssystemversionen des `AwsVssComponents`-Pakets für Ihr Betriebssystem verwenden. Das von Ihnen beobachtete Problem wurde möglicherweise in neueren Versionen behoben.

Themen

- Protokolldateien prüfen
- Zusätzliche Diagnoseprotokolle sammeln
- VSS auf Instances mit konfiguriertem Proxy verwenden
- Fehler: Zeitüberschreitung bei der Thaw-Pipe-Verbindung, Fehler beim Thaw, Zeitüberschreitung beim Warten auf VSS Freeze oder andere Zeitüberschreitungsfehler
- Fehler: Methode kann nicht aufgerufen werden. Der Methodenaufruf wird in diesem Sprachmodus nur für Kerntypen unterstützt.

Protokolldateien prüfen

Wenn beim Erstellen von VSS-basierten EBS-Snapshots Probleme auftreten oder Fehlermeldungen angezeigt werden, können Sie die Befehlsausgabe in der Systems-Manager-Konsole anzeigen.

Für Systems-Manager-Dokumente, die VSS-Snapshots erstellen, können Sie den `CollectDiagnosticLogs`-Parameter zur Laufzeit auf „`True`“ setzen. Wenn der `CollectDiagnosticLogs`-Parameter auf „`True`“ gesetzt ist, sammelt VSS zusätzliche Protokolle, um das Debuggen zu erleichtern. Weitere Informationen finden Sie unter Zusätzliche Diagnoseprotokolle sammeln.

Wenn Sie Diagnoseprotokolle sammeln, speichert das Systems-Manager-Dokument sie auf Ihrer Instance am folgenden Ort: `C:\ProgramData\Amazon\AwsVss\Logs\`*`timestamp`*`.zip`. Der Standardwert für den Parameter `CollectDiagnosticLogs` ist „`False`“.

> **Note**
>
> Wenn Sie weitere Hilfe beim Debuggen benötigen, können Sie die `.zip`-Datei an Support senden.

Die folgenden zusätzlichen Protokolle sind verfügbar, unabhängig davon, ob Sie Diagnoseprotokolle sammeln oder nicht:

- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stdout`
- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stderr`

Sie können auch die Windows-Anwendung Event Viewer öffnen und Windows Logs (Windows-Protokolle), Application (Anwendung) auswählen, um zusätzliche Protokolle anzuzeigen. Um Ereignisse speziell vom EC2 Windows VSS Provider und dem Volume Shadow Copy Service anzuzeigen, filtern Sie nach Source (Quelle) nach den Begriffen **`Ec2VssSoftwareProvider`** und **`VSS`**.

Wenn Sie Systems Manager mit VPC-Endpunkten verwenden und die API-Aktion send-command von Systems Manager (Run Command in der Konsole) fehlgeschlagen ist, überprüfen Sie, ob Sie den folgenden Endpunkt richtig konfiguriert haben: com.amazonaws.***`region`***.ec2.

Ohne den definierten Amazon-EC2-Endpunkt schlägt der Aufruf zur Auflistung angefügter EBS-Volumes fehl. Dies führt dazu, dass der Systems-Manager-Befehl fehlschlägt. Weitere Informationen zum Einrichten von VPC-Endpunkten mit Systems Manager finden Sie unter Erstellen eines Virtual Private Cloud-Endpunkts im Benutzerhandbuch für AWS Systems Manager.

Zusätzliche Diagnoseprotokolle sammeln

Um zusätzliche Diagnoseprotokolle zu sammeln, wenn Sie das VSS-Snapshot-Dokument mit dem Sendebefehl von Systems Manager ausführen, setzen Sie den `CollectDiagnosticLogs`-Eingabeparameter zur Laufzeit auf „`True`“. Wir empfehlen Ihnen, diesen Parameter bei der Problembehandlung auf „`True`“ festzulegen.

Wählen Sie eine der folgenden Registerkarten, um ein Befehlszeilenbeispiel anzuzeigen.

AWS CLI

Im folgenden Beispiel wird das `AWSEC2-CreateVssSnapshot`-Systems-Manager-Dokument in der AWS CLI ausgeführt:

```
aws ssm send-command \
    --document-name "AWSEC2-CreateVssSnapshot" \
    --instance-ids "i-1234567890abcdef0" \
```

```
    --parameters '{"description":["Example - create diagnostic logs at
 runtime."],"tags":["Key=tag_name,Value=tag_value"],"CollectDiagnosticLogs":
["True"]}'
```

PowerShell

Im folgenden Beispiel wird das `AWSEC2-CreateVssSnapshot`-Systems-Manager-Dokument in PowerShell ausgeführt:

```
Send-SSMCommand `
    -DocumentName "AWSEC2-CreateVssSnapshot" `
    -InstanceId "i-1234567890abcdef0" `
    -Parameter @{'description'='Example - create diagnostic logs at
 runtime.';'tags'='Key=tag_name,Value=tag_value';'CollectDiagnosticLogs'='True'}
```

VSS auf Instances mit konfiguriertem Proxy verwenden

Wenn beim Erstellen von VSS-fähigen EBS-Snapshots in Instances, die einen Proxy zum Erreichen von EC2-Endpunkten verwenden, Probleme auftreten, stellen Sie folgende Einstellungen an Ihrer Instance sicher:

- Überprüfen Sie, ob der Proxy so konfiguriert ist, dass die EC2-Service-Endpunkte in der Region der Instance und IMDS erreichbar sind, indem AWS Tools for Windows PowerShell als SYSTEM ausgeführt werden.
- Um die Verwendung des vom System konfigurierten WinHTTP-Proxys zu unterstützen, stellen Sie sicher, dass Sie die neueste `AwsVssComponents`-Version auf Ihrer Instance installiert haben. Weitere Informationen zum Konfigurieren des WinHTTP-Proxys finden Sie unter Netsh-Befehle für Windows Hypertext Transfer Protocol (WINHTTP) auf der Microsoft-Website.

Fehler: Zeitüberschreitung bei der Thaw-Pipe-Verbindung, Fehler beim Thaw, Zeitüberschreitung beim Warten auf VSS Freeze oder andere Zeitüberschreitungsfehler

Der EC2-Windows-VSS-Provider kann aufgrund von Aktivitäten oder Services auf der Instance, die verhindern, dass VSS-fähige Snapshots rechtzeitig ausgeführt werden, die Zeit überschreiten. Das Windows VSS Framework bietet ein nicht konfigurierbares 10-Sekunden-Fenster, in dem die Kommunikation mit dem Dateisystem unterbrochen wird. Während dieser Zeit erstellt `AWSEC2-CreateVssSnapshot` Snapshots Ihrer Volumes.

Die folgenden Probleme können dazu führen, dass der EC2 Windows VSS Provider während eines Snapshots auf Zeitlimits stößt:

- Übermäßiger I/O für ein Volume
- Langsame Reaktion der EC2-API auf der Instance
- Fragmentierte Volumes
- Inkompatibilität mit einigen Antivirensoftwares
- Probleme mit einem VSS Application Writer
- Wenn die Modul-Logging für eine große Anzahl von PowerShell-Modulen aktiviert ist, kann dies dazu führen, dass PowerShell-Skripts langsam ausgeführt werden

Die meisten Zeitüberschreitungsprobleme, die bei der Ausführung des `AWSEC2-CreateVssSnapshot`-Befehlsdokuments auftreten, hängen damit zusammen, dass die Workload auf der Instance zum Zeitpunkt der Sicherung zu hoch ist. Die folgenden Aktionen können Ihnen dabei helfen, einen erfolgreichen Snapshot zu erstellen:

- Wiederholen Sie den Befehl `AWSEC2-CreateVssSnapshot`, um zu sehen, ob der Snapshot-Versuch erfolgreich ist. Wenn der Wiederholungsversuch in einigen Fällen erfolgreich ist, kann das Reduzieren der Instance-Last Snapshots erfolgreicher machen.
- Warten Sie eine Weile, bis der Workload der Instance abnimmt, und wiederholen Sie den Befehl `AWSEC2-CreateVssSnapshot`. Alternativ können Sie Snapshots versuchen, wenn bekannt ist, dass die Instance unter geringem Stress steht.
- Versuchen Sie VSS-Snapshots, wenn die Antivirensoftware auf dem System ausgeschaltet ist. Wenn das Problem dadurch behoben wird, lesen Sie die Anweisungen der Antivirensoftware und konfigurieren Sie sie so, dass VSS-Snapshots zulässig sind.
- Wenn Ihr Konto in derselben Region, in der Sie einen Snapshot ausführen, eine große Anzahl von Amazon-EC2-API-Aufrufen enthält, kann die API-Drosselung Snapshot-Vorgänge verzögern. Verwenden Sie das neueste `AwsVssComponents`-Paket, um die Auswirkungen der Drosselung zu reduzieren. Dieses Paket verwendet die EC2-API-Aktion `CreateSnapshots`, um die Anzahl mutierender Aktionen wie das Erstellen und Taggen von Snapshots pro Volume zu reduzieren.
- Wenn Sie mehrere `AWSEC2-CreateVssSnapshot`-Befehlsskripte gleichzeitig ausführen, können Sie die folgenden Schritte unternehmen, um Gleichzeitigkeitsprobleme zu verringern.
  - Erwägen Sie die Planung von Snapshots in Zeiten geringerer API-Aktivität.

  - Wenn Sie Run Command in der Systems-Manager-Konsole (oder SendCommand in der API) verwenden, um das Befehlsskript auszuführen, können Sie die Systems-Manager-Ratensteuerung verwenden, um die Gleichzeitigkeit zu reduzieren.

    Sie können auch Systems-Manager-Ratensteuerungen verwenden, um die Gleichzeitigkeit von Services wie AWS Backup zu reduzieren, die Systems Manager zur Ausführung des Befehlsskripts verwenden.
- Führen Sie den Befehl `vssadmin list writers` in einer Shell aus und prüfen Sie, ob er Fehler im Feld Last error (Letzter Fehler) für alle Autoren auf dem System meldet. Wenn Autoren einen time out (Timeout)-Fehler melden, sollten Sie Snapshots erneut versuchen, Snapshots erneut zu versuchen, wenn die Instance weniger belastet ist.
- Wenn Sie kleinere Instance-Typen wie *t2 | t3 | t3a*.nano oder *t2 | t3 | t3a*.micro verwenden, kann es aufgrund von Speicher- und CPU-Einschränkungen zu Timeouts kommen. Die folgenden Aktionen können dazu beitragen, Timeout-Probleme zu reduzieren.
  - Versuchen Sie, speicher- oder CPU-intensive Anwendungen zu schließen, bevor Sie Snapshots erstellen.
  - Versuchen Sie, Snapshots in Zeiten mit geringerer Instance-Aktivität zu erstellen.

Fehler: Methode kann nicht aufgerufen werden. Der Methodenaufruf wird in diesem Sprachmodus nur für Kerntypen unterstützt.

Dieser Fehler tritt auf, wenn der PowerShell-Sprachmodus nicht auf `FullLanguage` eingestellt ist. Das SSM-Dokumente `AWSEC2-CreateVssSnapshot` erfordert, dass PowerShell im `FullLanguage`-Modus konfiguriert ist.

Um den Sprachmodus zu überprüfen, führen Sie den folgenden Befehl auf der Instance in einer PowerShell-Konsole aus:

```
$ExecutionContext.SessionState.LanguageMode
```

Weitere Informationen über Sprachmodi finden Sie unter about_Language_Modes in der Microsoft-Dokumentation.

Verwenden Sie die AWS-VSS-Lösung, um Daten für Ihre Instance wiederherzustellen.

Sie können EBS-Volumes für eine Windows-Instance aus VSS-basierten Snapshots wiederherstellen, die von der AWS-VSS-Lösung erstellt wurden. Wenn Ihre AWS-VSS-Lösungssnapshots Backups einer Microsoft-SQL-Server-Datenbank enthalten, können Sie die Datenbank mithilfe des AWS Systems Manager Automation Runbooks `AWSEC2-RestoreSqlServerDatabaseWithVss` wiederherstellen.

Das Runbook zur Datenbankwiederherstellung automatisiert den gesamten Wiederherstellungsprozess, einschließlich der Erstellung von Volumes aus den Snapshots und deren Anfügung an die Instance. Bei der Automatisierung wird die Datenbank mithilfe der VSS-Technologie wiederhergestellt, sodass Sie die Datenbank wiederherstellen können, ohne Ihre SQL-Server-Anwendung anzuhalten oder aktive Verbindungen zu trennen.

Ausführliche Anweisungen zur Verwendung des Runbooks für Microsoft-SQL-Server-Datenbanken finden Sie unter Wiederherstellung aus VSS-basierten Snapshots im Benutzerhandbuch für Microsoft SQL Server in Amazon EC2.

Ein Skript anpassen, um EBS-Volumes aus Snapshots von AWS-VSS-Lösungen wiederherzustellen

Sie können das `RestoreVssSnapshotSampleScript.ps1`-Skript als Modell verwenden, um Ihr eigenes benutzerdefiniertes Skript zu erstellen, das EBS-Volumes aus Snapshots von AWS-VSS-Lösungen wiederherstellt. Das Beispielsskript führt die folgenden Aufgaben aus:

- Anhalten einer Instance
- Entfernen aller vorhandenen Laufwerke aus der Instance (mit Ausnahme des Stamm-Volumes, wenn es ausgeschlossen wurde)
- Erstellen neuer Volumes von den Snapshots
- Anfügen der Volumes an die Instance mithilfe des Geräte-ID-Tags (Markierung) auf dem Snapshot
- Neustart der Instance

> **Important**
>
> Das folgende Skript trennt alle Volumes ab, die einer Instance angefügt sind, und erstellt dann neue Volumes von einem Snapshot. Stellen Sie sicher, dass Sie die Instance

ordnungsgemäß gesichert haben. Die alten Volumes werden nicht gelöscht. Wenn Sie möchten, können Sie das Skript bearbeiten, um die alten Volumes zu löschen.

So stellen Sie Volumes aus VSS-fähigen EBS-Snapshots wieder her

1. Laden Sie die Datei RestoreVssSnapshotSampleScript.zip herunter und extrahieren Sie die Inhalte.
2. Öffnen Sie `RestoreVssSnapshotSampleScript.ps1` in einem Texteditor und bearbeiten Sie den Beispielaufruf unten im Skript mit einer gültigen EC2-Instance-ID und EBS-Snapshot-ID und führen Sie dann das Skript in PowerShell aus.

Versionsverlauf der AWS VSS-Lösung

Diese Seite enthält Versionshinweise für das AWS-VSS-Komponentenpaket und die Anforderungen an die Komponenten- und Skriptversion für jede unterstützte Version von Windows Server.

Themen

- AwsVssComponents-Paketversionen
- Support von Windows-Betriebssystemversionen

AwsVssComponents-Paketversionen

In der folgenden Tabelle werden die veröffentlichten Versionen des AWS VSS-Komponentenpakets beschrieben.

Version	Details	Datum der Veröffentlichung	herunterladbar
2.5.1	Es wurde ein Fall behoben, bei dem die Wiederherstellung der SQL-Datenbank fehlschlagen konnte, wenn der Zieldatenbankparameter angegeben wurde.	13. März 202	Ja
2.5.0	•	17. Januar 2025	Ja

Version	Details	Datum der Veröffentlichung	herunterladbar
	Es wurde die Möglichkeit hinzugefügt, VSS-Metadatendateien zu lesen und eine Microsoft-SQL-Server-Datenbank auf der Instance wiederherzustellen. Weitere Informationen finden Sie unter Wiederherstellung aus VSS-basierten Snapshots im Benutzerhandbuch für Microsoft SQL Server in Amazon EC2. • Unterstützung für die Option zum direkten Update bei der Installation oder Aktualisierung des `AwsVssComponents` -Pakets wurde hinzugefügt.		
2.4.0	Es wurde die Möglichkeit hinzugefügt, VSS-Metadatendateien bei der Snapshot-Erstellung zu speichern. Informationen zum Aktivieren dieses Features finden Sie unter SaveVssMetadata in Parameter für VSS-Snapshot-Dokumente von Systems Manager.	7. Oktober 2024	Ja
2.3.3	Der VSS-Agent wurde aktualisiert, um sicherzustellen, dass der `Ec2VssProvider` bei der Snapshot-Erstellung verwendet wird.	25. Juni 2024	Ja
2.3.2	Es wurde ein Fall behoben, bei dem die Registrierung des VSS-Anbieters bei der Deinstallation nicht entfernt wurde.	9. Mai 2024	Ja
2.3.1	Es wurde ein neues Standard-Tag `AwsVssConfig` zur Identifizierung von Snapshots und AMIs hinzugefügt, die von AWS-VSS erstellt wurden.	7. März 2024	Ja

Version	Details	Datum der Veröffentlichung	herunterladbar
2.2.1	• Unterstützung für die Verwendung der `DescribeInstanceAttribute` -API hinzugefügt. • Fehlerbehebungen und verbesserte Zuverlässigkeit. • Die Unterstützung für Windows Server 2012 und 2012 R2 wurde eingestellt. AWS Die Installation der VSS-Komponenten Version 2.2.1 auf Windows Server 2012 und 2012 R2 wird fehlschlagen. AWS VSS-Komponentenversion 2.1.0 ist die letzte Version, die Windows Server 2012 und 2012 R2 unterstützt.	18. Januar 2(	Ja
2.1.0	Unterstützung für die Verwendung der `CreateSnapshots` -API hinzugefügt.	6. November	Ja
2.0.1	Unterstützung für die Verwendung der WinHTTP-Proxy-Einstellungen hinzugefügt.	26. Oktober 2023	Nein
2.0.0	Die AWS-VSS-Komponente wurde um die Fähigkeit erweitert, Snapshots und AMIs zu erstellen, was die Kompatibilität mit PowerShell-Modulprotokollierung, Skriptblockprotokollierung und Transkriptionsfeatures ermöglicht.	28. April 202	Nein
1.3.2.0	Es wurde ein Fall behoben, bei dem ein Installationsfehler nicht korrekt gemeldet wurde.	10. Mai 2022	Nein

Version	Details	Datum der Veröffentlichung	herunterladbar
1.3.1.0	• Snapshots, die auf Domain-Controllern im Zusammenhang mit einem NTDS-VSS Schreiber-Protokollierungsfehler fehlgeschlagen sind, wurden behoben. • Es wurde ein VSS-Agent-Fehler beim Deinstallieren von Version 1.0 des VSS-Anbieters behoben.	6. Februar 2020	Ja
1.3.00	• Verbesserte Protokollierung durch Reduzierung unerwünschter Ausführlichkeit. • Es wurden Regionalisierungsprobleme während der Installation behoben. • Es wurden Rückgabecodes für einige Anbieter-Registrierungsfehlerbedingungen korrigiert. • Es wurden verschiedene Installationsprobleme behoben.	19. März 2019	Nein
1.2.00	• Dem Agenten wurden Befehlszeilenparameter `-nw` (no-writers) und `-copy` (copy-only) hinzugefügt. • Es wurden EventLog-Fehler behoben, die durch falsche Speicherzuweisungsaufrufe verursacht wurden.	15. Novembe	Nein

Version	Details	Datum der Veröffentlichung	herunterladbar
1.1	Es wurde behoben, dass AWS-VSS-Komponenten fälschlicherweise als standardmäßiger Windows-Sicherungs- und Wiederherstellungsanbieter verwendet wurde.	12. Dezember 2017	Nein
1,0	Erstversion.	20. November 2017	Nein

Support von Windows-Betriebssystemversionen

Die folgende Tabelle zeigt, welche AWS VSS-Lösungsversionen Sie unter den einzelnen Versionen von Windows Server in Amazon EC2 verwenden sollten.

Windows Server Version	AwsVssComponents-Version	AWSEC2-VssInstallAndSnapshot-Versionsname	AWSEC2-CreateVssSnapshot-Versionsname
Windows Server 2025	default	default	default
Windows Server 2022	default	default	default
Windows Server 2019	default	default	default
Windows Server 2016	default	default	default

Windows Server Version	AwsVssComponents-Version	AWSEC2-VssInstallAndSnapshot-Versionsname	AWSEC2-CreateVssSnapshot-Versionsname
Windows Server 2012 R2	2.1.0	Nicht unterstützt	2012R2
Windows Server 2012	2.1.0	Nicht unterstützt	2012R2
Windows Server 2008 R2	1.3.1.0	Nicht unterstützt	2008R2

Objektspeicher, Dateispeicher und Datei-Caching in Amazon EC2

Der Cloud-Datenspeicher ist eine Methode zur Speicherung von Daten in der Cloud, die Servern und Anwendungen den Zugriff auf Daten über gemeinsam genutzte Dateisysteme ermöglicht. Dank dieser Kompatibilität eignet sich der Cloud-Datenspeicher ideal für Workloads, die auf gemeinsam genutzten Dateisystemen basieren und ermöglicht zudem eine einfache Integration ohne Codeänderungen.

Es gibt zahlreiche Dateispeicherlösungen. Sie reichen von einem Einzelknoten-Dateiserver auf einer Datenverarbeitungs-Instance – mit Blockspeicher als Fundament, ohne Skalierbarkeit oder mit wenig Redundanz zum Schutz von Daten – über eine selbst erstellte Cluster-Lösung bis hin zu vollständig verwalteten Lösungen. Der folgende Inhalt enthält einige der Speicherservices, die von AWS zur Verwendung mit Amazon-EC2-Instances bereitgestellt werden.

Inhalt

- Amazon S3 mit Amazon EC2 verwenden
- Amazon EFS mit Amazon-EC2-Linux-Instances verwenden
- Amazon FSx mit Amazon-EC2-Instances verwenden
- Amazon File Cache mit Amazon-EC2-Instances verwenden

Amazon S3 mit Amazon EC2 verwenden

Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, der branchenführende Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet. Sie können Amazon S3 verwenden, um beliebige Datenmengen für eine Reihe von Anwendungsfällen zu speichern und abzurufen, z. B. für Data Lakes, Websites, Backups und Big-Data-Analytik, von einer Amazon-EC2-Instance oder von einem beliebigen Ort im Internet aus. Weitere Informationen finden Sie unter Was ist Amazon S3?

Objekte sind die Grundeinheiten, die in Amazon S3 gespeichert sind. Jedes in Amazon S3 gespeicherte Objekt ist in einem Bucket enthalten. Buckets organisieren den Amazon S3-Namespace auf der höchsten Ebene und ermitteln das für die Speicherung verantwortliche Konto. Amazon-S3-Buckets sind ähnlich wie Internet-Domain-Namen. Die in den Buckets gespeicherten Objekte haben einen eindeutigen Schlüsselwert und werden über eine URL abgerufen. Wenn beispielsweise ein Objekt mit dem Schlüsselwert `/photos/mygarden.jpg` in dem Bucket `amzn-s3-demo-bucket1` gespeichert ist, kann es über die URL `https://amzn-s3-demo-bucket1.s3.amazonaws.com/photos/mygarden.jpg` abgerufen werden. Weitere Informationen finden Sie unter Funktionsweise von Amazon S3.

Verwendungsbeispiele

Wegen der Vorteile, die Amazon S3 bei der Speicherung hat, können Sie diesen Service zum Speichern von Dateien und Datensätzen zur Verwendung mit EC2-Instances nutzen. Es gibt verschiedene Möglichkeiten, Daten zu und von Amazon S3 zu Ihren Instances zu verschieben. Zusätzlich zu den unten dargestellten Beispielen gibt es eine Vielzahl von Tools, die von Developern verfasst wurden und die Sie dazu verwenden können, von Ihrem Computer oder Ihrer Instance auf die in Amazon S3 gespeicherten Daten zuzugreifen.

Wenn Sie eine entsprechende Berechtigung haben, können Sie mit einer der folgenden Methoden eine Datei zu oder von Amazon S3 und Ihrer Instance kopieren.

wget

> **Note**
>
> Diese Methode funktioniert nur für öffentliche Objekte. Wenn das Objekt nicht öffentlich ist, erhalten Sie die Meldung `ERROR 403: Forbidden`. Wenn Sie diese Fehlermeldung erhalten, müssen Sie die Amazon-S3-Konsole, die AWS CLI, die AWS-API, das AWS-SDK oder die AWS Tools for Windows PowerShell verwenden sowie über die

erforderlichen Berechtigungen verfügen. Weitere Informationen finden Sie unter Identity and Access Management für Amazon S3 und Herunterladen eines Objekts im Amazon-S3-Benutzerhandbuch.

Das Dienstprogramm wget ist ein HTTP- und FTP-Client, der es ermöglicht, öffentliche Objekte von Amazon S3 herunterzuladen. Es ist standardmäßig in Amazon Linux und den meisten anderen Verteilungen installiert und bei Windows zum Download verfügbar. Verwenden Sie zum Herunterladen eines Amazon S3-Objekts den folgenden Befehl, wobei die URL des herunterzuladenden Objekts ersetzt wird.

```
[ec2-user ~]$ wget https://amzn-s3-demo-bucket.s3.amazonaws.com/path-to-file
```

PowerShell

Sie können AWS Tools for Windows PowerShell verwenden, um Objekte zu und von Amazon S3 zu verschieben.

Verwenden Sie das cmdlet Copy-S3Object, um ein Amazon S3-Objekt in Ihre Windows-Instance zu kopieren:

```
Copy-S3Object `
    -BucketName amzn-s3-demo-bucket `
    -Key path-to-file `
    -LocalFile my_copied_file.ext
```

Alternativ können Sie die Amazon-S3-Konsole mit einem Webbrowser auf der Windows-Instance öffnen.

AWS CLI

Sie können die AWS Command Line Interface (AWS CLI) verwenden, um Elemente mit beschränktem Zugriff von Amazon S3 herunterzuladen und auch, um Elemente hochzuladen. Weitere Informationen, z. B. darüber, wie die Tools installiert und konfiguriert werden, finden Sie auf der AWS Command Line Interface-Detailseite.

Der Befehl aws s3 cp ähnelt dem Unix-cp-Befehl. Sie können Dateien von Amazon S3 in Ihre Instance, von Ihrer Instance in Amazon S3 und von einem Amazon S3-Standort zu einem anderen kopieren.

Verwenden Sie den folgenden Befehl, um ein Objekt von Amazon S3 in Ihre Instance zu kopieren.

```
aws s3 cp s3://amzn-s3-demo-bucket/my_folder/my_file.ext my_copied_file.ext
```

Verwenden Sie den folgenden Befehl, um ein Objekt von Ihrer Instance zurück nach Amazon S3 zu kopieren.

```
aws s3 cp my_copied_file.ext s3://amzn-s3-demo-bucket/my_folder/my_file.ext
```

Mit dem Befehl aws s3 sync lässt sich ein ganzer Amazon-S3-Bucket mit einem Speicherort in einem lokalen Verzeichnis synchronisieren. Dies kann hilfreich sein, um einen Datensatz herunterzuladen und die lokale Kopie mit dem dezentralen Datensatz aktuell zu halten. Wenn Sie die entsprechenden Berechtigungen für den Amazon S3-Bucket haben, können Sie Ihr lokales Verzeichnis nach Abschluss der Änderungen wieder in die Cloud verlagern, indem Sie in dem Befehl die Quell- und Zielspeicherorte vertauschen.

Verwenden Sie den folgenden Befehl, um einen ganzen Amazon S3-Bucket zu einem lokalen Verzeichnis auf Ihrer Instance herunterzuladen.

```
aws s3 sync s3://amzn-s3-demo-source-bucket local_directory
```

Amazon S3 API

Wenn Sie Developer sind, können Sie eine API zum Zugriff auf Daten in Amazon S3 verwenden. Sie können diese API verwenden, um Ihre Anwendung zu entwickeln und sie in andere APIs und SDKs zu integrieren. Weitere Informationen finden Sie unter Codebeispiele für Amazon S3 mit AWS-SDKs in der API-Referenz für Amazon Simple Storage Service.

Amazon EFS mit Amazon-EC2-Linux-Instances verwenden

> **Note**
>
> Amazon EFS wird von Windows-Instances nicht unterstützt.

Amazon EFS bietet skalierbaren Dateispeicher für die Verwendung mit Amazon EC2. Sie können ein EFS-Dateisystem als gemeinsame Datenquelle für Workloads und Anwendungen verwenden,

die jeweils auf mehr als einer Instance ausgeführt werden. Weitere Informationen finden Sie auf der Amazon Elastic File System-Produktseite.

Dieses Tutorial zeigt Ihnen, wie Sie ein Amazon-EFS-Dateisystem auf einer Linux-Instance mithilfe dem Amazon-EFS-Schnellerstellungs-Assistenten beim Instance-Start erstellen und anhängen. Ein Tutorial zum Erstellen eines Dateisystems mit der Amazon-EFS-Konsole finden Sie unter Erste Schritte mit Amazon Elastic File System im Benutzerhandbuch zu Amazon Elastic File System.

> **Note**
>
> Wenn Sie ein EFS-Dateisystem mit EFS-Quick-Create erstellen, wird das Dateisystem mit den folgenden vom Dienst empfohlenen Einstellungen erstellt:
>
> - Automatische Sicherungen sind aktiviert.
> - Mount-Ziele verwalten in der ausgewählten VPC.
> - Allzweck-Leistungsmodus.
> - Bursting-Durchsatzmodus.
> - Verschlüsselung von Daten im Ruhezustand aktiviert mit Ihrem Standardschlüssel für Amazon EFS (`aws/elasticfilesystem`).
> - Amazon-EFS-Lebenszyklusverwaltung aktiviert mit einer 30-Tage-Richtlinie.

Aufgaben

- Erstellen eines EFS-Dateisystems mit Amazon EFS-Quick-Create
- Testen des EFS-Dateisystems
- Löschen des EFS-Dateisystems

Erstellen eines EFS-Dateisystems mit Amazon EFS-Quick-Create

Sie können ein EFS-Dateisystem erstellen und es in Ihrer Instance mounten, wenn Sie Ihre Instance mit dem Quick-Create-Feature von Amazon EFS des Launch Instance Wizard von Amazon EC2 starten.

Erstellen eines EFS-Dateisystems mit Amazon EFS-Quick-Create

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Launch Instance (Instance starten) aus.

3. (Optional) Geben Sie unter Name and tags (Name und Tags) für Name einen Namen ein, um Ihre Instance zu identifizieren.
4. Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) ein Linux-Betriebssystem und dann für Amazon Machine Image (AMI) ein Linux-AMI aus.
5. Wählen Sie unter Instance type (Instance-Typ) einen Instance type (Instance-Typ) aus oder behalten Sie die Standardeinstellung bei.
6. Wählen Sie unter Schlüsselpaar (Anmeldung) für Schlüsselpaarname ein vorhandenes Schlüsselpaar aus oder erstellen Sie ein neues.
7. Wählen Sie unter Network settings (Netzwerkeinstellungen) Edit (Bearbeiten) (rechts) und dann für Subnet (Subnetz) ein Subnetz aus.

   > **Note**
   >
   > Sie müssen ein Subnetz auswählen, bevor Sie ein EFS-Dateisystem hinzufügen können.

8. Wählen Sie unter Configure storage (Speicher konfigurieren) die Option Edit (Bearbeiten) (unten rechts) und gehen Sie dann wie folgt vor:

   a. Stellen Sie für Dateisysteme sicher, dass EFS ausgewählt ist, und wählen Sie dann Neues gemeinsam genutztes Dateisystem erstellen aus.

   b. Geben Sie unter Dateisystemname einen Namen für das Amazon-EFS-Dateisystem ein und wählen Sie dann Dateisystem erstellen.

   c. Geben Sie für Mount-Punkt einen Mount-Punkt an oder behalten Sie die Standardeinstellung bei.

   d. Um den Zugriff auf das Dateisystem zu ermöglichen, wählen Sie Automatically create and attach security groups (Sicherheitsgruppen automatisch erstellen und anfügen) aus. Wenn Sie dieses Kontrollkästchen aktivieren, werden die erforderlichen Sicherheitsgruppen automatisch erstellt und der Instance und den Mounting-Zielen des Dateisystems angefügt:

      - Instance-Sicherheitsgruppe – Enthält eine Ausgangsregel, die Datenverkehr über den Port NFS 2049 zulässt, enthält jedoch keine Eingangsregeln.
      - Sicherheitsgruppe für Mounting-Ziele für Dateisysteme – Enthält eine eingehende Regel, die den Datenverkehr über den NFS-2049-Port von der Instance-Sicherheitsgruppe (oben beschrieben) zulässt, und eine Regel für ausgehenden Datenverkehr über den NFS-2049-Port.

> **Note**
>
> Sie können die Sicherheitsgruppen alternativ auch manuell erstellen und anhängen. Wenn Sie die Sicherheitsgruppen manuell erstellen und anfügen möchten, deaktivieren Sie Automatically create and attach the required security groups (Erforderliche Sicherheitsgruppen automatisch erstellen und anfügen).

e. Um das gemeinsam genutzte Dateisystem beim Start der Instance automatisch zu mounten, wählen Sie Automatically mount shared file system by attaching required user data script (Gemeinsam genutztes Dateisystem automatisch mounten, indem Sie das erforderliche Benutzerdatenskript anfügen). Um die automatisch generierten Benutzerdaten anzuzeigen, erweitern Sie Advanced details (Erweiterte Details) und scrollen Sie nach unten zu User data (Benutzerdaten).

> **Note**
>
> Wenn Sie Benutzerdaten hinzugefügt haben, bevor Sie dieses Kontrollkästchen aktiviert haben, werden die ursprünglichen Benutzerdaten durch die automatisch generierten Benutzerdaten überschrieben.

9. Konfigurieren Sie alle anderen Einstellungen der Instance-Konfiguration nach Bedarf.
10. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten.

Testen des EFS-Dateisystems

Sie können eine Verbindung zu Ihrer Instance herstellen und überprüfen, ob das Dateisystem in dem von Ihnen angegebenen Verzeichnis gemountet ist (z. B. /mnt/efs).

Überprüfen Sie wie folgt, ob das Dateisystem aufgespielt wurde:

1. Verbinden Sie sich mit der Instance. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance mit SSH.
2. Führen Sie im Terminalfenster der Instance den df -T-Befehl aus, um zu überprüfen, ob das EFS-Dateisystem gemountet ist.

```
$ df -T
Filesystem     Type              1K-blocks    Used          Available Use% Mounted
 on
/dev/xvda1     ext4                8123812 1949800            6073764  25% /
devtmpfs       devtmpfs            4078468      56            4078412   1% /dev
tmpfs          tmpfs               4089312       0            4089312   0% /dev/shm
efs-dns        nfs4       9007199254740992       0   9007199254740992   0% /mnt/efs
```

Beachten Sie, dass der Name des Dateisystems, der in der Beispielausgabe *efs-dns* lautet, das folgende Format aufweist.

```
file-system-id.efs.aws-region.amazonaws.com:/
```

3. (Optional) Erstellen Sie eine Datei im Dateisystem der Instance, und überprüfen Sie dann, ob Sie die Datei von einer anderen Instance aus anzeigen können.

   a. Führen Sie in der Instance den folgenden Befehl aus, um die Datei zu erstellen.

   ```
   $ sudo touch /mnt/efs/test-file.txt
   ```

   b. Führen Sie in der anderen Instance den folgenden Befehl aus, um die Datei anzuzeigen.

   ```
   $ ls /mnt/efs
   test-file.txt
   ```

Löschen des EFS-Dateisystems

Sie können Ihren Dateisystem löschen, falls Sie ihn nicht mehr benötigen.

Löschen Sie das Dateisystem wie folgt:

1. Öffnen Sie die Amazon Elastic File System-Konsole unter https://console.aws.amazon.com/efs/.
2. Wählen Sie das Dateisystem aus, das Sie löschen möchten.
3. Wählen Sie Actions (Aktionen) und Delete file system (Dateisystem löschen) aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie die Dateisystem-ID ein und wählen Sie Dateisystem löschen.

Amazon FSx mit Amazon-EC2-Instances verwenden

Die Amazon-FSx-Servicefamilie erleichtert das Starten, Ausführen und Skalieren von freigegebenem Speicher, der auf gängigen kommerziellen und Open-Source-Dateisystemen basiert. Sie können den neuen Launch Instance Wizard verwenden, um beim Start automatisch die folgenden Arten von Amazon-FSx-Dateisystemen an Ihre Amazon-EC2-Instances anzufügen:

- Amazon FSx for NetApp ONTAP bietet vollständig verwalteten freigegebenen Speicher in der AWS Cloud mit den beliebten Datenzugriffs- und Verwaltungsfunktionen von NetApp ONTAP.
- Amazon FSx for OpenZFS bietet vollständig verwalteten, kosteneffektiven freigegebenen Speicher, der auf dem beliebten OpenZFS-Dateisystem basiert.

> **Note**
>
> - Diese Funktionalität ist nur im neuen Launch Instance Wizard verfügbar. Weitere Informationen finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten
> - Amazon-FSx-for-Windows-File-Server- und Amazon-FSx-for-Lustre-Dateisysteme können beim Start nicht bereitgestellt werden. Sie müssen diese Dateisysteme nach dem Start manuell bereitstellen.

Sie können ein vorhandenes Dateisystem bereitstellen, das Sie zuvor erstellt haben oder Sie können ein neues Dateisystem erstellen, das beim Start in einer Instance bereitgestellt werden soll.

Themen

- Sicherheitsgruppen und Benutzerdatenskript
- Bereitstellen eines Amazon-FSx-Dateisystems beim Start

Sicherheitsgruppen und Benutzerdatenskript

Wenn Sie ein Amazon-FSx-Dateisystem mithilfe des Launch Instance Wizard in einer Instance bereitstellen, können Sie wählen, ob die Sicherheitsgruppen, die zum Aktivieren des Zugriffs auf das Dateisystem erforderlich sind, automatisch erstellt und angefügt werden sollen, und ob die Benutzerdatenskripte, die benötigt werden, um das Dateisystem bereitzustellen und zur Nutzung verfügbar zu machen, automatisch eingeschlossen werden sollen.

Themen

- Sicherheitsgruppen
- Benutzerdatenskript

Sicherheitsgruppen

Wenn Sie wählen, die Sicherheitsgruppen, die erforderlich sind, um den Zugriff auf das Dateisystem zu ermöglichen, automatisch zu erstellen, erstellt der Launch Instance Wizard zwei Sicherheitsgruppen und fügt sie an. Eine Sicherheitsgruppe wird an die Instance angefügt, die andere an das Dateisystem. Weitere Informationen zu den Anforderungen an Sicherheitsgruppen finden Sie unter Zugriffskontrolle für das FSx-for-ONTAP-Dateisystem mit Amazon VPC und Zugriffskontrolle für das FSx-for-OpenZFS-Dateisystem mit Amazon VPC.

Wir fügen das Tag `Name=instance-sg-1` der Sicherheitsgruppe hinzu, die erstellt und an die Instance angehängt wird. Der Wert im Tag wird jedes Mal, wenn der Launch Instance Wizard eine Sicherheitsgruppe für Amazon-FSx-Dateisysteme erstellt, automatisch erhöht.

Die Sicherheitsgruppe umfasst die folgenden Ausgaberegeln, jedoch keine Regeln für eingehenden Datenverkehr.

Regeln für ausgehenden Datenverkehr

Protokolltyp	Port-Nummer	Bestimmungsort
UDP	111	*Dateisystem-Sicherheitsgruppe*
UDP	20 001 – 20 003	*Dateisystem-Sicherheitsgruppe*
UDP	4 049	*Dateisystem-Sicherheitsgruppe*
UDP	2049	*Dateisystem-Sicherheitsgruppe*
UDP	635	*Dateisystem-Sicherheitsgruppe*
UDP	4 045 - 4 046	*Dateisystem-Sicherheitsgruppe*
TCP	4 049	*Dateisystem-Sicherheitsgruppe*
TCP	635	*Dateisystem-Sicherheitsgruppe*

Protokolltyp	Port-Nummer	Bestimmungsort
TCP	2049	*Dateisystem-Sicherheitsgruppe*
TCP	111	*Dateisystem-Sicherheitsgruppe*
TCP	4 045 - 4 046	*Dateisystem-Sicherheitsgruppe*
TCP	20 001 – 20 003	*Dateisystem-Sicherheitsgruppe*
Alle	Alle	*Dateisystem-Sicherheitsgruppe*

Die Sicherheitsgruppe, die erstellt und an das Dateisystem angehängt wird, ist mit `Name=fsx-sg-`*1* gekennzeichnet. Der Wert im Tag wird jedes Mal, wenn der Launch Instance Wizard zum Starten von Instance eine Sicherheitsgruppe für Amazon-FSx-Dateisysteme erstellt, automatisch erhöht.

Die Sicherheitsgruppe umfasst die folgenden Regeln.

Regeln für eingehenden Datenverkehr

Protokolltyp	Port-Nummer	Quelle
UDP	2049	*Instance-Sicherheitsgruppe*
UDP	20 001 – 20 003	*Instance-Sicherheitsgruppe*
UDP	4 049	*Instance-Sicherheitsgruppe*
UDP	111	*Instance-Sicherheitsgruppe*
UDP	635	*Instance-Sicherheitsgruppe*
UDP	4 045 - 4 046	*Instance-Sicherheitsgruppe*
TCP	4 045 - 4 046	*Instance-Sicherheitsgruppe*
TCP	635	*Instance-Sicherheitsgruppe*
TCP	2049	*Instance-Sicherheitsgruppe*
TCP	4 049	*Instance-Sicherheitsgruppe*

Protokolltyp	Port-Nummer	Quelle
TCP	20 001 – 20 003	*Instance-Sicherheitsgruppe*
TCP	111	*Instance-Sicherheitsgruppe*

Regeln für ausgehenden Datenverkehr

Protokolltyp	Port-Nummer	Bestimmungsort
Alle	Alle	0.0.0.0/0

Benutzerdatenskript

Wenn Sie wählen, Benutzerdatenskripte automatisch anzufügen, fügt der Launch Instance Wizard der Instance die folgenden Benutzerdaten hinzu. Dieses Skript installiert die erforderlichen Pakete, stellt das Dateisystem bereit und aktualisiert Ihre Instance-Einstellungen so, dass das Dateisystem bei jedem Neustart der Instance automatisch neu bereitgestellt wird.

```
#cloud-config
package_update: true
package_upgrade: true
runcmd:
- yum install -y nfs-utils
- apt-get -y install nfs-common
- svm_id_1=svm_id
- file_system_id_1=file_system_id
- vol_path_1=/vol1
- fsx_mount_point_1=/mnt/fsx/fs1
- mkdir -p "${fsx_mount_point_1}"
- if [ -z "$svm_id_1" ]; then printf "\n${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev
 0 0\n" >> /etc/fstab; else printf "\n${svm_id_1}.${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0
 0\n" >> /etc/fstab; fi
- retryCnt=15; waitTime=30; while true; do mount -a -t nfs4 defaults; if [ $? = 0 ] ||
 [ $retryCnt -lt 1 ]; then echo File system mounted successfully; break; fi; echo File
 system not available, retrying to mount.; ((retryCnt--)); sleep $waitTime; done;
```

Bereitstellen eines Amazon-FSx-Dateisystems beim Start

Neues oder vorhandenes Amazon-FSx-Dateisystem beim Start bereitstellen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Instance starten, um den Launch Instance Wizard zu öffnen.
3. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) das zu verwendende AMI aus.
4. Wählen Sie im Bereich Instance type (Instance-Typ) den Instance-Typ aus.
5. Wählen Sie im Bereich Key pair (Schlüsselpaar) ein vorhandenes Schlüsselpaar aus oder erstellen Sie ein neues.
6. Gehen Sie im Bereich Network settings (Netzwerkeinstellungen) wie folgt vor:

   a. Wählen Sie Bearbeiten aus.

   b. Wenn Sie ein vorhandenes Dateisystem bereitstellen möchten, wählen Sie bei Subnet (Subnetz) das bevorzugte Subnetz des Dateisystems aus. Wir empfehlen, die Instance in derselben Availability Zone zu starten wie das bevorzugte Subnetz des Dateisystems, um die Leistung zu optimieren.

      Wenn Sie ein neues Dateisystem erstellen möchten, um eine Instance zu bereitzustellen, wählen Sie bei Subnet (Subnetz) das Subnetz aus, in dem die Instance gestartet werden soll.

      > **Important**
      >
      > Sie müssen ein Subnetz auswählen, um die Amazon-FSx-Funktionalität im neuen Launch Instance Wizard zu aktivieren. Wenn Sie kein Subnetz auswählen, können Sie kein vorhandenes Dateisystem bereitstellen oder ein neues erstellen.

7. Gehen Sie im Abschnitt Storage (Speicher) wie folgt vor:

   a. Konfigurieren Sie die Volumes nach Bedarf.

   b. Erweitern Sie den Bereich File systems (Dateisysteme) und wählen Sie FSx aus.

   c. Wählen Sie Add shared file system (Freigegebenes Dateisystem hinzufügen) aus.

d. Wählen Sie bei File system (Dateisystem) das Dateisystem aus, das bereitgestellt werden soll.

> **Note**
>
> Die Liste zeigt alle Amazon-FSx-für-NetApp-ONTAP- und Amazon-FSx-für-OpenZFS-Dateisysteme in Ihrem Konto in der ausgewählten Region.

e. Um die Sicherheitsgruppen, die zum Aktivieren des Zugriffs auf das Dateisystem erforderlich sind, automatisch zu erstellen und anzufügen, wählen Sie Automatically create and attach security groups (Sicherheitsgruppen automatisch erstellen und anfügen) aus. Wenn Sie es vorziehen, die Sicherheitsgruppen manuell zu erstellen, deaktivieren Sie das Kontrollkästchen. Weitere Informationen finden Sie unter Sicherheitsgruppen.

f. Um die Benutzerdatenskripte, die zum Bereitstellen des Dateisystems erforderlich sind, automatisch anzufügen, wählen Sie Automatically mount shared file system by attaching required user data script (Freigegebenes Dateisystem automatisch bereitstellen, indem erforderliches Benutzerdatenskript angefügt wird) aus. Wenn Sie es vorziehen, die Benutzerdatenskripts manuell zu erstellen, deaktivieren Sie das Kontrollkästchen. Weitere Informationen finden Sie unter Benutzerdatenskript.

8. Konfigurieren Sie im Bereich Advanced (Erweitert) die weiteren Instance-Einstellungen nach Bedarf.
9. Wählen Sie Launch (Starten) aus.

Amazon File Cache mit Amazon-EC2-Instances verwenden

Amazon-Datei-Cache ist ein vollständig verwalteter Hochgeschwindigkeits-Cache in AWS, der zur Verarbeitung von Dateidaten verwendet wird, unabhängig davon, wo die Daten gespeichert sind. Amazon-Datei-Cache dient als temporärer Hochleistungsspeicherort für Daten, die in On-Premises-Dateisystemen, AWS-Dateisystemen und Amazon Simple Storage Service (Amazon S3)-Buckets gespeichert sind. Sie können diese Fähigkeit nutzen, um verteilte Datensätze für dateibasierte Anwendungen auf AWS mit einer einheitlichen Ansicht und mit hohen Geschwindigkeiten – Latenzen von weniger als einer Millisekunde und hohem Durchsatz – verfügbar zu machen. Weitere Informationen finden Sie in Benutzerhandbuch zu Amazon File Cache.

Amazon-Datei-Cache funktioniert mit den gängigsten Linux-AMIs und ist mit x86-basierten Instance-Typen und Graviton-Instance-Typen kompatibel. Sie können von Ihren Amazon-EC2-Instances aus

mit dem Open-Source-Lustre-Client auf Ihren Cache zugreifen. Sie können Ihren Cache mounten und dann mithilfe von Linux-Standardbefehlen mit den Dateien und Verzeichnissen in Ihrem Cache arbeiten. Amazon-EC2-Instances können von anderen Availability Zones innerhalb derselben Virtual Private Cloud (VPC) aus auf Ihren Cache zugreifen, sofern Ihre Netzwerkkonfiguration den Zugriff über Subnetze innerhalb der VPC ermöglicht. Sie können auch einen Cache in einer freigegebenen VPC erstellen.

Informationen zu den ersten Schritten finden Sie unter Erste Schritte mit Amazon-Datei-Cache im Benutzerhandbuch für Amazon-Datei-Cache.

Verwalte deine EC2 Amazon-Ressourcen

Eine Ressource ist eine Entität, mit der Sie arbeiten können. Amazon EC2 erstellt Ressourcen, wenn Sie die Funktionen des Dienstes nutzen. Zu den EC2 Amazon-Ressourcen gehören beispielsweise Bilder, Instances, Flotten, Schlüsselpaare und Sicherheitsgruppen. Alle EC2 Amazon-Ressourcentypen enthalten Attribute, die die Ressourcen beschreiben. Zum Beispiel Namen, Beschreibungen, Ressourcen-Identifikatoren und Amazon-Ressourcennamens (ARN).

EC2 Amazon-Ressourcen sind spezifisch für die AWS Region oder Zone, in der sie sich befinden. Ein Amazon Machine Image (AMI) ist beispielsweise spezifisch für eine AWS Region, aber die Instance, die Sie von einem AMI aus starten, ist spezifisch für die Zone, in der Sie sie starten. Sie können eine EC2 Amazon-Ressource in einer Berechtigungsrichtlinie mithilfe ihres ARN angeben.

Ihr AWS-Konto hat Standardkontingente für Amazon EC2. Diese Kontingente definieren die maximale Anzahl von Ressourcen, die Sie erstellen können. Beispielsweise gibt es Kontingente für die maximale Anzahl von v CPUs in Ihren laufenden Instances. Wenn das Starten einer Instance oder das Starten einer gestoppten Instance dazu führen würde, dass Sie Ihr Kontingent überschreiten, schlägt der Vorgang fehl.

Sie können mithilfe AWS-Konto von Ressourcen IDs oder Tags nach bestimmten Ressourcen in Ihrer Region suchen. Verwenden Sie Amazon EC2 Global View, um nach bestimmten Ressourcen oder Ressourcentypen in mehreren Regionen zu suchen.

Inhalt

- Wählen Sie eine Region für Ihre EC2 Amazon-Ressourcen
- Finden Sie Ihre EC2 Amazon-Ressourcen
- Mit AWS Global View können Sie Ressourcen regionsübergreifend anzeigen
- Kennzeichnen Sie Ihre EC2 Amazon-Ressourcen
- EC2 Amazon-Servicekontingente

Wählen Sie eine Region für Ihre EC2 Amazon-Ressourcen

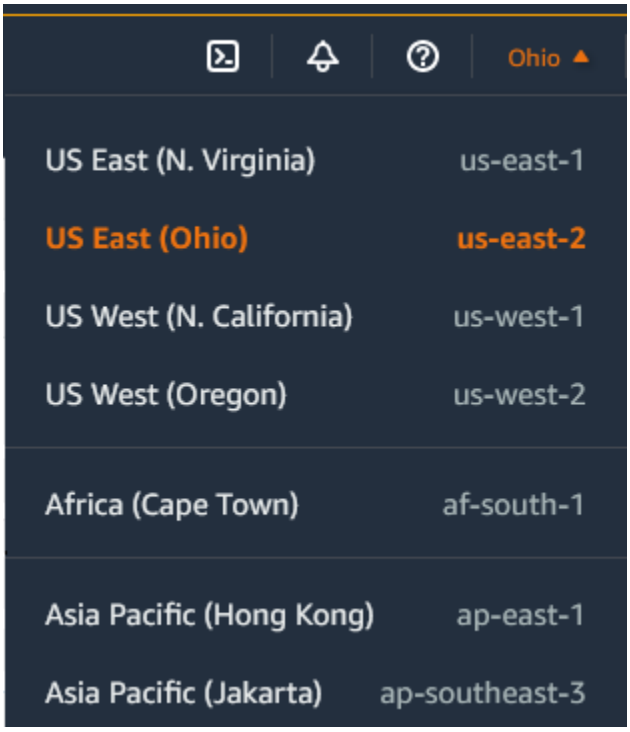
EC2 Amazon-Ressourcen sind spezifisch für die AWS Region oder Zone, in der sie sich befinden. Wenn Sie eine EC2 Amazon-Ressource erstellen, wählen Sie die Region für die Ressource aus.

Überlegungen

- Einige AWS Ressourcen sind möglicherweise nicht in allen Regionen verfügbar. Stellen Sie sicher, dass Sie alle AWS Ressourcen, die Sie in einer Region benötigen, erstellen können, bevor Sie mit der Erstellung von Ressourcen in einer Region beginnen.
- Manche Regionen sind standardmäßig deaktiviert. Sie müssen diese Regionen aktivieren, bevor Sie sie verwenden können. Weitere Informationen finden Sie unter AWS -Regionen.

Region für eine Ressource mit der Konsole auiswählen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie in der Navigationsleiste auf die Auswahl der Regions (Regionen) und wählen Sie dann die Region aus.



3. Die Regionsauswahl umfasst alle Ressourcen, die für die Verwendung in Ihrem AWS-Konto verfügbar sind. Wählen Sie den unterstrichenen Text am Ende der Liste aus, um die Regionen anzuzeigen, die für Ihr Konto nicht aktiviert sind.

Um eine Region für eine Ressource auszuwählen, verwenden Sie AWS CLI

Sie können die so konfigurieren AWS CLI , dass sie eine Standardregion verwendet. Wenn Sie im Befehl keine Region angeben, wird die Standardregion verwendet. Um eine andere Region für einen bestimmten Befehl zu verwenden, fügen Sie die folgende Option hinzu.

```
--region us-east-1
```

Um eine Region für eine Ressource auszuwählen, verwenden Sie die Tools für PowerShell

Sie können die Tools für Windows so konfigurieren PowerShell , dass sie eine Standardregion verwenden. Wenn Sie im Befehl keine Region angeben, wird die Standardregion verwendet. Um eine andere Region für einen bestimmten Befehl zu verwenden, fügen Sie den folgenden Parameter hinzu.

```
-Region us-east-1
```

Finden Sie Ihre EC2 Amazon-Ressourcen

Über die EC2 Amazon-Konsole können Sie eine Liste einiger Ressourcentypen abrufen. Sie erhalten eine Liste für jeden Ressourcentyp mit dem entsprechenden Befehl oder einer API-Aktion. Falls Sie über viele Ressourcen verfügen, können Sie die Ergebnisse so filtern, dass sie nur die Ressourcen enthalten oder ausschließen, die bestimmten Kriterien entsprechen.

Inhalt

- Auflisten und Filtern von Ressourcen über die Konsole
- Auflisten und Filtern mithilfe der Befehlszeile
- Ressourcen in allen Regionen mit Amazon EC2 Global View anzeigen

Auflisten und Filtern von Ressourcen über die Konsole

Inhalt

- Auflisten von Ressourcen mithilfe der Konsole
- Filtern von Ressourcen mithilfe der Konsole
  - Unterstützte Filter
- Filtersätze mit der Konsole speichern
  - Wichtige Features

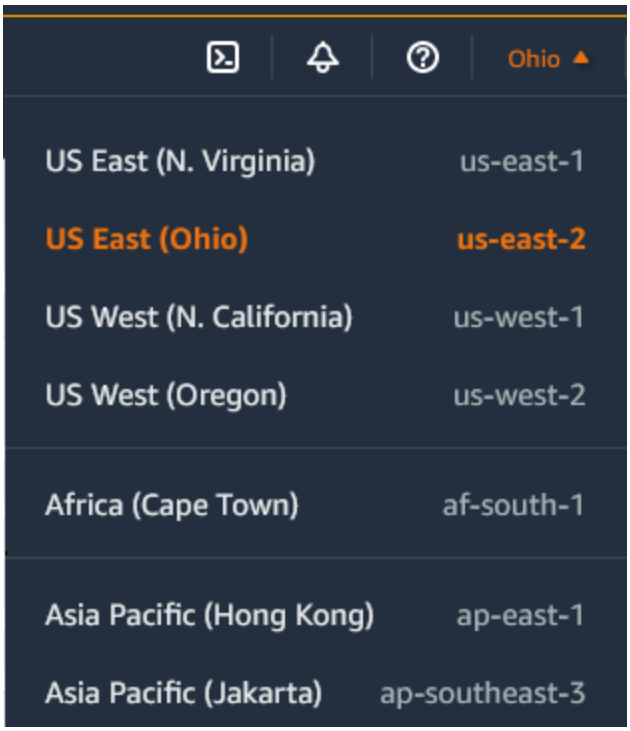
- Einen Filtersatz erstellen
- Einen Filtersatz ändern
- Einen Filtersatz löschen

Auflisten von Ressourcen mithilfe der Konsole

Sie können die gängigsten EC2 Amazon-Ressourcentypen mithilfe der Konsole anzeigen. Zum Anzeigen zusätzlicher Ressourcen verwenden Sie die Befehlszeilenschnittstelle oder die API-Aktionen.

Um EC2 Ressourcen mithilfe der Konsole aufzulisten

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. EC2 Amazon-Ressourcen sind spezifisch für eine AWS-Region. Klicken Sie in der Navigationsleiste auf die Auswahl der Regionen.

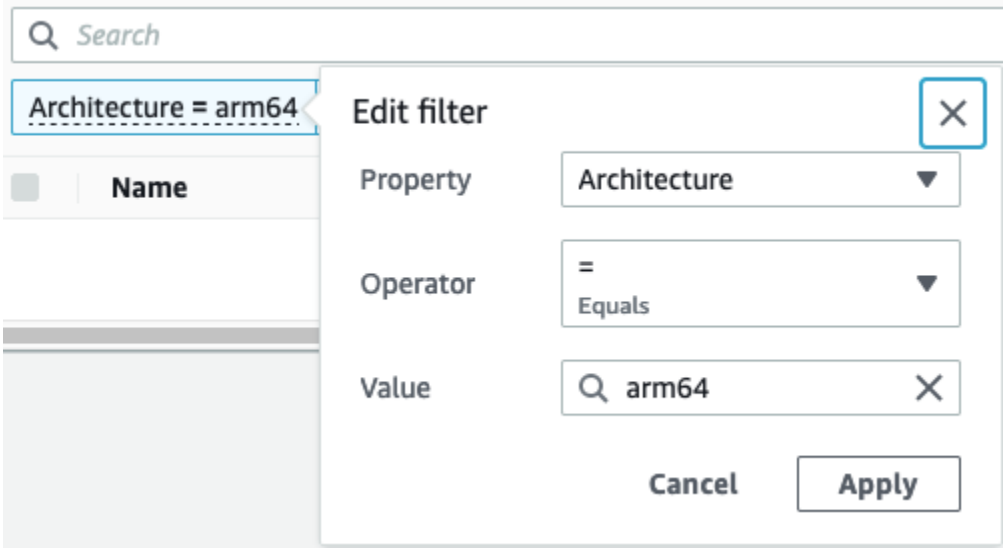


3. Wählen Sie im Navigationsbereich die Option aus, die dem Ressourcentyp entspricht. Wenn Sie beispielsweise all Ihre Instances auflisten möchten, wählen Sie Instances aus.

Filtern von Ressourcen mithilfe der Konsole

So filtern Sie eine Liste von Ressourcen

1. Wählen Sie im Navigationsbereich einen Ressourcentyp aus (z. B. Instances).
2. Wählen Sie das Suchfeld aus.
3. Wählen Sie den Filter aus der Liste aus.
4. Wählen Sie einen Operator aus, z. B.= (gleich). Einige Attribute haben mehr verfügbare Operatoren zur Auswahl. Beachten Sie, dass nicht alle Bildschirme die Auswahl eines Operators unterstützen.
5. Wählen Sie einen Filterwert aus.
6. Um einen ausgewählten Filter zu bearbeiten, wählen Sie das Filtertoken (blaues Feld) aus, nehmen Sie die erforderlichen Änderungen vor und wählen Sie dann Apply (Anwenden) aus. Beachten Sie, dass nicht alle Bildschirme ein Bearbeiten des ausgewählten Filters unterstützen.



7. Wenn Sie fertig sind, entfernen Sie den Filter.

Unterstützte Filter

Die EC2 Amazon-Konsole unterstützt zwei Arten der Filterung.

- Die API-Filterung erfolgt auf der Serverseite. Die Filterung wird auf den API-Aufruf angewendet, was die Anzahl der Ressourcen reduziert, die vom Server zurückgegeben werden. Sie ermöglicht eine schnelle Filterung über große Mengen von Ressourcen und kann die Datenübertragungszeit

und Kosten zwischen dem Server und dem Browser reduzieren. API-Filterung unterstützt die Operatoren = (gleich) und : (enthält) und berücksichtigt immer die Groß- und Kleinschreibung.

- Die Clientfilterung erfolgt auf der Clientseite. Sie ermöglicht Ihnen, nach Daten zu filtern, die bereits im Browser verfügbar sind (also Daten, die bereits von der API zurückgegeben wurden). Die Clientfilterung funktioniert gut in Verbindung mit einem API-Filter, um auf kleinere Datensätze im Browser zu filtern. Zusätzlich zu den Operatoren = (gleich) und : (enthält) kann die Client-Filterung auch Bereichsoperatoren unterstützen, wie >= (größer als oder gleich) und (inverse) Operatoren für die Negation, wie != (ist nicht gleich).

Die EC2 Amazon-Konsole unterstützt die folgenden Suchtypen:

Nach Schlüsselwort suchen

Die Suche nach Schlüsselwörtern ist eine Freitextsuche, mit der Sie nach einem Wert über alle Attribute oder Tags Ihrer Ressourcen hinweg suchen können, ohne ein zu suchendes Attribut oder Tag anzugeben.

> **Note**
>
> Bei allen Schlüsselwortsuchen wird die Clientfilterung verwendet.

Zur Suche nach Schlüsselwörtern geben oder fügen Sie in das Suchfeld ein, wonach Sie suchen, und drücken dann die Eingabetaste. Die Suche nach 123 findet als Übereinstimmung beispielsweise alle Instances mit 123 in einem ihrer Attribute, z. B. einer IP-Adresse, einer Instance-ID, einer VPC-ID oder einer AMI-ID oder in einem ihrer Tags, wie z. B. der Name. Wenn Ihre Freitextsuche unerwartete Übereinstimmungen zurückgibt, wenden Sie zusätzliche Filter an.

Suche nach Attribut

Wenn Sie nach einem Attribut suchen, können Sie ein bestimmtes Attribut über alle Ressourcen hinweg suchen.

> **Note**
>
> Attributsuchen verwenden je nach ausgewähltem Attribut entweder API-Filterung oder Clientfilterung. Bei einer Attributsuche werden die Attribute entsprechend gruppiert.

Sie können beispielsweise alle Instances nach dem Instance state (Instance-Status)-Attribut durchsuchen, um nur Instances mit dem Status `stopped` zurückzugeben. So gehen Sie vor:

1. Beginnen Sie im Suchfeld im Bildschirm Instances mit der Eingabe von `Instance state`. Wenn Sie die Zeichen eingeben, werden die beiden Filtertypen für den Instance-Status angezeigt: API-Filter und Client-Filter.
2. Um serverseitig zu suchen, wählen Sie unter API-Filter Instance-Status aus. Um clientseitig zu suchen, wählen Sie unter Client-Filter Instance-Status (Client) aus.

   Eine Liste möglicher Operatoren für das ausgewählte Attribut wird angezeigt.
3. Wählen Sie den Operator = (gleich) aus.

   Eine Liste möglicher Werte für das ausgewählte Attribut und den Operator wird angezeigt.
4. Wählen Sie in der Liste Gestoppt aus.

Suchen anhand eines Tags

Durch die Suche nach einem Tag können Sie die Ressourcen in der aktuell angezeigten Tabelle nach einem Tag-Schlüssel oder einem Tag-Wert filtern.

Tag-Suchen verwenden entweder die API-Filterung oder die Client-Filterung, abhängig von den Einstellungen im Fenster „Preferences“ (Voreinstellungen).

API-Filterung für Tags

1. Öffnen Sie die Registerkarte Preferences (Voreinstellungen).
2. Deaktivieren Sie das Kontrollkästchen Übereinstimmung mit regulären Ausdrücken verwenden. Wenn dieses Kontrollkästchen aktiviert ist, wird die Client-Filterung durchgeführt.
3. Wählen Sie das Kontrollkästchen Groß-/Kleinschreibung bei Abgleich beachten. Wenn dieses Kontrollkästchen deaktiviert ist, wird die Client-Filterung durchgeführt.
4. Wählen Sie Bestätigen aus.

Wenn Sie nach Tag suchen, können Sie die folgenden Werte verwenden:

- (empty) (leer) – sucht alle Ressourcen mit dem angegebenen Tag-Schlüssel, aber es darf keinen Tag-Wert geben.
- All values (Alle Werte) – sucht alle Ressourcen mit dem angegebenen Tag-Schlüssel und einem beliebigen Tag-Wert.

- Not tagged (Nicht markiert) – sucht nach Ressourcen, denen der angegebene Tag-Schlüssel nicht zugewiesen wurde.
- „The displayed value“ (Der angezeigte Wert) – sucht alle Ressourcen mit dem angegebenen Tag-Schlüssel und dem angegebenen Tag-Wert.

Sie können Ihre Suche mit den folgenden Methoden verbessern oder verfeinern:

Inverse search (Umgekehrte Suche)

Mit umgekehrten Suchvorgängen können Sie nach Ressourcen suchen, die nicht mit einem angegebenen Wert übereinstimmen. In den Instanzen und AMIsBildschirmen werden inverse Suchen durchgeführt, indem Sie die Option! auswählen = (Entspricht nicht) oder! : (Enthält nicht) Operator und dann Auswahl eines Werts. Auf anderen Bildschirmen wird die umgekehrte Suche durchgeführt, indem dem Suchbegriff das Ausrufezeichen (!) vorangestellt wird.

> **Note**
>
> Die umgekehrte Suche wird nur bei Schlüsselwortsuchen und Attributsuchen in Clientfiltern unterstützt. Sie wird bei Attributsuchen in API-Filtern nicht unterstützt.

Sie können beispielsweise alle Instances nach dem Instance state (Instance-Status)-Attribut durchsuchen, um alle Instances mit dem Status `terminated` auszuschließen. So gehen Sie vor:

1. Beginnen Sie im Suchfeld im Bildschirm Instances mit der Eingabe von `Instance state`. Wenn Sie die Zeichen eingeben, werden die beiden Filtertypen für den Instance-Status angezeigt: API-Filter und Client-Filter.
2. Wählen Sie unter Client filters (Client-Filter) die Option Instance state (client) (Instance-Status (Client)) aus. Die umgekehrte Suche wird nur für Client-Filter unterstützt.

   Eine Liste möglicher Operatoren für das ausgewählte Attribut wird angezeigt.
3. Klicken Sie auf != (ist nicht gleich), und wählen Sie dann terminated (beendet) aus.

Um Instances basierend auf einem Instance-Statusattribut zu filtern, können Sie auch die Suchsymbole (

) in der Spalte Instance-Status verwenden. Das Suchsymbol mit einem Pluszeichen (+) zeigt alle

Instances an, die mit diesem Attribut übereinstimmen . Das Suchsymbol mit einem Minuszeichen (-) schließt alle Instances aus, die mit diesem Attribut übereinstimmen.

Hier ist ein weiteres Beispiel für die Verwendung der umgekehrten Suche: Wenn Sie alle Instances auflisten möchten, denen die Sicherheitsgruppe `launch-wizard-1` nicht zugewiesen ist, suchen Sie unter Client filters (Client-Filter) nach dem Attribut Security group name (Sicherheitsgruppenname), wählen Sie != aus und geben Sie in der Suchleiste `launch-wizard-1` ein.

Partial search (Partielle Suche)

Bei partiellen Suchvorgängen können Sie nach partiellen Zeichenfolgenwerten suchen. Um eine Teilsuche durchzuführen, geben Sie nur einen Teil des Schlüsselwortes ein, nach dem Sie suchen möchten. Auf den Instanzen und AMIsBildschirmen können Teilsuchen nur mit dem Operator: (Enthält) durchgeführt werden. Auf anderen Bildschirmen können Sie das Client-Filterattribut auswählen und sofort nur den Teil des Suchbegriffs eingeben, nach dem Sie suchen möchten. Um beispielsweise auf dem Bildschirm Instance type (Instance-Typ) nach allen `t2.micro`-, `t2.small`- und `t2.medium`-Instances zu suchen, suchen Sie nach dem Attribut Instance type (Instance-Typ) und geben Sie als Schlüsselwort `t2` ein.

Suche nach regulären Ausdrücken

Um Suchen mit regulären Ausdrücken zu verwenden, müssen Sie in den Einstellungen das Kontrollkästchen Übereinstimmung mit regulären Ausdrücken verwenden im Fenster Voreinstellungen aktivieren.

Reguläre Ausdrücke sind hilfreich, wenn Sie die Werte in einem Feld an ein spezifisches Muster angleichen müssen. Um beispielsweise nach einem Wert zu suchen, der mit `s` beginnt, suchen Sie nach `^s`. Um nach einem Wert zu suchen, der mit `xyz` endet, suchen Sie nach `xyz$`. Um nach einem Wert zu suchen, der mit einer Zahl beginnt, auf die ein oder mehrere Zeichen folgen, suchen Sie nach `[0-9]+.*`.

> **Note**
>
> Die Suche nach regulären Ausdrücken wird nur bei Schlüsselwortsuchen und Attributsuchen in Clientfiltern unterstützt. Sie wird bei Attributsuchen in API-Filtern nicht unterstützt.

Suche mit Unterscheidung von Groß-/Kleinschreibung

Um Suchvorgänge mit Beachtung der Groß-/Kleinschreibung zu verwenden, müssen Sie das Kontrollkästchen Abgleich mit Unterscheidung von Groß-/Kleinschreibung im Fenster Voreinstellungen auswählen. Die Einstellung für die Groß-/Kleinschreibung gilt nur für Client- und Tag-Filter.

> **Note**
>
> Bei API-Filtern wird immer zwischen Groß-/Kleinschreibung unterschieden.

Suche nach Platzhaltern

Verwenden Sie den Platzhalter `*` als Entsprechung für null oder ein Zeichen. Verwenden Sie den Platzhalter `?` als Entsprechung für null oder ein Zeichen. Beispiel: Wenn Sie einen Datensatz mit den Werten `prod`, `prods` und `production` haben, gleicht eine Suche nach `prod*` alle Werte ab, während `prod?` nur `prod` und `prods` abgleicht. Um die Literalwerte zu verwenden, versehen Sie sie als Escape-Zeichen mit einem umgekehrten Schrägstrich (\). Beispielsweise würde „`prod \*`“ mit `prod*` übereinstimmen.

> **Note**
>
> Die Platzhaltersuche wird nur bei Attribut- und Tag-Suchen in API-Filtern unterstützt. Sie wird nicht bei Schlüsselwortsuchen und bei Attribut- und Tag-Suchen in Client-Filtern unterstützt.

Kombinieren von Suchen

Im Allgemeinen werden mehrere Filter mit demselben Attribut automatisch mit verbunde `OR`. Beispielsweise gibt die Suche nach `Instance State : Running` und `Instance State : Stopped` alle Instances zurück, die entweder ausgeführt werden ODER gestoppt sind. Um die Suche mit `AND` zu verbinden, suchen Sie über verschiedene Attribute hinweg. Die Suche nach `Instance State : Running` und `Instance Type : c4.large` gibt z. B. nur Instances zurück, die vom Typ `c4.large` sind UND sich im Ausführungszustand befinden.

Filtersätze mit der Konsole speichern

Ein gespeicherter Filtersatz ist eine benutzerdefinierte Gruppe von Filtern, die Sie erstellen und wiederverwenden können, um Ihre EC2 Amazon-Ressourcen effizient anzuzeigen. Dieses Feature hilft Ihnen dabei, Ihren Arbeitsablauf zu optimieren, indem es einen schnellen Zugriff auf bestimmte Ressourcenansichten ermöglicht.

Gespeicherte Filtersätze werden nur in der EC2 Amazon-Konsole unterstützt und sind derzeit nur für die Volumenseite verfügbar.

Wichtige Features

- Anpassung: Erstellen Sie Filtersätze, die auf Ihre Bedürfnisse zugeschnitten sind. Sie können beispielsweise ein Filterset erstellen, um nur Ihre gp3-Volumes anzuzeigen, die nach einem bestimmten Datum erstellt wurden.
- Standardfilter: Legen Sie einen Standardfiltersatz für eine Seite fest. Die Standardfilter werden automatisch angewendet, wenn Sie zu der Seite navigieren. Wenn kein Standard festgelegt ist, werden keine Filter angewendet.
- Einfache Anwendung: Wählen Sie einen gespeicherten Filtersatz aus, um ihn sofort anzuwenden. Amazon zeigt EC2 dann die relevanten Ressourcen an, wobei die aktiven Filter durch blaue Token gekennzeichnet sind.
- Flexibilität: Erstellen, ändern und löschen Sie Filtersätze nach Bedarf.

Einen Filtersatz erstellen

Einen neuen Filtersatz erstellen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Volumes aus.

> **Note**
>
> Gespeicherte Filtersätze sind derzeit nur für Volumes verfügbar.

3. Wählen Sie im Suchfeld Filter für Ihren Filtersatz aus.
4. Klicken Sie auf den Pfeil neben der Schaltfläche Filter löschen und wählen Sie Neuen Filtersatz speichern.

5. Gehen Sie im Fenster Filtersatz speichern wie folgt vor:

   a. Geben Sie für Name einen Namen für den Filtersatz ein.

   b. (Optional) Geben Sie in das Feld Filtersatzbeschreibung eine Beschreibung für den Filtersatz ein.

   c. (Optional) Um den Filtersatz als Standardfilter festzulegen, aktivieren Sie das Kontrollkästchen Als Standard festlegen.

   > **Note**
   >
   > Der Standardfilter wird jedes Mal automatisch angewendet, wenn Sie die Konsolenseite öffnen.

   d. Wählen Sie Speichern.

Einen Filtersatz ändern

Einen Filtersatz ändern

1. Wählen Sie in der Liste Gespeicherte Filtersätze den Filter aus, den Sie ändern möchten.
2. Um einen Filter hinzuzufügen, wählen Sie im Suchfeld einen Filter aus, den Sie Ihrem Filtersatz hinzufügen möchten. Um einen Filter in der Gruppe zu löschen, wählen Sie das X auf dem Filter-Token.
3. Klicken Sie auf den Pfeil neben der Schaltfläche Filter löschen und wählen Sie Filtersatz ändern aus.
4. Gehen Sie im Fenster Filtersatz ändern wie folgt vor:

   a. (Optional) Um den Filtersatz als Standardfilter festzulegen, aktivieren Sie das Kontrollkästchen Als Standard festlegen.

   > **Note**
   >
   > Der Standardfilter wird jedes Mal automatisch angewendet, wenn Sie die Konsolenseite öffnen.

   b. Wählen Sie Ändern aus.

Einen Filtersatz löschen

Löschen eines Filtersatzes

1. Wählen Sie in der Liste Gespeicherte Filtersätze den Filter aus, den Sie löschen möchten.
2. Klicken Sie auf den Pfeil neben der Schaltfläche Filter löschen und wählen Sie Filtersatz löschen aus.
3. Überprüfen Sie im Fenster Filtersatz löschen den Filter, um sicherzustellen, dass es sich um den Filter handelt, den Sie löschen möchten, und wählen Sie dann Löschen aus.

Auflisten und Filtern mithilfe der Befehlszeile

Jeder Ressourcentyp hat eine entsprechende API-Aktion, die Sie verwenden können, um die Ressourcen dieses Typs zu beschreiben, aufzulisten oder abzurufen. Die resultierenden Listen von Ressourcen können lang sein, sodass es schneller und hilfreicher sein kann, die Ergebnisse so zu filtern, dass nur die Ressourcen berücksichtigt werden, die bestimmten Kriterien entsprechen.

Überlegungen zum Filtern

- Sie können bis zu 50 Filter und bis zu 200 Werte pro Filter in einer einzigen Anforderung angeben.
- Filterzeichenfolgen können bis zu 255 Zeichen lang sein.
- Sie können Platzhalter in den Filterwerten verwenden. Ein Sternchen (*) steht für kein Zeichen oder eine beliebige Kombination von mehreren Zeichen, und ein Fragezeichen (?) entspricht Null oder einem Zeichen.
- Bei Filterwerten muss die Groß- und Kleinschreibung beachtet werden.
- Ihre Suche kann die Literalwerte der Platzhalterzeichen enthalten. Sie müssen dafür nur einen Backslash vor dem Zeichen eingeben. Beispiel: Mit dem Wert `\*amazon\?\\` wird nach der Literalzeichenfolge `*amazon?\` gesucht.
- Sie können keinen Filterwert von null angeben. Verwenden Sie stattdessen clientseitige Filterung. Der folgende Befehl verwendet beispielsweise die --query Option und gibt die IDs Instances zurück, die ohne ein key pair gestartet wurden.

```
aws ec2 describe-instances \
    --query 'Reservations[*].Instances[?!not_null(KeyName)].InstanceId' \
    --output text
```

AWS CLI

Example Beispiel: Angeben eines einzelnen Filters

Sie können Ihre EC2 Amazon-Instances auflisten mit describe-instances. Ohne Filter enthält die Antwort Informationen für alle Ihre Ressourcen. Sie können die folgende Option verwenden, um nur die laufenden Instances in Ihre Ausgabe aufzunehmen.

```
--filters Name=instance-state-name,Values=running
```

Um nur die Instance IDs für Ihre laufenden Instances aufzulisten, fügen Sie die `--query` Option wie folgt hinzu.

```
--query "Reservations[*].Instances[*].InstanceId"
```

Example Beispiel: Angeben mehrerer Filter oder Filterwerte

Wenn Sie mehrere Filter oder mehrere Filterwerte angeben, muss die Ressource mit allen Filtern übereinstimmen, um in die Ausgabe aufgenommen zu werden.

Mit der folgenden Option können Sie alle Instances auflisten, deren Typ entweder `m5.large` oder `m5d.large` ist.

```
--filters Name=instance-type,Values=m5.large,m5d.large
```

Sie können die folgende Option verwenden, um alle angehaltenen Instances aufzulisten, deren Typ `t2.micro` ist.

```
--filters Name=instance-state-name,Values=stopped Name=instance-type,Values=t2.micro
```

Example Beispiel: Verwenden von Platzhaltern in einem Filterwert

Sie können die folgende Option mit describe-snapshots verwenden, um nur die Snapshots zurückzugeben, deren Beschreibung „database“ lautet.

```
--filters Name=description,Values=database
```

Der Platzhalter „*“ entspricht null oder mehr Zeichen. Sie können die folgende Option verwenden, um nur die Snapshots zurückzugeben, deren Beschreibung das Wort database enthält.

```
--filters Name=description,Values=*database*
```

Der Platzhalter „?“ entspricht genau 1 Zeichen. Sie können die folgende Option verwenden, um nur die Snapshots zurückzugeben, deren Beschreibung „database“ oder „database“ gefolgt von einem Zeichen ist.

```
--filters Name=description,Values=database?
```

Sie können die folgende Option verwenden, um nur die Snapshots zurückzugeben, deren Beschreibung „database“ gefolgt von bis zu vier Zeichen ist. Beschreibungen mit „database“, gefolgt von fünf oder mehr Zeichen, werden ausgeschlossen.

```
--filters Name=description,Values=database????
```

Example Beispiel: Filtern basierend auf Datum

Mit der AWS CLI können Sie Ergebnisse mithilfe von Ausdrücken filtern. JMESPath Mit dem folgenden describe-snapshotsBefehl werden beispielsweise alle Schnappschüsse angezeigt, die IDs an dem angegebenen Datum AWS-Konto vor dem angegebenen Datum erstellt wurden. Wenn Sie den Eigentümer nicht angeben, enthalten die Ergebnisse alle öffentlichen Snapshots.

```
aws ec2 describe-snapshots \
    --filters Name=owner-id,Values=123456789012 \
    --query "Snapshots[?(StartTime<='2024-03-31')].[SnapshotId]" \
    --output text
```

Im folgenden Beispiel werden alle Snapshots angezeigt, die im angegebenen Zeitraum erstellt wurden. IDs

```
aws ec2 describe-snapshots \
    --filters Name=owner-id,Values=123456789012 \
    --query "Snapshots[?(StartTime>='2024-01-01') && (StartTime<='2024-12-31')].
[SnapshotId]" \
    --output text
```

Beispiel: Filtern basierend auf Tags

Beispiele zum Filtern einer Liste von Ressourcen nach ihren Tags (Markierungen) finden Sie unter EC2 Amazon-Ressourcen nach Tag filtern.

PowerShell

Example Beispiel: Angeben eines einzelnen Filters

Sie können Ihre EC2 Amazon-Instances auflisten mit Get-EC2Instance. Ohne Filter enthält die Antwort Informationen für alle Ihre Ressourcen. Sie können den folgenden Parameter verwenden, um nur die laufenden Instances in Ihre Ausgabe aufzunehmen.

```
-Filter @{Name="instance-state-name"; Values="running"}
```

Das folgende Beispiel listet nur die Instance IDs für Ihre laufenden Instances auf.

```
(Get-EC2Instance -Filter @{Name="instance-state-name"; Values="stopped"}).Instances
 | Select InstanceId
```

Example Beispiel: Angeben mehrerer Filter oder Filterwerte

Wenn Sie mehrere Filter oder mehrere Filterwerte angeben, muss die Ressource mit allen Filtern übereinstimmen, um in die Ergebnisse aufgenommen zu werden.

Mit der folgenden Option können Sie alle Instances auflisten, deren Typ entweder `m5.large` oder `m5d.large` ist.

```
-Filter @{Name="instance-type"; Values="m5.large", "m5d.large"}
```

Sie können die folgende Option verwenden, um alle angehaltenen Instances aufzulisten, deren Typ `t2.micro` ist.

```
-Filter @{Name="instance-state-name"; Values="stopped"}, @{Name="instance-type";
 Values="t2.micro"}
```

Ressourcen in allen Regionen mit Amazon EC2 Global View anzeigen

Mit Amazon EC2 Global View können Sie Amazon- EC2 und Amazon VPC-Ressourcen in einer einzelnen AWS Region oder in mehreren Regionen gleichzeitig in einer einzigen Konsole anzeigen und suchen. Weitere Informationen finden Sie unter Mit AWS Global View können Sie Ressourcen regionsübergreifend anzeigen.

Mit AWS Global View können Sie Ressourcen regionsübergreifend anzeigen

AWS Mit Global View können Sie einige Ihrer Amazon EC2 - und Amazon VPC-Ressourcen in einer einzigen AWS Region oder in mehreren Regionen in einer einzigen Konsole anzeigen. AWS Global View bietet auch globale Suchfunktionen, mit denen Sie in mehreren Regionen gleichzeitig nach bestimmten Ressourcen oder bestimmten Ressourcentypen suchen können.

AWS In der globalen Ansicht können Sie Ressourcen in keiner Weise ändern.

Unterstützte Ressourcen

Mithilfe der AWS globalen Ansicht können Sie eine globale Zusammenfassung der folgenden Ressourcen in allen Regionen anzeigen, für die Ihre aktiviert AWS-Konto ist.

- Auto-Scaling-Gruppen
- Kapazitätsreservierungen und Kapazitätsblöcke
- DHCP-Optionsliste
- Internet-Gateways nur für ausgehenden Datenverkehr
- Elastisch IPs
- Endpunkt-Services
- Instances
- Internet-Gateways
- Verwaltete Präfixlisten
- NAT gateways (NAT-Gateways)
- Netzwerk ACLs
- Netzwerkschnittstellen
- Routing-Tabellen
- Sicherheitsgruppen
- Subnets
- Datenträger
- VPCs

- VPC-Endpunkte
- VPC-Peering-Verbindungen

Erforderliche Berechtigungen

Ein Benutzer muss über die folgenden Berechtigungen verfügen, um AWS Global View verwenden zu können.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
    "autoscaling:DescribeAutoScalingGroups",
    "ec2:DescribeRegions",
    "ec2:DescribeCapacityReservations",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeEgressOnlyInternetGateways",
    "ec2:DescribeAddresses",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribePrefixLists",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections"
  ],
  "Resource": "*"
  }]
}
```

Um AWS Global View zu verwenden

Melden Sie sich bei der Konsole von AWS Global View an.

> **Important**
>
> Sie können in Firefox kein privates Fenster verwenden, um auf AWS Global View zuzugreifen.

Die Konsole enthält die folgenden Elemente:

- Region Explorer – Diese Seite enthält die folgenden Abschnitte:
  - Zusammenfassung – Bietet einen allgemeinen Überblick über Ihre Ressourcen in allen Regionen.

    Expand Alle Ressourcenübersicht anzeigen gibt die Anzahl der Regionen an, für die Ihr aktiviert AWS-Konto ist. Die verbleibenden Felder geben die Anzahl der Ressourcen an, die Sie derzeit in diesen Regionen haben. Wählen Sie einen der Links, um die Ressourcen dieses Typs in allen Regionen anzuzeigen. Wenn beispielsweise der Link unter dem Label Instances 29 in 10 Regionen ist, gibt es an, dass Sie derzeit 29 Instances über 10Regionen haben. Wählen Sie den Link, um eine Liste aller 29 Instances anzuzeigen.
  - Regions-Explorer — Listet alle auf AWS-Regionen (einschließlich derjenigen, für die Ihr Konto nicht aktiviert ist) und bietet Gesamtwerte für jeden Ressourcentyp und jede Region.

    Wählen Sie eine Regionsbezeichnung, um alle Ressourcen aller Arten für diese bestimmte Region anzuzeigen. Wählen Sie beispielsweise Africa (Cape Town) af-south-1, um alle Subnetze, Instances VPCs, Sicherheitsgruppen, Volumes und Auto Scaling Scaling-Gruppen in dieser Region anzuzeigen. Alternativ können Sie eine Region auswählen und Ressourcen für ausgewählte Region anzeigen auswählen.

    Wählen Sie den Wert für einen bestimmten Ressourcentyp in einer bestimmten Region aus, um nur Ressourcen dieses Typs in dieser Region anzuzeigen. Wählen Sie z. B. den Wert für Instances für Afrika (Kapstadt) af-south-1, um nur die Instances in dieser Region anzuzeigen.
- Globale Suche – Auf dieser Seite können Sie nach bestimmten Ressourcen oder bestimmten Ressourcentypen in einer einzelnen Region oder in mehreren Regionen suchen. Außerdem können Sie Details zu einer bestimmten Ressource anzeigen.

Um nach Ressourcen zu suchen, geben Sie die Suchkriterien in das Feld vor dem Raster ein. Sie können nach Region, Ressourcentyp und nach den Tags suchen, die Ressourcen zugewiesen sind.

Um die Details für eine bestimmte Ressource anzuzeigen, wählen Sie sie im Raster aus. Sie können auch die Ressourcen-ID einer Ressource auswählen, um sie in ihrer jeweiligen Konsole zu öffnen. Wählen Sie beispielsweise eine Instance-ID, um die Instance in der EC2 Amazon-Konsole zu öffnen, oder wählen Sie eine Subnetz-ID, um das Subnetz in der Amazon VPC-Konsole zu öffnen.

- Regionen und Zonen – Auf dieser Seite können Sie alle verfügbaren Regionen, Availability Zones, Local Zones und Wavelength Zones anzeigen und verwalten.

  Auf der Registerkarte Regionen können Sie alle Regionen einsehen. AWS In der Spalte Status werden die Regionen angezeigt, die für Ihr AWS-Konto aktiviert sind. Auf dieser Seite können Sie eine Region auswählen, um:

  - Details der Region anzuzeigen, z. B. den Regioncode, die Geografie und die Nummer der einzelnen Zonentypen.

    Sie können auch die Liste der Availability Zones, Local Zones und Wavelength Zones sowie die Liste Ihrer Ressourcen in der Region anzeigen.
  - Die Region aktivieren oder deaktivieren

  Auf jeder Zonen-Registerkarte können Sie die Liste des jeweiligen Zonentyps einsehen. Auf der Registerkarte Local Zones können Sie sich für eine Local Zone anmelden.

> **Tip**
>
> Wenn Sie nur bestimmte Regionen oder Ressourcentypen verwenden, können Sie die AWS globale Ansicht so anpassen, dass nur diese Regionen und Ressourcentypen angezeigt werden. Um die angezeigten Regionen und Ressourcentypen anzupassen, wählen Sie im Navigationsbereich Einstellungen und dann auf den Registerkarten Ressourcen und Regionen die Regionen und Ressourcentypen aus, die nicht in der AWS globalen Ansicht angezeigt werden sollen.

Kennzeichnen Sie Ihre EC2 Amazon-Ressourcen

Um Ihnen bei der Verwaltung Ihrer Instances, Bilder und anderer EC2 Amazon-Ressourcen zu helfen, können Sie jeder Ressource Ihre eigenen Metadaten in Form von Tags zuweisen. Mithilfe von Tags können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Dies ist nützlich, wenn Sie viele Ressourcen desselben Typs haben — In diesem Fall können Sie schnell bestimmte Ressourcen basierend auf den zugewiesenen Tags (Markierungen) bestimmen. In diesem Thema werden Tags (Markierungen) und deren Erstellung beschrieben.

> **Warning**
>
> Tag (Markierung)-Schlüssel und ihre Werte werden von vielen verschiedenen API-Aufrufen zurückgegeben. Wenn Sie den Zugriff auf verweigern, wird `DescribeTags` nicht automatisch der Zugriff auf Tags verweigert, die von anderen zurückgegeben wurden. APIs Als bewährte Vorgehensweise empfehlen wir Ihnen, keine sensiblen Daten in Ihre Tags (Markierungen) aufzunehmen.

Inhalt

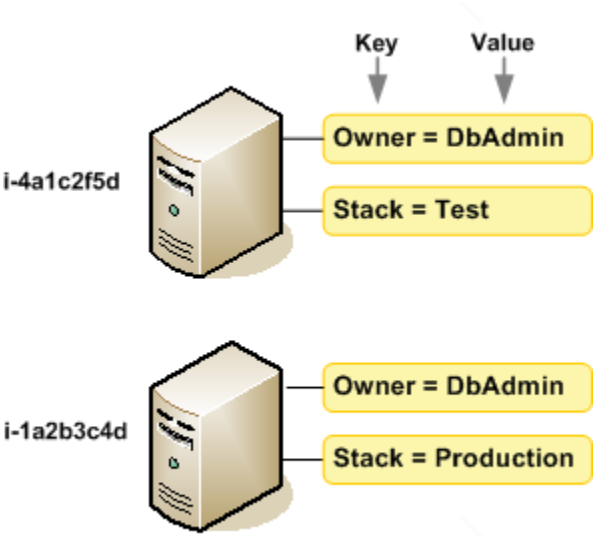
- Grundlagen zu Tags (Markierungen)
- Markieren Ihrer -Ressourcen mit Tags (Markierungen)
- Tag (Markierung)-Einschränkungen
- Tags (Markierungen) und Access Management
- Markieren von Ressourcen für die Fakturierung
- Erteilen Sie die Erlaubnis, EC2 Amazon-Ressourcen während der Erstellung zu taggen
- Hinzufügen und Entfernen von Tags für EC2 Amazon-Ressourcen
- EC2 Amazon-Ressourcen nach Tag filtern
- Zeigen Sie Tags für Ihre EC2 Instances mithilfe von Instanz-Metadaten an

Grundlagen zu Tags (Markierungen)

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Jeder Tag (Markierung) besteht aus einem Schlüssel und einem optionalen Wert, beides können Sie bestimmen.

Mithilfe von Tags können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Sie könnten beispielsweise eine Reihe von Tags für die EC2 Amazon-Instances Ihres Kontos definieren, mit deren Hilfe Sie den Besitzer und die Stack-Ebene jeder Instance verfolgen können.

Das folgende Diagramm veranschaulicht, wie Markieren funktioniert. In diesem Beispiel wurden jeder Instance zwei Tags (Markierungen) zugewiesen: ein Tag (Markierung) mit dem Schlüssel `Owner` und ein Tag (Markierung) mit dem Schlüssel `Stack`. Jeder Tag (Markierung) verfügt außerdem über einen zugewiesenen Wert.



Wir empfehlen die Verwendung von Tag (Markierung)-Schlüsseln, die die Anforderungen der jeweiligen Ressourcentypen erfüllen. Die Verwendung einheitlicher Tag-Schlüssel vereinfacht das Verwalten der -Ressourcen. Sie können die Ressourcen auf Grundlage der hinzugefügten Tags (Markierungen) filtern und danach suchen. Weitere Informationen zur Implementierung einer effektiven Strategie zur Kennzeichnung von Ressourcen finden Sie im Whitepaper Best Practices AWS für Tagging.

Tags haben für Amazon keine semantische Bedeutung EC2 und werden ausschließlich als Zeichenfolge interpretiert. Außerdem werden Tags (Markierungen) nicht automatisch Ihren Ressourcen zugewiesen. Sie können Tag (Markierung)-Schlüssel und -Werte bearbeiten und Tags (Markierungen) jederzeit von einer Ressource entfernen. Sie können den Wert eines Tags (Markierung) zwar auf eine leere Zeichenfolge, jedoch nicht null festlegen. Wenn Sie ein Tag (Markierung) mit demselben Schlüssel wie ein vorhandener Tag (Markierung) für die Ressource hinzufügen, wird der alte Wert mit dem neuen überschrieben. Wenn Sie eine Ressource löschen, werden alle Tags (Markierungen) der Ressource ebenfalls gelöscht.

> **Note**
>
> Nachdem Sie eine Ressource gelöscht haben, bleiben ihre Tags möglicherweise für einen kurzen Zeitraum in der Konsolen-, API- und CLI-Ausgabe sichtbar. Diese Tags werden schrittweise von der Ressource getrennt und dauerhaft gelöscht.

Markieren Ihrer -Ressourcen mit Tags (Markierungen)

Wenn Sie die EC2 Amazon-Konsole verwenden, können Sie Tags auf Ressourcen anwenden, indem Sie die Registerkarte Tags auf dem entsprechenden Ressourcenbildschirm verwenden, oder Sie können den Tags-Editor in der AWS -Ressourcengruppen Konsole verwenden. Auf bestimmten Ressourcenbildschirmen können Sie Tags (Markierungen) beim Erstellen einer Ressource angeben, z. B. ein Tag (Markierung) mit einem Schlüssel von `Name` und einem benutzerdefinierten Wert. In den meisten Fällen wendet die Konsole Tags (Markierungen) direkt nach dem Erstellen der Ressource an und nicht während des Erstellens. Die Konsole organisiert Ressourcen möglicherweise nach dem `Name` Tag, aber dieses Tag hat für den EC2 Amazon-Service keine semantische Bedeutung.

Wenn Sie die EC2 Amazon-API AWS CLI, das oder ein AWS SDK verwenden, können Sie die `CreateTags` EC2 API-Aktion verwenden, um Tags auf vorhandene Ressourcen anzuwenden. Zudem können Sie mit einigen Aktionen zur Ressourcenerstellung Tags beim Erstellen einer Ressource angeben. Wenn Tags (Markierungen) nicht während der Ressourcenerstellung angewendet werden können, wird die Ressourcenerstellung rückgängig gemacht. Auf diese Weise werden Ressourcen entweder mit Tags (Markierungen) oder überhaupt nicht erstellt und keine Ressourcen verbleiben ohne Tags (Markierungen). Indem Sie Ressourcen zum Erstellungszeitpunkt markieren, müssen Sie anschließend keine benutzerdefinierten Skripts ausführen. Weitere Informationen darüber, wie Sie Benutzern ermöglichen, Ressourcen bei der Erstellung zu markieren, finden Sie unter Erteilen Sie die Erlaubnis, EC2 Amazon-Ressourcen während der Erstellung zu taggen.

Sie können in Ihren IAM-Richtlinien tagbasierte Berechtigungen auf Ressourcenebene auf die EC2 Amazon-API-Aktionen anwenden, die das Tagging bei der Erstellung unterstützen, um eine detaillierte Kontrolle über die Benutzer und Gruppen zu implementieren, die Ressourcen bei der Erstellung taggen können. Ihre Ressourcen sind ab Erstellung ordnungsgemäß geschützt. Tags (Markierungen) werden direkt auf Ihre Ressourcen angewendet. Daher treten alle Tag (Markierung)-basierten Berechtigungen auf Ressourcenebene, die die Verwendung von Ressourcen steuern, direkt in Kraft. Ihre Ressourcen können nachverfolgt und genauer erfasst werden. Sie können das

Markieren neuer Ressourcen gewährleisten und steuern, welche Tag (Markierung)-Schlüssel und Werte für Ihre Ressourcen festgelegt sind.

Sie können in Ihren IAM-Richtlinien auch Berechtigungen auf Ressourcenebene auf die `CreateTags` und die `DeleteTags` EC2 Amazon-API-Aktionen anwenden, um zu kontrollieren, welche Tag-Schlüssel und -Werte für Ihre vorhandenen Ressourcen festgelegt werden. Weitere Informationen finden Sie unter Beispiel: Markieren von Ressourcen.

Weitere Informationen zum Markieren von Ressourcen für die Fakturierung finden Sie unter Verwendung von Tags (Markierungen) zur Kostenzuordnung im Benutzerhandbuch für AWS Billing .

Tag (Markierung)-Einschränkungen

Die folgenden grundlegenden Einschränkungen gelten für Tags (Markierungen):

- Maximale Anzahl von Tags (Markierungen) pro Ressource: 50
- Jeder Tag (Markierung) muss für jede Ressource eindeutig sein. Jeder Tag (Markierung) kann nur einen Wert haben.
- Maximale Schlüssellänge: 128 Unicode-Zeichen in UTF-8
- Maximale Wertlänge — 256 Unicode-Zeichen in UTF-8
- Zulässige Zeichen
  - Obwohl jedes Zeichen in seinen Tags EC2 zulässig ist, sind andere AWS Dienste restriktiver. In allen AWS Diensten sind folgende Zeichen zulässig: Buchstaben (`a-z`,`A-Z`), Zahlen (`0-9`) und Leerzeichen, die in UTF-8 dargestellt werden können, sowie die folgenden Zeichen:. `+ - = . _ : / @`
  - Wenn Sie Instance-Tags in Instance-Metadaten aktivieren, kann das Instance-Tag keys nur Buchstaben (`a-z`,`A-Z`), Zahlen (`0-9`) und die folgenden Zeichen verwenden: `+ - = . , _ : @`. Instance-Tag Schlüssel dürfen keine Leerzeichen oder `/` enthalten und dürfen nur `.` (ein Komma), `..` (zwei Kommas) oder `_index` enthalten. Weitere Informationen finden Sie unter Zeigen Sie Tags für Ihre EC2 Instances mithilfe von Instanz-Metadaten an.
- Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden.
- Das `aws:` Präfix ist für die Verwendung reserviert. AWS Wenn der Tag (Markierung) über einen Tag (Markierung)-Schlüssel mit diesem Präfix verfügt, können Sie den Schlüssel oder Wert des Tags (Markierung) nicht bearbeiten oder löschen. Tags (Markierungen) mit dem Präfix `aws:` werden nicht als Ihre Tags (Markierungen) pro Ressourcenlimit angerechnet.

Sie können Ressourcen nicht allein auf Grundlage ihrer Tags (Markierungen) beenden, anhalten oder löschen. Sie müssen den Ressourcenbezeichner angeben. Um Snapshots zu löschen, die Sie mit dem Tag (Markierung)-Schlüssel `DeleteMe` markiert haben, müssen Sie die `DeleteSnapshots`-Aktion mit den Ressourcenbezeichnern der Snapshots verwenden, z. B. `snap-1234567890abcdef0`.

Wenn Sie öffentliche oder gemeinsam genutzte Ressourcen taggen, sind die von Ihnen zugewiesenen Tags nur für Ihr AWS Konto verfügbar. Kein anderes AWS Konto hat Zugriff auf diese Tags. Für die tagbasierte Zugriffskontrolle auf gemeinsam genutzte Ressourcen muss jedem AWS Konto ein eigener Satz von Stichwörtern zugewiesen werden, um den Zugriff auf die Ressource zu kontrollieren.

Tags (Markierungen) und Access Management

Wenn Sie AWS Identity and Access Management (IAM) verwenden, können Sie steuern, welche Benutzer in Ihrem AWS Konto berechtigt sind, Tags zu erstellen, zu bearbeiten oder zu löschen. Weitere Informationen finden Sie unter Erteilen Sie die Erlaubnis, EC2 Amazon-Ressourcen während der Erstellung zu taggen.

Sie können auch Resource-Tags (Markierungen) verwenden, um eine attributbasierte Steuerung (ABAC) zu implementieren. Sie können IAM-Richtlinien erstellen, die Vorgänge basierend auf den Tags (Markierungen) für die Ressource zulassen. Weitere Informationen finden Sie unter Den Zugriff mithilfe des attributbasierten Zugriffs steuern.

Markieren von Ressourcen für die Fakturierung

Sie können Tags verwenden, um Ihre AWS Rechnung so zu organisieren, dass sie Ihrer eigenen Kostenstruktur entspricht. Melden Sie sich dazu an, um Ihre AWS Kontorechnung mit den Tag-Schlüsselwerten zu erhalten. Weitere Informationen zum Einrichten eines Kostenzuordnungsberichts mit Markierungen finden Sie unter Monatlicher Kostenzuordnungsbericht im AWS Billing - Benutzerhandbuch. Um die Kosten kombinierter Ressourcen anzuzeigen, können Sie Ihre Fakturierungsinformationen nach Ressourcen mit gleichen Tag (Markierung)-Schlüsselwerten strukturieren. Beispielsweise können Sie mehrere Ressourcen mit einem bestimmten Anwendungsnamen markieren und dann Ihre Fakturierungsinformationen so organisieren, dass Sie die Gesamtkosten dieser Anwendung über mehrere Services hinweg sehen können. Weitere Informationen finden Sie unter Verwendung von Tags (Markierungen) zur Kostenzuordnung im Benutzerhandbuch für AWS Billing .

> **Note**
>
> Wenn Sie die Berichterstellung gerade erst aktiviert haben, werden die Daten für den aktuellen Monat nach 24 Stunden bereitgestellt.

Kostenzuordnungs-Tags (Markierungen) dienen der Anzeige, welche Ressourcen zu Ihrer Nutzung und Ihren Kosten beitragen. Das Löschen oder Deaktivieren der Ressourcen führt nicht zwangsläufig zur Kostensenkung. Beispiel: Snapshot-Daten, auf die von einem anderen Snapshot verwiesen wird, werden selbst dann beibehalten, wenn der Snapshot gelöscht wird, der die ursprünglichen Daten enthält. Weitere Informationen finden Sie unter Amazon Elastic Block Store-Volumes und -Snapshots im Benutzerhandbuch für AWS Billing .

> **Note**
>
> Elastic IP-Adressen, die mit Tags (Markierungen) versehen sind, erscheinen nicht in Ihrem Kostenzuordnungsbericht.

Erteilen Sie die Erlaubnis, EC2 Amazon-Ressourcen während der Erstellung zu taggen

Bei einigen Amazon EC2 API-Aktionen zur Ressourcenerstellung können Sie Tags angeben, wenn Sie die Ressource erstellen. Sie können Resource-Tags (Markierungen) verwenden, um eine attributbasierte Steuerung (ABAC) zu implementieren. Weitere Informationen erhalten Sie unter Markieren Ihrer -Ressourcen mit Tags (Markierungen) und Den Zugriff mithilfe des attributbasierten Zugriffs steuern.

Damit Benutzer diese Möglichkeit erhalten, benötigen sie die Berechtigungen zum Verwenden der Aktion, die die Ressource wie `ec2:RunInstances` oder `ec2:CreateVolume` erstellt. Wenn Tags in der Aktion angegeben werden, mit der die Ressource erstellt wird, führt Amazon eine zusätzliche Autorisierung für die `ec2:CreateTags`-Aktion aus, um die Berechtigungen der Benutzer zum Erstellen von Tags zu überprüfen. Daher benötigen die Benutzer außerdem die expliziten Berechtigungen zum Verwenden der `ec2:CreateTags`-Aktion.

Verwenden Sie in der IAM-Richtliniendefinition für die `ec2:CreateTags`-Aktion das `Condition`-Element mit dem `ec2:CreateAction`-Bedingungsschlüssel, um der Aktion, die die Ressource erstellt, Markierungsberechtigungen zu erteilen.

Die folgende Beispiel zeigt eine Richtlinie, die es Benutzern erlaubt, Instances zu starten und Instances und Volumes während des Starts beliebige Tags (Markierungen) hinzuzufügen. Die Markierung von bestehenden Ressourcen durch die Benutzer ist nicht zulässig. (Sie können die `ec2:CreateTags`-Aktion nicht direkt aufrufen.)

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

In ähnlicher Weise erlaubt die folgende Richtline Benutzern, Volumes zu erstellen und ihnen dabei beliebige Tags (Markierungen) hinzuzufügen. Die Markierung von bestehenden Ressourcen durch die Benutzer ist nicht zulässig. (Sie können die `ec2:CreateTags`-Aktion nicht direkt aufrufen.)

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateVolume"
      ],
      "Resource": "*"
    },
```

```
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:111122223333:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "CreateVolume"
          }
       }
    }
  ]
}
```

Die `ec2:CreateTags`-Aktion wird nur ausgewertet, wenn die Tags während der Aktion zur Ressourcenerstellung angewendet werden. Folglich benötigt ein Benutzer, der über die Berechtigungen zum Erstellen einer Ressource verfügt (vorausgesetzt, es bestehen keine Markierungsbedingungen), keine Berechtigungen zur Verwendung der `ec2:CreateTags`-Aktion, wenn keine Tags in der Anforderung angegeben werden. Wenn der Benutzer allerdings versucht, eine Ressource mit Tags zu erstellen, schlägt die Anforderung fehl, wenn der Benutzer nicht über die Berechtigungen für die `ec2:CreateTags`-Aktion verfügt.

Die `ec2:CreateTags`-Aktion wird auch ausgewertet, wenn Tags in einer Startvorlage bereitgestellt werden. Eine Beispielrichtlinie finden Sie unter Tags (Markierungen) in einer Startvorlage.

Kontrollieren des Zugriffs auf bestimmte Tags (Markierungen)

Sie können zusätzliche Bedingungen im `Condition`-Element Ihrer IAM-Richtlinien verwenden, um die Tag-Schlüssel und -Werte zu steuern, die auf Ressourcen angewendet werden können.

Die folgenden Bedingungsschlüssel können mit den Beispielen im vorangegangenen Abschnitt verwendet werden:

- `aws:RequestTag`: Gibt an, dass eine Anforderung einen bestimmten Tag-Schlüssel oder Tag-Schlüssel und -Wert enthalten muss. In der Anforderung können auch andere Tags (Markierungen) angegeben werden.
  - Zusammen mit dem `StringEquals`-Bedingungsoperator können Sie eine bestimmte Tag-Schlüssel- und -Wert-Kombination erzwingen, z. B. den Tag `cost-center=cc123`:

```
"StringEquals": { "aws:RequestTag/cost-center": "cc123" }
```

- In Kombination mit dem `StringLike`-Bedingungsoperator erzwingen Sie einen bestimmten Tag-Schlüssel in der Anforderung, beispielsweise den Tag-Schlüssel `purpose`:

```
"StringLike": { "aws:RequestTag/purpose": "*" }
```

- `aws:TagKeys`: Erzwingt die Tag-Schlüssel, die in der Anforderung verwendet werden.
  - Verwenden Sie diesen Bedingungsschlüssel mit dem `ForAllValues`-Modifikator, um bestimmte Tag-Schlüssel zu erzwingen, die in der Anforderung bereitgestellt werden (wenn in der Anforderung Tags angegeben werden, sind nur bestimmte Tags erlaubt und keine anderen Tags gestattet). Im folgenden Beispiel sind die Tag-Schlüssel `environment` oder `cost-center` erlaubt:

```
"ForAllValues:StringEquals": { "aws:TagKeys": ["environment","cost-center"] }
```

  - Zusammen mit dem `ForAnyValue`-Modifikator wird erzwungen, dass die Anforderung mindestens einen der angegebenen Tag-Schlüssel umfassen muss. Zum Beispiel muss mindestens einer der Tag-Schlüssel `environment` und `webserver` in der Anforderung enthalten sein:

```
"ForAnyValue:StringEquals": { "aws:TagKeys": ["environment","webserver"] }
```

Diese Bedingungsschlüssel können auf Aktionen zur Ressourcenerstellung, die Markierungen unterstützen, sowie `ec2:CreateTags`- und `ec2:DeleteTags`-Aktionen angewendet werden. Informationen darüber, ob eine EC2 Amazon-API-Aktion Tagging unterstützt, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2.

Wenn Sie erzwingen möchten, dass die Benutzer beim Erstellen einer Ressource Tags angeben, müssen Sie den `aws:RequestTag`-Bedingungsschlüssel oder den `aws:TagKeys`-Bedingungsschlüssel mit dem `ForAnyValue`-Modifikator für die Aktion zur Erstellung von Ressourcen verwenden. Wenn ein Benutzer für diese Aktion zur Ressourcenerstellung keine Tags angibt, wird die `ec2:CreateTags`-Aktion nicht ausgewertet.

Bei Bedingungen gilt, dass die Groß- und Kleinschreibung für den Bedingungsschlüssel nicht berücksichtigt und für den Bedingungswert beachtet wird. Verwenden Sie aus diesem Grund den `aws:TagKeys`-Bedingungsschlüssel und geben Sie den Tag (Markierung)-Schlüssel als Wert

dieser Bedingung an, wenn Sie die Berücksichtigung der Groß- und Kleinschreibung für einen Tag (Markierung)-Schlüssel erzwingen möchten.

Beispiele für IAM-Richtlinien finden Sie unter Beispielrichtlinien zur Steuerung des Zugriffs auf die EC2 Amazon-API. Weitere Informationen finden Sie unter Bedingungen mit mehrfachen Kontextschlüsseln oder Werten im IAM-Benutzerhandbuch.

Hinzufügen und Entfernen von Tags für EC2 Amazon-Ressourcen

Wenn Sie eine EC2 Amazon-Ressource erstellen, z. B. eine EC2 Amazon-Instance, können Sie die Tags angeben, die der Ressource hinzugefügt werden sollen. Sie können auch die EC2 Amazon-Konsole verwenden, um die Tags für eine bestimmte EC2 Amazon-Ressource anzuzeigen. Sie können auch Tags zu einer vorhandenen EC2 Amazon-Ressource hinzufügen oder daraus entfernen.

Sie können den Tag-Editor in der AWS -Ressourcengruppen Konsole verwenden, um Tags für all Ihre AWS Ressourcen in allen Regionen anzuzeigen, hinzuzufügen oder zu entfernen. Sie können Markierungen jeweils mehreren Ressourcen und mehreren Ressourcentypen gleichzeitig hinzuzufügen oder diese entfernen. Weitere Informationen finden Sie im Tagging AWS Resources User Guide.

Aufgaben

- Hinzufügen von Tags mithilfe der Konsole
- Fügen Sie Tags hinzu mit dem AWS CLI
- Fügen Sie Tags hinzu, indem Sie PowerShell
- Fügen Sie Tags hinzu mit CloudFormation

Hinzufügen von Tags mithilfe der Konsole

Sie können einer bestehenden Ressourcen direkt auf der Seite der Ressource Tags hinzufügen.

So fügen Sie Tags zu einer vorhandenen Ressource hinzu

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste die Region aus, in der sich die Ressource befindet.
3. Wählen Sie im Navigationsbereich einen Ressourcentyp aus (z. B. Instances).
4. Wählen Sie die Ressource aus der Liste aus.

5. Wählen Sie auf der Registerkarte Tags die Option Tags verwalten.
6. Wählen Sie Neues Tag hinzufügen und geben Sie dann einen Schlüssel und einen Wert für das Tag ein.
7. Wählen Sie Speichern.

Fügen Sie Tags hinzu mit dem AWS CLI

Sie können Tags zu vorhandenen Ressourcen oder beim Erstellen einer Ressource hinzufügen.

So fügen Sie ein Tag bei der Ressourcenerstellung hinzu

Verwenden Sie die Option `-tag-specifications`, um eine Ressource bei der Erstellung zu markieren. Eine Tag-Spezifikation erfordert den Typ der zu markierenden Ressource, den Tag-Schlüssel und den Tag-Wert. Im folgenden Beispiel wird ein Tag erstellt und einer Tag-Spezifikation hinzugefügt.

```
--tag-specifications 'ResourceType=instance,Tags=[{Key=stack,Value=production}]'
```

So fügen Sie ein Tag zu einer vorhandenen Ressource hinzu

In den folgenden Beispielen wird veranschaulicht, wie Sie mithilfe des Befehls create-tags Tags zu vorhandenen Ressourcen hinzufügen.

Example Beispiel: Hinzufügen eines Tags (Markierung) zu einer Ressource

Der folgende Befehl fügt das Tag **`Stack=production`** zu dem angegebenen Image hinzu oder überschreibt ein vorhandenes Tag für das AMI, wobei der Tag-Schlüssel stack ist. Wird der Befehl erfolgreich ausgeführt, wird keine Ausgabe zurückgegeben.

```
aws ec2 create-tags \
    --resources ami-0abcdef1234567890 \
    --tags Key=stack,Value=production
```

Example Beispiel: Hinzufügen von Tags (Markierungen) zu mehreren Ressourcen

In diesem Beispiel werden zwei Tags (Markierungen) für ein AMI und eine Instance hinzugefügt (oder überschrieben). Eines der Tags enthält nur einen Schlüssel (webserver) ohne Wert (Wir legen den Wert auf eine leere Zeichenfolge fest). De andere Tag (Markierung) besteht aus einem Schlüssel (stack) und einem Wert (**`Production`**). Wird der Befehl erfolgreich ausgeführt, wird keine Ausgabe zurückgegeben.

```
aws ec2 create-tags \
    --resources ami-0abcdef1234567890 i-1234567890abcdef0 \
    --tags Key=webserver,Value=  Key=stack,Value=Production
```

Example Beispiel: Hinzufügen von Tags (Markierungen) mit Sonderzeichen

In diesem Beispiel wird der Tag (Markierung) [Group]=test zu einer Instance hinzugefügt. Die eckigen Klammern ([und]) sind Sonderzeichen, die mit Escape-Zeichen versehen werden müssen.

Wenn Sie Linux oder OS X verwenden, um die Sonderzeichen mit Escape-Zeichen zu versehen, schließen Sie das Element mit dem Sonderzeichen in doppelte Anführungszeichen (") ein und schließen Sie dann die gesamte Schlüssel- und Wertstruktur in einfache Anführungszeichen (') ein.

```
aws ec2 create-tags \
    --resources i-1234567890abcdef0 \
    --tags 'Key="[Group]",Value=test'
```

Wenn Sie Windows verwenden, um die Sonderzeichen mit Escape-Zeichen zu versehen, schließen Sie das Element, das Sonderzeichen enthält, in doppelte Anführungszeichen (") ein und stellen Sie jedem doppelten Anführungszeichen wie folgt einen umgekehrten Schrägstrich (\) voran:

```
aws ec2 create-tags ^
    --resources i-1234567890abcdef0 ^
    --tags Key=\"[Group]\",Value=test
```

Wenn Sie Windows verwenden PowerShell, schließen Sie den Wert, der Sonderzeichen enthält, in doppelte Anführungszeichen (**"**) ein, stellen Sie jedem doppelten Anführungszeichen einen umgekehrten Schrägstrich (****) voran und schließen Sie dann die gesamte Schlüssel- und Wertstruktur wie folgt in einfache Anführungszeichen () ein: **'**

```
aws ec2 create-tags `
    --resources i-1234567890abcdef0 `
    --tags 'Key=\"[Group]\",Value=test'
```

Fügen Sie Tags hinzu, indem Sie PowerShell

Sie können Tags zu vorhandenen Ressourcen oder beim Erstellen einer Ressource hinzufügen.

So fügen Sie ein Tag bei der Ressourcenerstellung hinzu

Verwenden Sie den Parameter `-TagSpecification`, um eine Ressource bei der Erstellung zu markieren. Eine Tag-Spezifikation erfordert den Typ der zu markierenden Ressource, den Tag-Schlüssel und den Tag-Wert. Im folgenden Beispiel wird ein Tag erstellt und einer Tag-Spezifikation hinzugefügt.

```
$tag = @{Key="stack"; Value="production"}
$tagspec = new-object Amazon.EC2.Model.TagSpecification
$tagspec.ResourceType = "instance"
$tagspec.Tags.Add($tag)
```

Im folgenden Beispiel wird dieses Tag im `-TagSpecification`-Parameter angegeben.

```
-TagSpecification $tagspec
```

So fügen Sie ein Tag zu einer vorhandenen Ressource hinzu

Verwenden Sie das cmdlet New-EC2Tag. Sie müssen die Ressource, den Tag-Schlüssel und den Tag-Wert angeben.

```
New-EC2Tag `
    -Resource i-1234567890abcdef0 `
    -Tag @{Key="purpose"; Value="production"}
```

Fügen Sie Tags hinzu mit CloudFormation

Bei EC2 Amazon-Ressourcentypen geben Sie Tags entweder mit einer `TagSpecifications` Eigenschaft `Tags` oder an.

In den folgenden Beispielen wird das Tag **`Stack=Production`** AWS::EC2::Instancemithilfe seiner `Tags` Eigenschaft hinzugefügt.

Example Beispiel: Tags (Markierungen) in YAML

```
Tags:
  - Key: "Stack"
    Value: "Production"
```

Example Beispiel: Tags (Markierungen) in JSON

```
"Tags": [
```

```
    {
        "Key": "Stack",
        "Value": "Production"
    }
]
```

In den folgenden Beispielen wird das Tag **`Stack=Production`** [AWS::EC2::LaunchTemplate LaunchTemplateData](#)mithilfe seiner `TagSpecifications` Eigenschaft hinzugefügt.

Example Beispiel: TagSpecifications in YAML

```
TagSpecifications:
  - ResourceType: "instance"
    Tags:
    - Key: "Stack"
      Value: "Production"
```

Example Beispiel: TagSpecifications in JSON

```
"TagSpecifications": [
    {
        "ResourceType": "instance",
        "Tags": [
            {
                "Key": "Stack",
                "Value": "Production"
            }
        ]
    }
]
```

EC2 Amazon-Ressourcen nach Tag filtern

Nachdem Sie Tags hinzugefügt haben, können Sie Ihre auf EC2 Amazon-Ressourcen basierenden Tag-Schlüssel und Tag-Werte filtern.

Console

So filtern Sie Ressourcen nach Tags

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich einen Ressourcentyp aus (z. B. Instances).
3. Wählen Sie das Suchfeld aus.
4. Wählen Sie in der Liste unter Markierungen den Markierungs-Schlüssel aus.
5. Wählen Sie den entsprechenden Tag (Markierung)-Wert aus der Liste.
6. Wenn Sie fertig sind, entfernen Sie den Filter.

Weitere Informationen zur Verwendung von Filtern in der EC2 Amazon-Konsole finden Sie unterFinden Sie Ihre EC2 Amazon-Ressourcen.

AWS CLI

So beschreiben Sie Ressourcen eines einzelnen Typs mit dem angegebenen Tag-Schlüssel

Fügen Sie den folgenden Filter zu einem `describe`-Befehl hinzu, um die Ressourcen dieses Typs mit einem Stack-Tag zu beschreiben, ungeachtet des Tag-Werts.

```
--filters Name=tag-key,Values=Stack
```

So beschreiben Sie Ressourcen eines einzelnen Typs mit dem angegebenen Tag

Fügen Sie den folgenden Filter zu einem `describe`-Befehl hinzu, um die Ressourcen dieses Typs mit einem Stack=production-Tag zu beschreiben.

```
--filters Name=tag:Stack,Values=production
```

So beschreiben Sie Ressourcen eines einzelnen Typs mit dem angegebenen Tag-Wert

Fügen Sie den folgenden Filter zu einem `describe`-Befehl hinzu, um die Ressourcen dieses Typs mit einem Tag mit dem Wert production zu beschreiben, ungeachtet des Tag-Schlüssels.

```
--filters Name=tag-value,Values=production
```

Um alle EC2 Ressourcen mit dem angegebenen Tag zu beschreiben

Fügen Sie dem Befehl describe-tags den folgenden Filter hinzu, um alle EC2 Ressourcen mit dem Tag zu beschreiben. Stack=test

```
--filters Name=key,Values=Stack Name=value,Values=test
```

PowerShell

So filtern Sie Ressourcen eines einzelnen Typs nach dem Tag-Schlüssel

Fügen Sie den folgenden Filter zu einem `Get`-cmdlet hinzu, um die Ressourcen dieses Typs mit einem Stack-Tag zu beschreiben, ungeachtet des Tag-Werts.

```
-Filter @{Name="tag-key"; Values="Stack"}
```

So filtern Sie Ressourcen eines einzelnen Typs nach dem Tag

Fügen Sie den folgenden Filter zu einem `Get`-cmdlet hinzu, um die Ressourcen dieses Typs mit dem Tag Stack=production zu beschreiben.

```
-Filter @{Name="tag:Stack"; Values="production"}
```

So filtern Sie Ressourcen eines einzelnen Typs nach dem Tag-Wert

Fügen Sie den folgenden Filter zu einem `Get`-cmdlet hinzu, um die Ressourcen dieses Typs mit einem Tag mit dem Wert production zu beschreiben, ungeachtet des Werts des Tag-Schlüssels.

```
-Filter @{Name="tag-value"; Values="production"}
```

Um alle EC2 Ressourcen nach einem Tag zu filtern

Fügen Sie dem Get-EC2TagCmdlet den folgenden Filter hinzu, um alle EC2 Ressourcen mit dem Tag zu beschreiben. Stack=test

```
-Filter @{Name="tag:Stack"; Values="test"}
```

Zeigen Sie Tags für Ihre EC2 Instances mithilfe von Instanz-Metadaten an

Sie können über die Instance-Metadaten auf die Tags einer Instance zugreifen. Wenn Sie über die Instance-Metadaten auf Tags zugreifen, werden die API-Aufrufe `DescribeInstances` und `DescribeTags` nicht mehr zum Abrufen von Tag-Informationen benötigt. Dadurch werden Ihre API-Transaktionen pro Sekunde reduziert und Ihre Tag-Abrufe können mit der Anzahl der Instances, die Sie steuern, skaliert werden. Darüber hinaus können lokale Prozesse, die auf einer Instance ausgeführt werden, die Tag-Informationen der Instance direkt in den Instance-Metadaten anzeigen.

Tags sind standardmäßig nicht in den Instance-Metadaten verfügbar; Sie müssen den Zugriff explizit zulassen. Sie können den Zugriff beim Start der Instance oder nach dem Start auf einer ausgeführten oder angehaltenen Instance zulassen. Sie können den Zugriff auf Tags auch zulassen, indem Sie dies in einer Startvorlage angeben. Instances, die mit der Vorlage gestartet werden, lassen den Zugriff auf Tags in den Instance-Metadaten zu.

Wenn Sie eine Instance-Markierung hinzufügen oder entfernen, werden die Instance-Metadaten aktualisiert, während die Instance läuft, ohne dass Sie die Instance anhalten und wieder starten müssen.

Aufgaben

- Zugriff auf Tags in Instance-Metadaten ermöglichen
- Abrufen von Tags aus Instance-Metadaten
- Zugriff auf Tags in Instance-Metadaten deaktivieren

Zugriff auf Tags in Instance-Metadaten ermöglichen

Standardmäßig gibt es keinen Zugriff auf Instance-Tags in den Instance-Metadaten. Sie müssen den Zugriff für jede Instance explizit ermöglichen.

> **Note**
>
> Wenn Sie den Zugriff auf Tags in Instance-Metadaten zulassen, unterliegen Instance-Tag-Schlüssel bestimmten Einschränkungen. Eine Nichteinhaltung der Vorschriften führt zu fehlgeschlagenen Starts für neue Instances oder zu einem Fehler bei vorhandenen Instances. Die Einschränkungen sind:
>
> - Kann nur Buchstaben (`a-z`, `A-Z`), Zahlen (`0-9`) und die folgenden Zeichen enthalten: `+ - = . , _ : @`.
> - Dürfen keine Leerzeichen oder `/` enthalten.
> - Kann nicht nur aus `.` (einer Periode), `..` (zwei Perioden) oder `_index` bestehen.
>
> Weitere Informationen finden Sie unter Tag (Markierung)-Einschränkungen.

Console

So ermöglichen Sie den Zugriff auf Tags in Instance-Metadaten beim Instance-Start

1. Befolgen Sie das Verfahren zum Starten einer Instance.
2. Erweitern Sie Erweiterte Details und wählen Sie für Tags in Metadaten zulassen die Option Aktivieren aus.
3. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten.

So ermöglichen Sie den Zugriff auf Tags in Instance-Metadaten nach dem Instance-Start

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie zuerst eine Instance aus und wählen Sie dann in den Instance-Einstellungen unter Aktionen die Option Tags in Instance-Metadaten zulassen.
4. Zum Zulassen des Zugriffs auf Tags in Instance-Metadaten aktivieren Sie das Kontrollkästchen Zulassen.
5. Wählen Sie Speichern.

AWS CLI

So ermöglichen Sie den Zugriff auf Tags in Instance-Metadaten beim Instance-Start

Verwenden Sie den Befehl run-instances und fügen Sie die Option `--metadata-options` hinzu.

```
--metadata-options "InstanceMetadataTags=enabled"
```

So ermöglichen Sie den Zugriff auf Tags in Instance-Metadaten nach dem Instance-Start

Verwenden Sie den folgenden modify-instance-metadata-options-Befehl.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --instance-metadata-tags enabled
```

So überprüfen Sie, ob der Zugriff auf Tags in Instance-Metadaten ermöglicht ist

Verwenden Sie den Befehl describe-instances und überprüfen Sie den Wert von `InstanceMetadataTags`.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query "Reservations[*].Instances[].MetadataOptions[].InstanceMetadataTags"
```

Es folgt eine Beispielausgabe. Der Wert ist entweder `enabled` oder `disabled`.

```
[
    "enabled"
]
```

PowerShell

So ermöglichen Sie den Zugriff auf Tags in Instance-Metadaten beim Instance-Start

Verwenden Sie das New-EC2InstanceCmdlet und fügen Sie den folgenden `-MetadataOptions_InstanceMetadataTags` Parameter hinzu.

```
-MetadataOptions_InstanceMetadataTags enabled
```

So ermöglichen Sie den Zugriff auf Tags in Instance-Metadaten nach dem Instance-Start

Verwenden Sie das cmdlet Edit-EC2InstanceMetadataOption.

```
Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -InstanceMetadataTags enabled
```

So überprüfen Sie, ob der Zugriff auf Tags in Instance-Metadaten ermöglicht ist

Verwenden Sie das Get-EC2InstanceCmdlet und überprüfen Sie den Wert von. `InstanceMetadataTags`

```
(Get-EC2Instance `
```

```
    -
InstanceId i-1234567890abcdef0).Instances.MetadataOptions.InstanceMetadataTags.Value
```

Es folgt eine Beispielausgabe. Der Wert ist entweder `enabled` oder `disabled`.

```
enabled
```

Abrufen von Tags aus Instance-Metadaten

Nachdem Sie den Zugriff auf Instance-Tags in den Instance-Metadaten erlaubt haben, können Sie über die Instance-Metadaten auf die `tags/instance`-Kategorie zugreifen. Weitere Informationen finden Sie unter Auf Instanz-Metadaten für eine EC2 Instanz zugreifen.

IMDSv2

Linux

Führen Sie den folgenden Befehl von Ihrer Linux-Instance aus, um alle Tag-Schlüssel für die Instance aufzulisten.

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
    && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/tags/instance
```

In diesem Beispiel wird der Wert eines Schlüssels abgerufen, der im vorherigen Beispiel ermittelt wurde. Die IMDSv2 Anforderung verwendet das gespeicherte Token, das mit dem Befehl im vorherigen Beispiel erstellt wurde. Das Token darf nicht abgelaufen sein.

```
curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/tags/instance/tag-key
```

Windows

Führen Sie das folgende cmdlet von Ihrer Windows-Instance aus, um alle Tag-Schlüssel für die Instance aufzulisten.

```
$token = Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
```

```
    -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/tags/instance
```

In diesem Beispiel wird der Wert eines Schlüssels abgerufen, der im vorherigen Beispiel ermittelt wurde. Die IMDSv2 Anfrage verwendet das gespeicherte Token, das mit dem Befehl im vorherigen Beispiel erstellt wurde. Das Token darf nicht abgelaufen sein.

```
Invoke-RestMethod `
    -Headers @{"X-aws-ec2-metadata-token" = $token} `
    -Method GET -Uri http://169.254.169.254/latest/meta-data/tags/instance/tag-key
```

IMDSv1

Linux

Führen Sie den folgenden Befehl von Ihrer Linux-Instance aus, um alle Tag-Schlüssel für die Instance aufzulisten.

```
curl http://169.254.169.254/latest/meta-data/tags/instance
```

In diesem Beispiel wird der Wert eines Schlüssels abgerufen, der im vorherigen Beispiel ermittelt wurde.

```
curl http://169.254.169.254/latest/meta-data/tags/instance/tag-key
```

Windows

Führen Sie das folgende cmdlet von Ihrer Windows-Instance aus, um alle Tag-Schlüssel für die Instance aufzulisten.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/tags/instance
```

In diesem Beispiel wird der Wert eines Schlüssels abgerufen, der im vorherigen Beispiel ermittelt wurde.

```
Invoke-RestMethod -Uri http://169.254.169.254/latest/meta-data/tags/instance/tag-key
```

Zugriff auf Tags in Instance-Metadaten deaktivieren

Sie können den Zugriff auf Instance-Tags in den Instance-Metadaten deaktivieren. Sie müssen den Zugriff auf Instance-Tags in Instance-Metadaten beim Start nicht deaktivieren, da dieser standardmäßig deaktiviert ist.

Console

So deaktivieren Sie den Zugriff auf Tags in Instance-Metadaten

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie zuerst eine Instance aus und wählen Sie dann in den Instance settings (Instance-Einstellungen) unter Actions (Aktionen) die Option Allow tags in instance metadata (Zulassen von Tags in Instance-Metadaten).
4. Zum Deaktivieren des Zugriffs auf Tags in Instance-Metadaten deaktivieren Sie das Kontrollkästchen Zulassen.
5. Wählen Sie Speichern.

AWS CLI

So deaktivieren Sie den Zugriff auf Tags in Instance-Metadaten

Verwenden Sie den folgenden modify-instance-metadata-options-Befehl.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567890abcdef0 \
    --instance-metadata-tags disabled
```

PowerShell

So deaktivieren Sie den Zugriff auf Tags in Instance-Metadaten

Verwenden Sie das cmdlet Edit-EC2InstanceMetadataOption.

```
Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567890abcdef0 `
    -InstanceMetadataTag disabled
```

EC2 Amazon-Servicekontingente

Wenn Sie Ihre erstellen AWS-Konto, legen wir Standardkontingente (auch als Limits bezeichnet) für Ihre AWS Ressourcen auf regionaler Basis fest. Wenn Sie versuchen, das Kontingent für eine Ressource zu überschreiten, schlägt die Anforderung fehl. Beispielsweise gibt es eine maximale Anzahl von Amazon EC2 v, CPUs die Sie für On-Demand-Instances in einer Region bereitstellen können. Wenn Sie versuchen, eine Instance in einer Region zu starten, und diese Anforderung dazu führen würde, dass Ihre Nutzung dieses Kontingent überschreitet, schlägt die Anforderung fehl. Wenn das passiert, können Sie Ihren Ressourcenverbrauch reduzieren oder eine Kontingenterhöhung beantragen.

Die Servicekontingenten-Konsole ist ein zentraler Ort, an dem Sie Ihre Kontingente für AWS Dienste anzeigen und verwalten und eine Erhöhung des Kontingents für viele der von Ihnen verwendeten Ressourcen beantragen können. Verwenden Sie die von uns bereitgestellten Kontingent , um Ihre AWS Infrastruktur zu verwalten. Planen Sie Anfragen zur Erhöhung der Kontingente im Voraus vor dem Zeitpunkt, zu dem Sie sie benötigen.

Dazugehörige Dokumentation zu Kontingenten

- EC2 Amazon-Endpunkte und Kontingente
- Kontingente für EC2 Amazon-Instance-Typen
- Kontingente für Amazon EBS
- Amazon-VPC-Kontingente

Anzeigen Ihrer aktuellen Kontingente

Sie können Ihre Kontingente für jede Region in der Console einsehen.

So zeigen Sie Ihre aktuellen Kontingente mit der Service-Quotas-Konsole an

1. Öffnen Sie die Service Quotas Quotas-Konsole unter https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Wählen Sie auf der Navigationsleiste (oben auf dem Bildschirm) eine Region aus.
3. Wählen Sie im Bereich „Kontingente verwalten“ einen Service aus, z. B. Amazon Elastic Compute Cloud (Amazon EC2). Wählen Sie Kontingente anzeigen aus.
4. Verwenden Sie das Filterfeld, um die Liste nach Ressourcennamen zu filtern. Geben Sie beispielsweise **`On-Demand`** ein, um die Kontingente für On-Demand-Instances zu ermitteln.

5. Wählen Sie zum Anzeigen weiterer Informationen den Kontingentnamen aus, um die Detailseite für das Kontingent zu öffnen.

Beantragen einer Erhöhung

Sie können eine Kontingenterhöhung für jede Region beantragen.

So fordern Sie eine Erhöhung über die Service-Quotas-Konsole an

1. Öffnen Sie die Service Quotas Quotas-Konsole unter https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Wählen Sie auf der Navigationsleiste (oben auf dem Bildschirm) eine Region aus.
3. Verwenden Sie das Filterfeld, um die Liste nach Ressourcennamen zu filtern. Geben Sie beispielsweise **`On-Demand`** ein, um die Kontingente für On-Demand-Instances zu ermitteln.
4. Wenn das Kontingent anpassbar ist, wählen Sie das Kontingent aus und wählen Sie dann Kontingenterhöhung anfordern.
5. Geben Sie unter Kontingentwert ändern den neuen Kontingentwert ein.
6. Wählen Sie Anfrage aus.
7. Um ausstehende oder kürzlich genehmigte Anfragen in der Konsole anzuzeigen, wählen Sie im Navigationsbereich die Option Dashboard . Wählen Sie für ausstehende Anfragen den Status der Anfrage, um die Anfrage zu öffnen. Der Anfangsstatus einer Anfrage ist Pending (Ausstehend). Nachdem sich der Status in „Kontingent angefordert“ geändert hat, wird die Fallnummer mit angezeigt Support. Wählen Sie die Fallnummer, um das Ticket für Ihre Anfrage zu öffnen.

Weitere Informationen, einschließlich der Verwendung von AWS CLI oder SDKs , um eine Kontingenterhöhung anzufordern, finden Sie unter Eine Kontingenterhöhung beantragen im Servicekontingents-Benutzerhandbuch.

Einschränkung für E-Mails, die über Port 25 gesendet werden

Standardmäßig EC2 erlaubt Amazon ausgehenden Verkehr über Port 25 nur an private IPv4 Adressen. Der Verkehr über Port 25 ist für öffentliche IPv4 Adressen und IPv6 Adressen gesperrt.

Sie können beantragen, dass diese Einschränkung entfernt wird. Weitere Informationen finden Sie unter Wie entferne ich die Beschränkung für Port 25 aus meiner EC2 Amazon-Instance oder Lambda-Funktion?

Diese Einschränkung gilt nicht für ausgehenden Datenverkehr über Port 25 an:

- IP-Adressen im primären CIDR-Block der VPC, in der die ursprüngliche Netzwerkschnittstelle vorhanden ist.
- IP-Adressen sind in RFC 1918, RFC6598 und RFC 4193 CIDRs definiert.

Überwachen Sie die EC2 Amazon-Ressourcen

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer EC2 Amazon-Instances und Ihrer AWS Lösungen. Sie sollten Überwachungsdaten aus allen Teilen Ihrer AWS Lösungen sammeln, damit Sie einen etwaigen Ausfall an mehreren Stellen leichter debuggen können.

AWS bietet verschiedene Tools, mit denen Sie Amazon überwachen können EC2. Die Amazon EC2 - und CloudWatch Konsolen-Dashboards bieten einen at-a-glance Überblick über den Zustand Ihrer EC2 Amazon-Umgebung. Zusätzlich bieten wir:

- Systemstatusprüfungen — Überwachen Sie die AWS Systeme, die für die Nutzung Ihrer Instance erforderlich sind, um sicherzustellen, dass sie ordnungsgemäß funktionieren. Bei diesen Prüfungen werden Probleme mit Ihrer Instance erkannt, bei deren Behebung ein AWS Eingreifen erforderlich ist. Wenn eine System-Statusprüfung fehlschlägt, können Sie wählen, bis AWS das Problem behebt oder Sie können es selbst lösen (zum Beispiel per Anhalten und Neustarten einer Instance oder deren Beendigung und Ersetzung). Beispiele für Probleme, die dazu führen, dass Systemstatusprüfungen fehlschlagen, sind:
  - Verlust der Netzwerkverbindung
  - Systemstromausfall
  - Softwareprobleme auf dem physischen Host
  - Hardwareprobleme auf dem physischen Host, die die Erreichbarkeit des Netzwerks beeinträchtigen

  Weitere Informationen finden Sie unter Statuschecks für EC2 Amazon-Instances.
- Instance-Statusprüfungen – Überwachen Sie die Software- und Netzwerkkonfiguration Ihrer individuellen Instance. Bei diesen Überprüfungen werden Probleme Ihrer Instance erkannt, für die zur Reparatur Ihre Beteiligung erforderlich ist. Wenn eine Instance-Statusprüfung nicht bestanden wird, müssen Sie das Problem normalerweise selbst lösen (z. B. per Neustart der Instance oder durch das Vornehmen von Änderungen an Ihrem Betriebssystem). Beispiele für Probleme, die dazu führen, dass Instance-Statusprüfungen fehlschlagen, sind unter anderem:
  - Fehlgeschlagene System-Statusprüfungen
  - Falsch konfigurierte Netzwerk- oder Startup-Konfiguration
  - Unzureichender Speicher
  - Beschädigtes Dateisystem

  - Inkompatibler Kernel

  Weitere Informationen finden Sie unter Statuschecks für EC2 Amazon-Instances.

- CloudWatch Amazon-Alarme — Überwachen Sie eine einzelne Metrik über einen von Ihnen angegebenen Zeitraum und führen Sie eine oder mehrere Aktionen aus, die auf dem Wert der Metrik im Verhältnis zu einem bestimmten Schwellenwert über mehrere Zeiträume basieren. Die Aktion ist eine Benachrichtigung, die an ein Amazon Simple Notification Service (Amazon SNS) -Thema oder eine Amazon EC2 Auto Scaling Scaling-Richtlinie gesendet wird. Alarme lösen nur Aktionen für anhaltende Statusänderungen aus. CloudWatch Alarme lösen keine Aktionen aus, nur weil sie sich in einem bestimmten Zustand befinden. Der Status muss sich geändert haben und für eine bestimmte Anzahl von Zeiträumen beibehalten worden sein. Weitere Informationen finden Sie unter Überwachen Sie Ihre Instances mit CloudWatch.
- Amazon EventBridge Events — Automatisieren Sie Ihre AWS Services und reagieren Sie automatisch auf Systemereignisse. Ereignisse von AWS Services werden nahezu EventBridge in Echtzeit übermittelt, und Sie können automatische Aktionen festlegen, die ergriffen werden, wenn ein Ereignis einer von Ihnen erstellten Regel entspricht. Weitere Informationen finden Sie unter the section called “Automatisieren mithilfe von EventBridge”.
- AWS CloudTrail Logs — Erfassen Sie detaillierte Informationen über die Aufrufe der EC2 Amazon-API und speichern Sie sie als Protokolldateien in Amazon S3. Mithilfe von CloudTrail Protokollen können Sie feststellen, welche Anrufe getätigt wurden, welche Quell-IP-Adresse für den Anruf verwendet wurde, wer den Anruf getätigt hat und wann der Anruf getätigt wurde. Weitere Informationen finden Sie unter the section called “Protokollieren von API-Aufrufen mit CloudTrail”.
- CloudWatch Agent — Erfassen Sie Protokolle und Metriken auf Systemebene von Hosts und Gästen auf Ihren EC2 Instances und lokalen Servern. Weitere Informationen finden Sie unter Erfassung von Metriken und Protokollen von EC2 Amazon-Instances und lokalen Servern mit dem CloudWatch Agenten im CloudWatch Amazon-Benutzerhandbuch.

Überwachen Sie den Status Ihrer EC2 Amazon-Instances

Sie können den Status Ihrer Instances überwachen, indem Sie Statusüberprüfungen und geplante Ereignisse für Ihre Instances anzeigen.

Eine Statusüberprüfung gibt Ihnen die Informationen, die sich aus automatisierten Prüfungen ergeben, die von Amazon durchgeführt wurden EC2. Mit diesen automatisierten Überprüfungen wird ermittelt, ob bestimmte Probleme Ihre Instances beeinflussen. Die Informationen zur Statusprüfung

bieten Ihnen zusammen mit den von Amazon CloudWatch bereitgestellten Daten einen detaillierten Einblick in den Betrieb jeder Ihrer Instanzen.

Sie können außerdem den Status bestimmter Ereignisse anzeigen, die für Ihre Instances geplant sind. Der Status von Ereignissen gibt Auskunft über anstehende Aktivitäten, die für Ihre Instances geplant sind (z. B. Neustart oder Ruhestand). Sie liefern außerdem die geplante Start- und Endzeit jedes Ereignisses.

Inhalt

- Statuschecks für EC2 Amazon-Instances
- Ereignisse zur Statusänderung für EC2 Amazon-Instances
- Geplante Ereignisse für EC2 Amazon-Instances

Statuschecks für EC2 Amazon-Instances

Mit der Instance-Statusüberwachung können Sie schnell feststellen, ob Amazon Probleme erkannt EC2 hat, die Ihre Instances daran hindern könnten, Anwendungen auszuführen. Amazon EC2 führt automatische Prüfungen für jede laufende EC2 Instance durch, um Hardware- und Softwareprobleme zu identifizieren. Sie können die Ergebnisse dieser Statusprüfungen anzeigen, um bestimmte bzw. erkennbare Probleme zu ermitteln. Die Daten zum Ereignisstatus ergänzen die Informationen, die Amazon EC2 bereits über den Status der einzelnen Instances (wie`pending`,`running`,`stopping`) und die von Amazon CloudWatch überwachten Nutzungsmetriken (CPU-Auslastung, Netzwerkverkehr und Festplattenaktivität) bereitstellt.

Statusprüfungen werden minütlich durchgeführt und geben als Status "Bestanden" oder "Fehler" zurück. Wenn alle Überprüfungen bestanden wurden, lautet der Gesamtstatus der Instance OK. Falls mindestens eine Überprüfung nicht bestanden wird, lautet der Gesamtstatus impaired (beeinträchtigt). Statusprüfungen sind in Amazon integriert EC2, sodass sie nicht deaktiviert oder gelöscht werden können.

Wenn eine Statusüberprüfung fehlschlägt, wird die entsprechende CloudWatch Metrik für Statusprüfungen inkrementiert. Weitere Informationen finden Sie unter Statusprüfungsmetriken. Sie können diese Metriken verwenden, um CloudWatch-Alarme zu erstellen, die basierend auf dem Ergebnis der Statusprüfungen ausgelöst werden. Beispielsweise können Sie einen Alarm erstellen, mit dem Sie gewarnt werden, wenn Statusprüfungen für eine bestimmte Instance fehlschlagen. Weitere Informationen finden Sie unter CloudWatch Alarme für EC2 Amazon-Instances erstellen, die Statusprüfungen nicht bestehen.

Sie können auch einen CloudWatch Amazon-Alarm erstellen, der eine EC2 Amazon-Instance überwacht und die Instance automatisch wiederherstellt, wenn sie aufgrund eines zugrunde liegenden Problems beeinträchtigt wird. Weitere Informationen finden Sie unter Automatische Instance-Wiederherstellung.

Inhalt

- Arten von Statusprüfungen
- Statuschecks für EC2 Amazon-Instances anzeigen
- CloudWatch Alarme für EC2 Amazon-Instances erstellen, die Statusprüfungen nicht bestehen

Arten von Statusprüfungen

Es gibt drei Arten von Statusprüfungen.

- System-Statusprüfungen
- Instance-Statusprüfungen
- Verknüpfte EBS-Statusprüfungen

System-Statusprüfungen

Systemstatusprüfungen überwachen die AWS Systeme, auf denen Ihre Instance ausgeführt wird. Bei diesen Überprüfungen werden die zugrunde liegenden Probleme Ihrer Instance erkannt, für die zur Reparatur die Beteiligung von AWS erforderlich ist. Wenn eine Systemstatusprüfung fehlschlägt, können Sie wählen, ob Sie warten AWS möchten, bis das Problem behoben ist, oder Sie können es selbst lösen. Für von Amazon EBS unterstützte Instances können Sie die Instance selbst stoppen und starten, was in den meisten Fällen dazu führt, dass die Instance auf einen neuen Host migriert wird. Für Instances, die vom Instance-Speicher gestützt sind (nur für Linux-Instances unterstützt), können Sie die Instance beenden und ersetzen. Beachten Sie, dass Instance-Speicher-Volumes kurzlebig sind und alle Daten verloren gehen, wenn die Instance gestoppt wird.

Hier sind Beispiele für Probleme aufgeführt, die dazu führen können, dass System-Statusprüfungen fehlschlagen:

- Verlust der Netzwerkverbindung
- Systemstromausfall
- Softwareprobleme auf dem physischen Host

- Hardwareprobleme auf dem physischen Host, die die Erreichbarkeit des Netzwerks beeinträchtigen

Wenn eine Systemstatusprüfung fehlschlägt, erhöhen wir die StatusCheckFailed_System-Metrik.

Bare Metal-Instances

Wenn Sie einen Neustart vom Betriebssystem auf einer Bare-Metal-Instance durchführen, gibt die Systemstatusprüfung möglicherweise vorübergehend einen Fehlerstatus zurück. Wenn die Instance verfügbar ist, sollte die Systemstatusprüfung einen Passstatus zurückgeben.

Instance-Statusprüfungen

Instance-Statusprüfungen überwachen die Software und Netzwerkkonfiguration Ihrer individuellen Instance. Amazon EC2 überprüft den Zustand der Instance, indem es eine ARP-Anfrage (Address Resolution Protocol) an die Netzwerkschnittstelle (NIC) sendet. Bei diesen Überprüfungen werden Probleme Ihrer Instance erkannt, für die zur Reparatur Ihre Beteiligung erforderlich ist. Wenn eine Instance-Statusprüfung nicht bestanden wird, müssen Sie das Problem normalerweise selbst lösen (z. B. per Neustart der Instance oder durch das Vornehmen von Konfigurationsänderungen für die Instance).

> **Note**
>
> Neuere Linux-Distributionen, die `systemd-networkd` für die Netzwerkkonfiguration verwenden, berichten möglicherweise anders über Integritätsprüfungen als frühere Distributionen. Während des Startvorgangs kann dieser Netzwerktyp früher gestartet und möglicherweise vor anderen Startaufgaben beendet werden, die sich ebenfalls auf den Zustand der Instance auswirken können. Statusprüfungen, die von der Netzwerkverfügbarkeit abhängen, können einen fehlerfreien Status melden, bevor andere Aufgaben abgeschlossen sind.

Hier sind Beispiele für Probleme aufgeführt, die dazu führen können, dass Instance-Statusprüfungen fehlschlagen:

- Fehlgeschlagene System-Statusprüfungen
- Fehlerhafte Netzwerk- oder Startup-Konfiguration
- Unzureichender Speicher
- Beschädigtes Dateisystem

- Inkompatibler Kernel
- Während eines Neustarts meldet die Instance-Statusprüfung einen Fehler, bis die Instance wieder verfügbar ist.

Wenn eine Überprüfung des Instance-Status fehlschlägt, erhöhen wir die StatusCheckFailed_Instance-Metrik.

Bare Metal-Instances

Wenn Sie einen Neustart des Betriebssystems auf einer Bare-Metal-Instance durchführen, gibt die Instance-Statusprüfung möglicherweise vorübergehend einen Fehlerstatus zurück. Wenn die Instance verfügbar wird, sollte die Instance-Statusprüfung einen Passstatus zurückgeben.

Verknüpfte EBS-Statusprüfungen

Bei den Statusprüfungen von angehängten EBS wird überwacht, ob die an eine Instance angehängten Amazon EBS-Volumes erreichbar sind und Vorgänge abschließen I/O können. Bei der `StatusCheckFailed_AttachedEBS` Metrik handelt es sich um einen binären Wert, der auf eine Beeinträchtigung hinweist, wenn eines oder mehrere der der Instance zugeordnete EBS-Volumes nicht in der Lage sind, den Betrieb abzuschließen. I/O Diese Statusprüfungen erkennen grundlegende Probleme mit der Datenverarbeitungs- oder Amazon EBS-Infrastruktur. Wenn die angehängte EBS-Statusprüfmetrik fehlschlägt, können Sie entweder warten, AWS bis das Problem behoben ist, oder Sie können Maßnahmen ergreifen, z. B. die betroffenen Volumes austauschen oder die Instance beenden und neu starten.

Hier sind Beispiele für Probleme aufgeführt, die dazu führen können, dass angehängte EBS-Statusprüfungen fehlschlagen:

- Hardware- oder Softwareprobleme auf den Speichersubsystemen, die den EBS-Volumes zugrunde liegen
- Hardwareprobleme auf dem physischen Host, die die Erreichbarkeit der EBS-Volumes beeinträchtigen
- Verbindungsprobleme zwischen der Instance und den EBS-Volumes

Sie können die `StatusCheckFailed_AttachedEBS`-Metrik verwenden, um die Stabilität Ihres Workloads zu verbessern. Sie können diese Metrik verwenden, um CloudWatch Amazon-Alarme zu erstellen, die auf der Grundlage des Ergebnisses der Statusprüfung ausgelöst werden. Sie könnten

beispielsweise ein Failover auf eine sekundäre Instance oder Availability Zone durchführen, wenn Sie eine anhaltende Auswirkung feststellen. Alternativ können Sie alle I/O performance of each attached volume using EBS CloudWatch metrics to detect and replace the impaired volume. If your workload is not driving I/O an Ihre Instance angeschlossenen EBS-Volumes überwachen und die EBS-Statusprüfung weist auf eine Beeinträchtigung hin. Sie können die Instance beenden und starten, um sie auf einen neuen Host zu verschieben. Dadurch können die zugrunde liegenden Hostprobleme behoben werden, die sich auf die Erreichbarkeit der EBS-Volumes auswirken. Weitere Informationen finden Sie unter CloudWatch Amazon-Metriken für Amazon EBS.

Sie können Ihre Amazon EC2 Auto Scaling Scaling-Gruppen auch so konfigurieren, dass sie Fehler bei der angehängten EBS-Statusprüfung erkennen und dann die betroffene Instance durch eine neue ersetzen. Weitere Informationen finden Sie unter Überwachen und Ersetzen von Amazon EC2 Auto Scaling Scaling-Instances mit beeinträchtigten Amazon EBS-Volumes im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

> **Note**
>
> Die verknüpfte EBS-Statusprüfungsmetrik ist nur für Nitro-Instances verfügbar.

Statuschecks für EC2 Amazon-Instances anzeigen

Wenn Ihre Instance eine nicht bestandene Statusprüfung aufweist, müssen Sie das Problem normalerweise selbst lösen (z. B. per Neustart der Instance oder durch das Vornehmen von Konfigurationsänderungen für die Instance). Informationen zur Problembehandlung für System- oder Instance-Statusprüfungen erhalten Sie unter Problembehandlung bei Amazon EC2 Linux-Instances mit fehlgeschlagenen Statusprüfungen.

Console

Anzeigen der Statusprüfungen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Auf der Seite Instances ist in der Spalte Statusprüfungen jeweils der Betriebszustand einer Instance angegeben.
4. Wählen Sie die Instance aus, um ihren Status anzuzeigen, und wählen Sie anschließend die Registerkarte Status und Alarme.

5. Um die CloudWatch Messwerte für Statuschecks zu überprüfen, erweitern Sie auf der Registerkarte Status und Alarme die Option Metriken, um die Grafiken für die folgenden Messwerte anzuzeigen:

   - Statusprüfung für System fehlgeschlagen
   - Statusprüfung für Instance fehlgeschlagen
   - Die Statusüberprüfung für das angefügte EBS ist fehlgeschlagen

   Weitere Informationen finden Sie unter the section called “Statusprüfungsmetriken”.

AWS CLI

Anzeigen der Statusprüfungen

Verwenden Sie den Befehl describe-instance-status.

Beispiel: Rufen Sie den Status aller laufenden Instances ab

```
aws ec2 describe-instance-status
```

Beispiel: Rufen Sie den Status aller Instances ab

```
aws ec2 describe-instance-status --include-all-instances
```

Beispiel: Rufen Sie den Status einer einzelnen laufenden Instance ab

```
aws ec2 describe-instance-status --instance-ids i-1234567890abcdef0
```

Beispiel: Rufen Sie alle Instances mit dem Status `impaired` ab

```
aws ec2 describe-instance-status \
--filters Name=instance-status.status,Values=impaired
```

PowerShell

Anzeigen der Statusprüfungen

Verwenden Sie den Befehl Get-EC2InstanceStatus.

Beispiel: Rufen Sie den Status aller laufenden Instances ab

```
Get-EC2InstanceStatus
```

Beispiel: Rufen Sie den Status aller Instances ab

```
Get-EC2InstanceStatus -IncludeAllInstance $true
```

Beispiel: Rufen Sie den Status einer einzelnen laufenden Instance ab

```
Get-EC2InstanceStatus -InstanceId i-1234567890abcdef0
```

Beispiel: Rufen Sie alle Instances mit dem Status `impaired` ab

```
Get-EC2InstanceStatus \
-Filter @{Name="instance-status.status"; Values="impaired"}
```

CloudWatch Alarme für EC2 Amazon-Instances erstellen, die Statusprüfungen nicht bestehen

Sie können die Metriken für die Statusprüfung verwenden, um CloudWatch Alarme zu erstellen, die Sie benachrichtigen, wenn die Statusprüfung einer Instanz fehlgeschlagen ist.

Alarme bei Statusprüfungen können vorübergehend in den Status ungenügend Daten wechseln, wenn metrische Datenpunkte fehlen. Dies ist zwar selten, kann aber passieren, wenn es zu einer Unterbrechung der metrischen Berichtssysteme kommt, selbst wenn eine Instance fehlerfrei ist. Wir empfehlen, diesen Status als fehlende Daten zu behandeln und nicht als Fehlschlag bei der Statusüberprüfung oder als Alarmverletzung. Dies ist besonders wichtig, wenn als Reaktion Aktionen zum Anhalten, Beenden, Neustarten oder Wiederherstellen der Instance ausgeführt werden.

Console

In diesem Beispiel wird ein Alarm konfiguriert, der eine Benachrichtigung sendet, wenn eine Instance eine Statusprüfung nicht besteht. Sie können die Instance optional anhalten, beenden oder wiederherstellen.

So erstellen Sie einen Statusprüfungsalarm

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance, dann die Registerkarte Statusprüfungen und Aktionen, Statusprüfalarm erstellen aus.
4. Wählen Sie auf der Seite CloudWatch Alarme verwalten unter Alarm hinzufügen oder bearbeiten die Option Alarm erstellen.
5. Aktivieren Sie für Alarmbenachrichtigung den Schalter, um Amazon Simple Notification Service (Amazon SNS) -Benachrichtigungen zu konfigurieren. Wählen Sie ein vorhandenes Amazon SNS-Thema aus oder geben Sie einen Namen ein, um ein neues Thema zu erstellen.

   Wenn Sie der Liste der Empfänger eine E-Mail-Adresse hinzufügen oder ein neues Thema erstellen, sendet Amazon SNS an jede neue Adresse eine Bestätigungs-E-Mail. Jeder Empfänger muss den Bestätigungslink in der E-Mail auswählen. Benachrichtigungen über Alarme werden nur an bestätigte Adressen gesendet.
6. Aktivieren Sie für Alarmaktion den Schalter, um eine Aktion anzugeben, die ausgeführt werden soll, wenn der Alarm ausgelöst wird. Wählen Sie die Aktion aus.
7. Wählen Sie unter larm thresholds (Alarmschwellenwerte) die Metrik und Kriterien für den Alarm aus.

   Sie können die Standardeinstellungen für Beispiele gruppieren nach (Durchschnitt) und für Datentypen für die Probenahme (Statusprüfung failed:either) übernehmen oder an Ihre Anforderungen anpassen.

   Legen Sie unter Consecutive period (Kontinuierlicher Zeitraum) die Anzahl von Zeiträumen fest, die ausgewertet werden sollen, und wählen Sie unter Period (Zeitraum) die Dauer des Auswertungszeitraums aus, nach dem der Alarm ausgelöst und eine E-Mail gesendet wird.
8. (Optional) Wählen Sie für Beispiel-Metrikdaten die Option Zu Dashboard hinzufügen aus.
9. Wählen Sie Erstellen aus.

Falls Sie Änderungen an einem Alarm zum Instance-Status vornehmen möchten, können Sie ihn bearbeiten.

Erstellen eines Ereignisfensters

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.

3. Wählen Sie die Instance aus und wählen Sie Aktionen, Überwachung, CloudWatchAlarme verwalten aus.
4. Wählen Sie auf der Seite CloudWatch Alarme verwalten unter Alarm hinzufügen oder bearbeiten die Option Alarm bearbeiten aus.
5. Wählen Sie unter Search for alarm (Alarmsuche) den Alarm aus.
6. Wenn Sie die Änderungen vorgenommen haben, wählen Sie Update (Aktualisieren) aus.

AWS CLI

Im folgenden Beispiel veröffentlicht der Alarm eine Benachrichtigung an das SNS-Thema, wenn die Instance entweder die Instance- oder die System-Statusprüfung in mindestens zwei aufeinanderfolgenden Zeiträumen nicht besteht. Die verwendete CloudWatch Metrik ist`StatusCheckFailed`.

So erstellen Sie einen Statusprüfungsalarm

1. Wählen Sie ein vorhandenes SNS-Thema aus oder erstellen Sie ein neues Thema. Weitere Informationen finden Sie unter Zugriff auf Amazon SNS in der AWS CLI im Benutzerhandbuch für AWS Command Line Interface .
2. Verwenden Sie den folgenden Befehl list-metrics, um die verfügbaren CloudWatch Amazon-Metriken für Amazon anzuzeigen. EC2

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

3. Verwenden Sie den folgenden put-metric-alarmBefehl, um den Alarm zu erstellen.

```
aws cloudwatch put-metric-alarm \
    --alarm-name StatusCheckFailed-Alarm-for-i-1234567890abcdef0 \
    --metric-name StatusCheckFailed \
    --namespace AWS/EC2 \
    --statistic Maximum \
    --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
    --unit Count \
    --period 300 \
    --evaluation-periods 2 \
    --threshold 1 \
    --comparison-operator GreaterThanOrEqualToThreshold \
    --alarm-actions arn:aws:sns:us-west-2:111122223333:my-sns-topic
```

Der Zeitraum ist der Zeitraum in Sekunden, in dem CloudWatch Amazon-Metriken erfasst werden. Im Beispiel wird der Wert 300 verwendet, also 60 Sekunden multipliziert mit 5 Minuten. Die Bewertungsperiode ist die Anzahl von aufeinanderfolgenden Zeiträumen, für die der Wert der Metrik mit dem Schwellenwert verglichen werden muss. In diesem Beispiel wird der Wert 2 verwendet. Die Alarmaktionen sind die Aktionen, die durchgeführt werden sollen, wenn dieser Alarm ausgelöst wird.

PowerShell

So erstellen Sie einen Statusprüfungsalarm

Verwenden Sie das Cmdlet CWMetric Write-Alarm wie folgt, um Benachrichtigungen zu einem SNS-Thema zu veröffentlichen, wenn die Instance die Statusprüfungen für mindestens zwei aufeinanderfolgende Zeiträume nicht bestanden hat.

```
Write-CWMetricAlarm `
    -AlarmName "StatusCheckFailed-Alarm-for-i-1234567890abcdef0" `
    -MetricName "StatusCheckFailed" `
    -Namespace "AWS/EC2" `
    -Statistic "Maximum" `
    -Dimension @{Name="InstanceId"; Values="i-1234567890abcdef0"} `
    -Unit "Count" `
    -Period 300 `
    -EvaluationPeriod 2 `
    -Threshold 1 `
    -ComparisonOperator "GreaterThanOrEqualToThreshold" `
    -AlarmAction "arn:aws:sns:us-west-2:111122223333:my-sns-topic"
```

Der Zeitraum ist der Zeitraum in Sekunden, in dem CloudWatch Amazon-Metriken erfasst werden. Im Beispiel wird der Wert 300 verwendet, also 60 Sekunden multipliziert mit 5 Minuten. Die Bewertungsperiode ist die Anzahl von aufeinanderfolgenden Zeiträumen, für die der Wert der Metrik mit dem Schwellenwert verglichen werden muss. In diesem Beispiel wird der Wert 2 verwendet. Die Alarmaktionen sind die Aktionen, die durchgeführt werden sollen, wenn dieser Alarm ausgelöst wird.

Ereignisse zur Statusänderung für EC2 Amazon-Instances

Amazon EC2 sendet ein `EC2 Instance State-change Notification` Ereignis an Amazon, EventBridge wenn sich der Status einer Instance ändert.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis. In diesem Beispiel ist die Instance in den `pending`-Status übergegangen.

```
{
   "id":"7bf73129-1428-4cd3-a780-95db273d1602",
   "detail-type":"EC2 Instance State-change Notification",
   "source":"aws.ec2",
   "account":"123456789012",
   "time":"2021-11-11T21:29:54Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
   ],
   "detail":{
      "instance-id":"i-1234567890abcdef0",
      "state":"pending"
   }
}
```

Die möglichen Werte für `state` sind:

- `pending`
- `running`
- `stopping`
- `stopped`
- `shutting-down`
- `terminated`

Wenn Sie eine Instance starten, geht sie zunächst in den `pending`-Status und dann in den `running`-Status über. Wenn Sie eine Instance stoppen, geht sie in den `stopping`-Status und dann in den `stopped`-Status über. Wenn Sie eine Instance beenden, geht sie in den `shutting-down`-Status und dann in den `terminated`-Status über. Weitere Informationen finden Sie unter Amazon-EC2-Instance-Statusänderungen.

Erstellen Sie einen Alarm, der eine E-Mail sendet, wenn sich der Status einer EC2 Amazon-Instance ändert

Um E-Mail-Benachrichtigungen zu erhalten, wenn sich der Status Ihrer Instance ändert, erstellen Sie ein Amazon SNS SNS-Thema und dann eine EventBridge Regel für das `EC2 Instance State-change Notification` Ereignis.

So erstellen Sie ein SNS-Thema

1. Öffnen Sie die Amazon SNS SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie im Navigationsbereich Themen aus.
3. Wählen Sie Thema erstellen aus.
4. Wählen Sie unter Type (Typ) die Option Standard aus.
5. Geben Sie unter Name einen Namen für Ihr Thema ein.
6. Wählen Sie Thema erstellen aus.
7. Wählen Sie Create subscription (Abonnement erstellen) aus.
8. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus.
9. Geben Sie unter Endpoint (Endpunkt) die E-Mail-Adresse ein, an die die Benachrichtigungen gesendet werden sollen.
10. Wählen Sie Create subscription (Abonnement erstellen) aus.
11. Sie erhalten eine E-Mail-Nachricht mit der folgenden Betreffzeile: AWS Notification - Subscription Confirmation. Befolgen Sie die Anweisungen, um Ihr Abonnement zu bestätigen.

Um eine Regel zu erstellen EventBridge

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie Regel erstellen aus.
3. Geben Sie unter Name einen Namen für Ihre Regel ein.
4. Bei Regeltyp wählen Sie Regel mit einem Ereignismuster aus.
5. Wählen Sie Weiter aus.
6. Bei Build event pattern (Ereignis-Muster erstellen) gehen Sie wie folgt vor:
   a. Wählen Sie für Ereignisquelle die Option AWS-Services aus.

b. Wählen Sie für AWS-Service EC2 aus.

c. Wählen Sie in Event Type (Ereignistyp) EC2 EC2 Instance State-change Notification (Benachrichtigung über die Statusänderung der EC2-Instance) aus.

d. Standardmäßig senden wir Benachrichtigungen für jede Statusänderung für jede Instance. Wenn Sie möchten, können Sie bestimmte Status oder bestimmte Instances auswählen.

7. Wählen Sie Weiter aus.
8. Geben Sie ein Ziel wie folgt an:

   a. Für Target types (Zieltypen), wählen Sie AWS-Service aus.

   b. Für Select a target (Wählen Sie ein Ziel aus), wählen Sie SNS-Thema aus.

   c. Wählen Sie für Topic (Thema) das SNS-Thema aus, das Sie im vorherigen Verfahren erstellt haben.

9. Wählen Sie Weiter aus.
10. (Optional) Fügen Sie Ihrer Regel Tags hinzu.
11. Wählen Sie Weiter aus.
12. Wählen Sie Regel erstellen aus.
13. Um Ihre Regel zu testen, initiieren Sie eine Statusänderung. Starten Sie beispielsweise eine gestoppte Instance, beenden Sie eine laufende Instance oder starten Sie eine Instance. Sie erhalten E-Mail-Nachrichten mit der folgenden Betreffzeile: AWS Notification Message. Der Text der E-Mail enthält die Ereignisdaten.

Geplante Ereignisse für EC2 Amazon-Instances

Um die Zuverlässigkeit und Leistung der Infrastruktur zu gewährleisten, AWS können Sie Ereignisse planen, um Ihre Instances neu zu starten, zu beenden und außer Betrieb zu nehmen. Diese Ereignisse treten nicht häufig auf.

Wenn eine Ihrer Instances von einem geplanten Ereignis betroffen sein wird, werden Sie vorab per E-Mail an die mit Ihrem AWS Konto verknüpfte E-Mail-Adresse AWS benachrichtigt. Die E-Mail enthält Details zum Ereignis, z. B. das Start- und Enddatum. Je nach Art des Ereignisses können Sie möglicherweise Maßnahmen ergreifen, um den Zeitpunkt des Ereignisses zu steuern. AWS sendet auch ein AWS Health Ereignis, das Sie mithilfe von Amazon überwachen und verwalten können EventBridge. Weitere Informationen finden Sie unter Ereignisse AWS Health mit Amazon überwachen EventBridge.

Geplante Ereignisse werden von verwaltet AWS. Sie können keine Ereignisse für Ihre Instances planen. Sie können jedoch:

- Geplante Ereignisse für Ihre Instances anzeigen.
- Benachrichtigungen für geplante Ereignisse so anpassen, dass Tags in die E-Mail-Benachrichtigung aufgenommen werden oder aus dieser entfernt werden.
- Bestimmte geplante Ereignisse verschieben.
- Benutzerdefinierte Ereignisfenster für geplante Ereignisse erstellen.
- Ergreifen Sie Maßnahmen, wenn für eine Instance ein Neustart, eine Anhaltung oder eine Außerbetriebnahme geplant ist.

Um sicherzustellen, dass Sie Benachrichtigungen über geplante Ereignisse erhalten, überprüfen Sie Ihre Kontaktinformationen auf der Kontoseite.

> **Note**
>
> Wenn eine Instance von einem geplanten Ereignis betroffen ist und Teil einer Amazon EC2 Auto Scaling-Gruppe ist, ersetzt Amazon EC2 Auto Scaling sie irgendwann im Rahmen seiner Zustandsprüfungen, ohne dass weitere Maßnahmen Ihrerseits erforderlich sind. Weitere Informationen zu den von Amazon EC2 Auto Scaling durchgeführten Zustandsprüfungen finden Sie unter Zustandsprüfungen für Instances in einer Amazon EC2 Auto Scaling Scaling-Gruppe im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Arten von geplanten Ereignissen

Amazon EC2 kann die folgenden Arten von geplanten Ereignissen für Ihre Instances erstellen, wobei das Ereignis zu einem geplanten Zeitpunkt stattfindet:

Ereignistyp	Ereigniscode	Ereignisaktion
Instance anhalten	`instance-stop`	Die Instance wird zur geplanten Zeit angehalten. Wenn Sie sie wieder starten, wird sie zu einem neuen Host migriert. Gilt nur für Instances

Ereignistyp	Ereigniscode	Ereignisaktion
		mit einem Amazon-EBS-Root-Volume.
Ausmusterung einer Instance	`instance-retirement`	Die Instance wird zur geplanten Zeit angehalten, wenn sie über ein Amazon-EBS-Root-Volume verfügt, oder beendet, wenn sie über ein Instance-Speicher-Root-Volume verfügt.
Instance-Neustart	`instance-reboot`	Die Instance wird zur geplanten Zeit neu gestartet. Die Instance verbleibt auf dem Host, und während des Neustarts wird der Host gewartet. Dies wird als direkter Neustart bezeichnet.
Systemneustart	`system-reboot`	Die Instance wird zur geplanten Zeit neu gestartet und zu einem neuen Host migriert. Dies wird als Neustart-Migration bezeichnet.
Systemwartung	`system-maintenance`	Zur geplanten Zeit kann die Instance vorübergehend von der Wartung des Netzwerks oder der Stromversorgung betroffen sein.

Den Ereignistyp bestimmen

Sie können überprüfen, welche Art von Ereignis für Ihre Instance geplant ist.

Console

So bestimmen Sie den Ereignistyp

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Events.
3. In der Tabelle wird der Ereigniscode in der Spalte Ereignistyp angezeigt.
4. Um die Tabelle so zu filtern, dass nur die Ereignisse für Instances angezeigt werden, wählen Sie im Suchfeld Ressourcentyp: Instance aus der Filterliste aus.

AWS CLI

So ermitteln Sie den Ereignistyp für eine Instance

Verwenden Sie den Befehl describe-instance-status. Wenn der Instance ein geplantes Ereignis zugeordnet ist, enthält die Ausgabe Informationen über das geplante Ereignis.

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0 \
    --query InstanceStatuses[].Events
```

Es folgt eine Beispielausgabe. Der Code für das geplante Ereignis lautet `system-reboot`.

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0d59937288b749b32",
            "Code": "system-reboot",
            "Description": "The instance is scheduled for a reboot",
            "NotAfter": "2020-03-14T22:00:00.000Z",
            "NotBefore": "2020-03-14T20:00:00.000Z",
            "NotBeforeDeadline": "2020-04-05T11:00:00.000Z"
        }
    ]
]
```

PowerShell

So ermitteln Sie den Ereignistyp für eine Instance

Verwenden Sie das cmdlet Get-EC2InstanceStatus. Wenn der Instance ein geplantes Ereignis zugeordnet ist, enthält die Ausgabe Informationen über das geplante Ereignis.

```
(Get-EC2InstanceStatus `
    -InstanceId i-1234567890abcdef0).Events
```

Es folgt eine Beispielausgabe. Der Code für das geplante Ereignis lautet `system-reboot`.

```
Code              : system-reboot
Description       : The instance is scheduled for a reboot
InstanceEventId   : instance-event-0d59937288b749b32
NotAfter          : 2020-03-14T22:00:00.000Z
NotBefore         : 2020-03-14T20:00:00.000Z
NotBeforeDeadline : 2020-04-05T11:00:00.000Z
```

Inhalt

- EC2 Amazon-Instances verwalten, deren Stopp oder Stilllegung geplant ist
- EC2 Amazon-Instances verwalten, die für den Neustart geplant sind
- EC2 Amazon-Instances verwalten, für die Wartung geplant ist
- Geplante Ereignisse anzeigen, die sich auf Ihre EC2 Amazon-Instances auswirken
- Passen Sie Benachrichtigungen über geplante Ereignisse für Ihre Instanzen an EC2
- Planen Sie ein geplantes Ereignis für eine Instanz neu EC2
- Erstellen Sie benutzerdefinierte Ereignisfenster für geplante Ereignisse, die sich auf Ihre EC2 Amazon-Instances auswirken

EC2 Amazon-Instances verwalten, deren Stopp oder Stilllegung geplant ist

Wenn ein AWS irreparabler Ausfall des zugrunde liegenden Hosts für Ihre Instance festgestellt wird, wird die Instance so geplant, dass sie je nach Root-Volume-Typ der Instance entweder beendet oder beendet wird.

- Wenn die Instance ein Amazon-EBS-Root-Volume hat, wird für die Instance das Anhalten geplant.
- Wenn die Instance ein Instance-Speicher-Root-Volume hat, wird für die Instance das Beenden geplant.

Weitere Informationen finden Sie unter Ausmusterung einer Instance.

> **Important**
>
> Alle Daten, die auf Instance-Speicher-Volumes gespeichert sind, gehen verloren, wenn eine Instance angehalten, in den Ruhezustand versetzt oder beendet wird. Dies gilt auch für Instance-Speicher-Volumes, die an eine Instance mit einem EBS-Root-Volume angehängt sind. Achten Sie darauf, dass Sie Daten von Ihren Instance-Speicher-Volumes speichern, die Sie später möglicherweise noch benötigen, bevor die Instance angehalten, in den Ruhezustand versetzt oder beendet wird.

Aktionen, die Sie ausführen können:

Aktionen, die Sie für Instances mit einem EBS-Root-Volume ausführen können

Wenn Sie eine Benachrichtigung über ein geplantes `instance-stop`-Ereignis erhalten, können Sie eine der folgenden Aktionen ausführen:

- Warten auf geplantes Anhalten: Sie können warten, bis die Instance innerhalb ihres geplanten Wartungsfensters angehalten wird.
- Manuelles Anhalten und Starten durchführen: Sie können die Instance zu einem geeigneten Zeitpunkt selbst anhalten und starten. Sie wird dann zu einem neuen Host migriert. Das ist nicht dasselbe wie ein Neustart der Instance. Weitere Informationen finden Sie unter Stoppen und starten Sie EC2 Amazon-Instances.
- Anhalten und Starten automatisieren: Sie können ein sofortiges Anhalten und Starten in Reaktion auf ein geplantes `instance-stop`-Ereignis automatisieren. Weitere Informationen finden Sie im AWS Health Benutzerhandbuch unter Automatisches Ausführen von Vorgängen auf EC2 Instances als Reaktion AWS Health auf Ereignisse.

Aktionen, die Sie für Instances mit einem Instance-Speicher-Root-Volume ausführen können

Wenn Sie eine Benachrichtigung über ein geplantes `system-retirement`-Ereignis erhalten und Ihre Daten beibehalten möchten, können Sie eine der folgenden Aktionen ausführen:

1. Starten Sie eine Ersatz-Instance aus Ihrem neuesten AMI.
2. Migrieren Sie alle notwendigen Daten zur Ersatz-Instance, bevor für die Instance das Beenden geplant ist.
3. Beenden Sie die ursprüngliche Instance oder warten Sie, bis sie wie geplant beendet wird.

Weitere Informationen über die Maßnahmen, die Sie ergreifen können, finden Sie unter Ausmusterung einer Instance.

EC2 Amazon-Instances verwalten, die für den Neustart geplant sind

Wenn Aufgaben wie die Installation von Updates oder die Wartung des zugrunde liegenden Hosts ausgeführt werden AWS müssen, kann es einen Instance-Neustart planen. Während des geplanten Neustarts bleibt die Instance je nach Ereignis entweder auf demselben Host oder migriert wie folgt auf einen anderen Host:

- `instance-reboot` event
  - Während des Neustarts verbleibt die Instance auf dem Host. Dies wird als direkter Neustart bezeichnet.
  - Der aktuelle Host wird gewartet.
  - In der Regel innerhalb von Sekunden abgeschlossen.
- `system-reboot` event
  - Die Instance wird während des Neustarts zu einem neuen Host migriert. Dies wird als Neustart-Migration bezeichnet.
  - In der Regel innerhalb von wenigen Minuten abgeschlossen.

Informationen zum Überprüfen, welche Ereignistyp für Ihre Instance geplant ist, finden Sie unter Den Ereignistyp bestimmen.

Aktionen, die Sie ausführen können:

Wenn Sie eine Benachrichtigung über ein geplantes `instance-reboot`- oder `system-reboot`-Ereignis erhalten, können Sie eine der folgenden Aktionen ausführen:

- Warten auf geplanten Neustart: Sie können warten, bis die Instance innerhalb ihres geplanten Wartungsfensters neu gestartet wird.
- Neustart verschieben: Sie können den Instance-Neustart auf ein geeignetes Datum um eine geeignete Uhrzeit verschieben.
- Einen vom Benutzer initiierten Neustart durchführen: Sie können die Instance zu einem für Sie passenden Zeitpunkt manuell neu starten. Das Ergebnis hängt jedoch vom Ereignis ab:
  - `instance-reboot`-Ereignis – Ihre Instance bleibt auf der aktuellen Hardware (direkter Neustart), es findet keine Host-Wartung statt und das Ereignis bleibt geöffnet.

- `system-reboot` event
  - Wenn die Neustart-Migration auf Ihrer Instance aktiviert ist, versucht ein vom Benutzer initiierter Neustart, Ihre Instance auf neue Hardware zu migrieren. Bei Erfolg wird das Ereignis gelöscht. Wenn dies nicht gelingt, erfolgt ein direkter Neustart und das Ereignis bleibt geplant.
  - Wenn die Neustartmigration auf Ihrer Instance deaktiviert ist, bleibt die Instance bei einem vom Benutzer initiierten Neustart auf derselben Hardware (direkter Neustart), es findet keine Host-Wartung statt und das Ereignis bleibt geplant. Wenn das geplante Ereignis irgendwann stattfindet, AWS wird Ihre Instance auf neue Hardware verschoben (Neustart-Migration).

Nach dem AWS Neustart Ihrer Instanz

Nach dem AWS Neustart Ihrer Instance gilt Folgendes:

- Das geplante Ereignis wird gelöscht.
- Die Beschreibung des Ereignisses wird aktualisiert.
- Für ein `instance-reboot`-Ereignis:
  - Die Wartung des zugrunde liegenden Hosts ist abgeschlossen.
- Für ein `system-reboot`-Ereignis:
  - Die Instance wird auf einen neuen Host verlagert.
  - Die Instance behält ihre IP-Adresse und ihren DNS-Namen bei.
  - Die Daten auf den lokalen Instance-Speicher-Volumes werden beibehalten.
- Sie können Ihre Instance verwenden, nachdem sie vollständig hochgefahren ist.

Alternative Optionen

Wenn Sie das Neustart-Ereignis nicht verschieben oder die Neustart-Migration für einen vom Benutzer initiierten Neustart nicht aktivieren können, Sie aber während des geplanten Wartungsfensters den normalen Betrieb beibehalten möchten, können Sie wie folgt vorgehen:

- Für eine Instance mit einem EBS-Root-Volume
  - Halten Sie Sie die Instance manuell an und starten Sie sie, um sie auf einen neuen Host zu migrieren. Dies ist nicht dasselbe wie ein manuelles Neustarten der Instance, bei dem die Instance auf demselben Host verbleibt.
  - Optional können Sie auch ein sofortiges Anhalten und Starten der Instance in Reaktion auf ein geplantes Neustart-Ereignis automatisieren. Weitere Informationen finden Sie im AWS Health

Benutzerhandbuch unter Automatisches Ausführen von Vorgängen auf EC2 Instances als Reaktion auf Ereignisse. AWS Health

> **Important**
>
> Die Daten auf den Instance-Speicher-Volumes gehen verloren, wenn die Instance angehalten wird. Weitere Informationen finden Sie unter Stoppen und starten Sie EC2 Amazon-Instances.

- Für eine Instance mit einem Instance-Speicher-Root-Volume
  1. Starten Sie eine Ersatz-Instance aus Ihrem neuesten AMI.
  2. Migrieren Sie vor dem geplanten Wartungsfenster alle notwendigen Daten zur Ersatz-Instance.
  3. Beenden Sie die ursprüngliche Instance.

Aktivieren bzw. deaktivieren Sie die Neustart-Migration

Wenn eine Instance für ein `system-reboot`-Ereignis geplant ist, können Sie sie vor dem Ereignis neu starten. Das Ergebnis eines vom Benutzer initiierten Neustarts hängt von den Einstellungen für die Neustart-Migration der Instance ab:

- Aktiviert – Ein vom Benutzer initiierter Neustart versucht, Ihre Instance auf neue Hardware zu migrieren (Neustart-Migration). Bei Erfolg wird das Ereignis gelöscht. Wenn dies nicht gelingt, erfolgt ein direkter Neustart und das Ereignis bleibt geplant. Beachten Sie, dass die Neustart-Migration auch bei Aktivierung nur erfolgen kann, wenn Ihre Instance die Anforderungen für die Neustart-Migration erfüllt.
- Deaktiviert – Bei einem vom Benutzer initiierten Neustart bleibt die Instance auf derselben Hardware (direkter Neustart), es findet keine Host-Wartung statt und das Ereignis bleibt geplant. Wenn das geplante Ereignis irgendwann stattfindet, AWS wird Ihre Instanz auf neue Hardware verschoben (Neustart-Migration).

Ein Neustart mit Migration dauert länger als ein direkter Neustart:

- Direkter Neustart: Ungefähr 30 Sekunden
- Neustart mit Migration: Einige Minuten

> **Note**
>
> Instances, die eine `system-reboot`-Ereignisbenachrichtigung erhalten, sind standardmäßig für die vom Benutzer initiierte Neustart-Migration aktiviert.

Anforderungen für die Aktivierung der Neustart-Migration

Die Neustart-Migration kann für Instances aktiviert werden, die die folgenden Kriterien erfüllen:

Instance-Typen

Nicht alle Instance-Typen unterstützen die Aktivierung der Neustart-Migration. Sie können die Instance-Typen anzeigen, die die Aktivierung der Neustart-Migration unterstützen.

Console

So zeigen Sie die Instance-Typen an, die die Aktivierung der Neustart-Migration unterstützen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich Instance Types (Instance-Typen) aus.
3. Geben Sie in der Filterleiste Reboot Migration support: supported ein. Während Sie die Zeichen eingeben erscheint der Filtername und Sie können ihn auswählen.

   Die Tabelle Instance-Typen zeigt alle Instance-Typen, die die Aktivierung der Neustart-Migration unterstützen.

AWS CLI

So zeigen Sie die Instance-Typen an, die die Aktivierung der Neustart-Migration unterstützen

Verwenden Sie den Befehl describe-instance-types mit dem Filter `reboot-migration-support`.

```
aws ec2 describe-instance-types \
    --filters Name=reboot-migration-support,Values=supported \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

PowerShell

So zeigen Sie die Instance-Typen an, die die Aktivierung der Neustart-Migration unterstützen

Verwenden Sie das Get-EC2InstanceTypeCmdlet mit dem `reboot-migration-support` Filter.

```
Get-EC2InstanceType `
    -Filter @{Name="reboot-migration-support";Values="true"} | `
    Select InstanceType | Sort-Object InstanceType
```

Tenancy

- Freigegeben
- Dedicated Instance

Weitere Informationen finden Sie unter Amazon-EC2-Dedicated-Instances.

Einschränkungen

Die Neustart-Migration wird für Instances mit den folgenden Merkmalen nicht unterstützt:

- Plattform: Instances, die nativ auf dem Xen-Hypervisor ausgeführt werden
- Instance-Größe: `metal`-Instances
- Tenancy: Dedicated Host. Verwenden Sie für Dedicated Hosts stattdessen Dedicated Host Auto Recovery.
- Speicher: Instances mit Instance-Speicher-Volumes
- Netzwerke: Instances, die einen Elastic Fabric Adapter verwenden
- Auto Scaling: Instances, die Teil einer Amazon EC2 Auto Scaling Scaling-Gruppe sind

Schritte zum Aktivieren oder Deaktivieren der Neustart-Migration

Wenn eine Instance ein `system-reboot`-Ereignis empfängt, ist sie standardmäßig für die Neustart-Migration aktiviert. Sie können die Neustartmigration deaktivieren, sodass die Instance bei einem vom Benutzer initiierten Neustart auf derselben Hardware bleibt (direkter Neustart).

Die `default`-Konfiguration ermöglicht keine Neustart-Migration für eine nicht unterstützte Instance. Weitere Informationen finden Sie unter Anforderungen für die Aktivierung der Neustart-Migration.

Sie können die Neustart-Migration für eine laufende oder angehaltene Instance deaktivieren oder aktivieren.

AWS CLI

So deaktivieren Sie die Neustart-Migration

Verwenden Sie den modify-instance-maintenance-optionsBefehl und setzen Sie den `--reboot-migration` Parameter auf`disabled`.

```
aws ec2 modify-instance-maintenance-options \

    --instance-id i-0abcdef1234567890 \

    --reboot-migration disabled
```

So aktivieren Sie die Neustart-Migration

Verwenden Sie den modify-instance-maintenance-optionsBefehl und setzen Sie den `--reboot-migration` Parameter auf`default`.

```
aws ec2 modify-instance-maintenance-options \

    --instance-id i-0abcdef1234567890 \

    --reboot-migration default
```

PowerShell

So deaktivieren Sie die Neustart-Migration

Verwenden Sie das cmdlet Edit-EC2InstanceMaintenanceOption.

```
Edit-EC2InstanceMaintenanceOption `
    -InstanceId  `
    -RebootMigration Disabled
```

So aktivieren Sie die Neustart-Migration

Verwenden Sie das cmdlet Edit-EC2InstanceMaintenanceOption.

```
Edit-EC2InstanceMaintenanceOption `
```

```
    -InstanceId i-1234567890abcdef0 `
    -RebootMigration Enabled
```

EC2 Amazon-Instances verwalten, für die Wartung geplant ist

Wenn der zugrundeliegende Host für eine Instance gewartet werden AWS muss, plant es die Wartung der Instance. Es gibt zwei Arten von Wartungsereignissen: Netzwerkwartung und Stromversorgungswartung.

- Bei der Netzwerkwartung wird die Netzwerkverbindung von geplanten Instances kurz unterbrochen. Die normale Netzwerkverbindung wird für Ihre Instance wiederhergestellt, nachdem die Wartung abgeschlossen ist.
- Bei der Stromversorgungswartung werden geplante Instances kurz in den Offlinezustand versetzt und dann neu gestartet. Wenn ein Neustart durchgeführt wird, werden alle Konfigurationseinstellungen Ihrer Instance beibehalten.

Überprüfen Sie nach dem Neustart Ihrer Instance (normalerweise nach nur wenigen Minuten), ob Ihre Anwendung wie erwartet funktioniert. An diesem Punkt sollte der Instance kein geplantes Ereignis mehr zugeordnet sein oder falls doch, sollte die Beschreibung des geplanten Ereignisses mit [Completed] ([Abgeschlossen]) beginnen. Es kann manchmal bis zu einer Stunde dauern, bis die Beschreibung des Instance-Status aktualisiert wird. Abgeschlossene Wartungsereignisse werden bis zu einer Woche lang auf dem Dashboard der EC2 Amazon-Konsole angezeigt.

Aktionen, die Sie ausführen können:

Aktionen, die Sie für Instances mit einem EBS-Root-Volume ausführen können

Wenn Sie eine `system-maintenance`-Ereignisbenachrichtigung erhalten, können Sie eine der folgenden Aktionen ausführen:

- Auf die geplante Wartung warten: Sie können warten, bis die Wartung wie geplant durchgeführt wird.
- Manuelles Anhalten und Starten durchführen: Sie können die Instance selbst anhalten und starten, wodurch sie zu einem neuen Host migriert wird. Das ist nicht dasselbe wie ein Neustart der Instance. Weitere Informationen finden Sie unter Stoppen und starten Sie EC2 Amazon-Instances.
- Anhalten und Starten automatisieren: Sie können ein sofortiges Anhalten und Starten in Reaktion auf ein geplantes Wartungsereignis automatisieren. Weitere Informationen finden Sie im AWS

Health Benutzerhandbuch unter Automatisches Ausführen von Vorgängen auf EC2 Instances als Reaktion auf Ereignisse. AWS Health

Aktionen, die Sie für Instances mit einem Instance-Speicher-Root-Volume ausführen können

Wenn Sie eine `system-maintenance`-Ereignisbenachrichtigung erhalten, können Sie eine der folgenden Aktionen ausführen:

- Auf die geplante Wartung warten: Sie können warten, bis die Wartung wie geplant durchgeführt wird.
- Ersatz-Instance starten: Wenn Sie während des geplanten Wartungsfensters den normalen Betrieb aufrechterhalten möchten:
  1. Starten Sie eine Ersatz-Instance aus Ihrem neuesten AMI.
  2. Migrieren Sie vor dem geplanten Wartungsfenster alle notwendigen Daten zur Ersatz-Instance.
  3. Beenden Sie die ursprüngliche Instance.

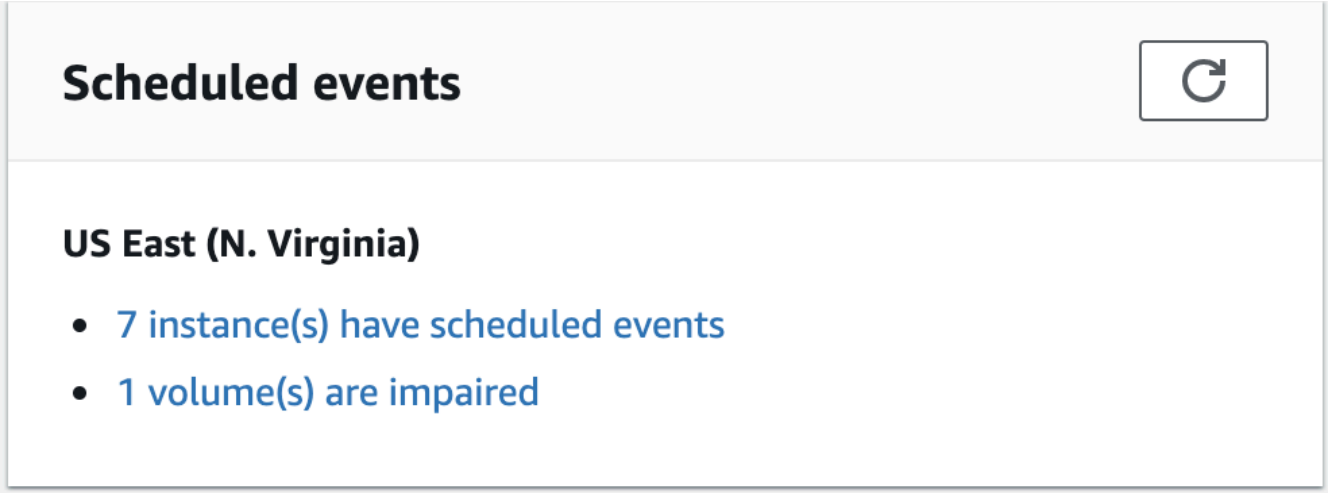
Geplante Ereignisse anzeigen, die sich auf Ihre EC2 Amazon-Instances auswirken

Zusätzlich zum Erhalt von Benachrichtigungen über geplante Ereignisse per E-Mail können Sie auch geplante Ereignisse überprüfen.

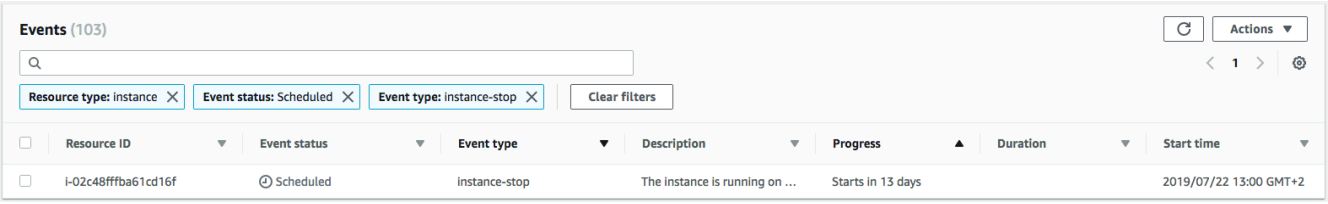
Console

Um geplante Ereignisse für Ihre Instances anzuzeigen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Alle Ressourcen mit einem zugeordneten Ereignis werden unter Geplante Ereignisse angezeigt.



3. Für weitere Einzelheiten, wählen Sie im Navigationsbereich die Option Ereignisse aus. Alle Ressourcen mit einem zugeordneten Ereignis werden angezeigt. Sie können nach Merkmalen wie Ereignistyp, Ressourcentyp und Availability Zone filtern.



AWS CLI

Um geplante Ereignisse für Ihre Instances anzuzeigen

Verwenden Sie den Befehl describe-instance-status.

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0 \
    --query "InstanceStatuses[].Events"
```

Die folgende Beispielausgabe zeigt ein Neustartereignis.

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0d59937288b749b32",
            "Code": "system-reboot",
            "Description": "The instance is scheduled for a reboot",
            "NotAfter": "2019-03-15T22:00:00.000Z",
```

```
            "NotBefore": "2019-03-14T20:00:00.000Z",
            "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
         }

    ]
]
```

Hier ist eine Beispielausgabe mit einem Ereignis zur Ausmusterung einer Instance angegeben.

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0e439355b779n26",

            "Code": "instance-stop",
            "Description": "The instance is running on degraded hardware",
            "NotBefore": "2015-05-23T00:00:00.000Z"
        }
    ]
]
```

PowerShell

Um geplante Ereignisse für Ihre Instances anzuzeigen

Verwenden Sie den folgenden Get-EC2InstanceStatus-Befehl.

```
(Get-EC2InstanceStatus -InstanceId i-1234567890abcdef0).Events
```

Hier ist eine Beispielausgabe mit einem Ereignis zur Ausmusterung einer Instance angegeben.

```
Code         : instance-stop
Description  : The instance is running on degraded hardware
NotBefore    : 5/23/2015 12:00:00 AM
```

Instance metadata

So zeigen Sie geplante Ereignisse für Ihre Instances mithilfe von Instance-Metadaten an

Sie können Informationen zu aktiven Wartungsereignissen für Ihre Instances mithilfe von Instance-Metadatenservice Version 2 oder Instance-Metadatenservice Version 1 aus den Instance-Metadaten abrufen.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

Es folgt eine Beispielausgabe mit Informationen zu einem geplanten Systemneustartereignis im JSON-Format.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "active"
  }
]
```

So zeigen Sie den Ereignisverlauf für abgeschlossene oder abgebrochene Ereignisse für Ihre Instances mit Instance-Metadaten an.

Sie können Informationen zu abgeschlossenen oder abgebrochenen Ereignissen für Ihre Instances mithilfe von Instance-Metadatenservice Version 2 oder Instance-Metadatenservice Version 1 aus den Instance-Metadaten abrufen.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/history
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/
history
```

Es folgt eine Beispielausgabe mit Informationen zu einem abgebrochenen und zu einem abgeschlossenen Systemneustartereignis im JSON-Format.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Canceled] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "canceled"
  },
  {
    "NotBefore" : "29 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Completed] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "29 Jan 2019 09:17:23 GMT",
    "State" : "completed"
  }
]
```

AWS Health

Sie können den verwenden AWS Health Dashboard , um mehr über Ereignisse zu erfahren, die sich auf Ihre Instance auswirken können. Die AWS Health Dashboard unterteilt Probleme in drei Gruppen: offene Probleme, geplante Änderungen und andere Benachrichtigungen. In der Gruppe der geplanten Änderungen werden laufende oder anstehende Elemente angegeben.

Weitere Informationen finden Sie unter Erste Schritte mit dem AWS Health Dashboard im AWS Health -Benutzerhandbuch.

Passen Sie Benachrichtigungen über geplante Ereignisse für Ihre Instanzen an EC2

Sie können geplante Ereignisbenachrichtigungen so anpassen, dass Tags (Markierungen) in die E-Mail-Benachrichtigung aufgenommen werden. Dies erleichtert die Identifizierung der

betroffenen Ressource (Instances oder Dedicated Hosts) und die Priorisierung von Aktionen für das bevorstehende Ereignis.

Wenn Sie Ereignisbenachrichtigungen so anpassen, dass sie Tags (Markierungen) einschließen, können Sie sich für das Einschließen der folgenden Elemente entscheiden:

- Alle Tags (Markierungen), die mit der betroffenen Ressource verknüpft sind
- Nur bestimmte Tags (Markierungen), die mit der betroffenen Ressource verknüpft sind

Angenommen, Sie weisen beispielsweise allen Ihren Instances `application`-, `costcenter`-, `project`- und `owner`-Tags (Markierungen) zu. Sie können sich dafür entscheiden, alle Tags (Markierungen) in Ereignisbenachrichtigungen aufzunehmen. Wenn Sie in Ereignisbenachrichtigungen nur die Tags (Markierungen) `owner` und `project` sehen möchten, können Sie alternativ auch nur diese Tags (Markierungen) einbeziehen.

Nachdem Sie die einzubeziehenden Tags (Markierungen) ausgewählt haben, enthalten die Ereignisbenachrichtigungen die Ressourcen-ID (Instance-ID oder Dedicated Host-ID) und die Schlüssel-Wert-Paare des Tags (Markierungen), die mit der betroffenen Ressource verknüpft sind.

Aufgaben

- Einschließen der Tags (Markierungen) in Ereignisbenachrichtigungen
- Entfernen der Tags (Markierungen) aus Ereignisbenachrichtigungen
- Anzeigen der Tags (Markierungen), die in Ereignisbenachrichtigungen einzubeziehen sind

Einschließen der Tags (Markierungen) in Ereignisbenachrichtigungen

Die Tags (Markierungen), die Sie einbeziehen möchten, gelten für alle Ressourcen (Instances und Dedicated Hosts) in der ausgewählten Region. Um Ereignisbenachrichtigungen in anderen Regionen anzupassen, wählen Sie zunächst die gewünschte Region aus und führen Sie dann die folgenden Schritte aus.

Console

So schließen Sie Tags (Markierungen) in Ereignisbenachrichtigungen ein:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Events.

3. Wählen Sie Actions (Aktionen), Manage event notifications (Ereignisbenachrichtigungen verwalten).
4. Aktivieren Sie Tags in Ereignisbenachrichtigungen einbeziehen.
5. Führen Sie je nach den Tags (Markierungen), die Sie in die Ereignisbenachrichtigungen aufnehmen möchten, eine der folgenden Aktionen aus:
   - Um alle der betroffenen Instance oder dem Dedicated Host zugeordneten Tags einzuschließen, wählen Sie Alle Tags einschließen aus.
   - Um die einzuschließenden Tags auszuwählen, wählen Sie Einzuschließende Tags auswählen und wählen Sie dann die Tag-Schlüssel aus oder geben Sie sie ein.
6. Wählen Sie Speichern.

AWS CLI

So schließen Sie alle Tags (Markierungen) in Ereignisbenachrichtigungen ein:

Verwenden Sie den Befehl register-instance-event-notification-attributes und setzen Sie den `IncludeAllTagsOfInstance` Parameter auf`true`.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute "IncludeAllTagsOfInstance=true"
```

So schließen Sie bestimmte Tags (Markierungen) in Ereignisbenachrichtigungen ein:

Verwenden Sie den Befehl register-instance-event-notification-attributes und geben Sie die Tags, die eingeschlossen werden sollen, mithilfe des `InstanceTagKeys` Parameters an.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_1", "tag_key_2",
 "tag_key_3"]'
```

PowerShell

So schließen Sie alle Tags (Markierungen) in Ereignisbenachrichtigungen ein:

Verwenden Sie das cmdlet Register-EC2InstanceEventNotificationAttribute.

```
Register-EC2InstanceEventNotificationAttribute `
```

```
    -InstanceTagAttribute_IncludeAllTagsOfInstance $true
```

So schließen Sie bestimmte Tags (Markierungen) in Ereignisbenachrichtigungen ein:

Verwenden Sie das cmdlet Register-EC2InstanceEventNotificationAttribute.

```
Register-EC2InstanceEventNotificationAttribute `
    -InstanceTagAttribute_InstanceTagKey tag_key_1, tag_key_2, tag_key_3
```

Entfernen der Tags (Markierungen) aus Ereignisbenachrichtigungen

Sie können Tags aus Ereignisbenachrichtigungen entfernen.

Console

So entfernen Sie Tags (Markierungen) aus Ereignisbenachrichtigungen:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Events.
3. Wählen Sie Actions (Aktionen), Manage event notifications (Ereignisbenachrichtigungen verwalten).
4. Um alle Tags aus Ereignisbenachrichtigungen zu entfernen, deaktivieren Sie Tags in Ereignisbenachrichtigungen einbeziehen.
5. Um bestimmte Tags aus Ereignisbenachrichtigungen zu entfernen, wählen Sie das X) für die entsprechenden Tag-Schlüssel aus.
6. Wählen Sie Speichern.

AWS CLI

So entfernen Sie alle Tags (Markierungen) aus Ereignisbenachrichtigungen:

Verwenden Sie den Befehl deregister-instance-event-notification-attributes und setzen Sie den `IncludeAllTagsOfInstance` Parameter auf`false`.

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute "IncludeAllTagsOfInstance=false"
```

So entfernen Sie ein Tag aus Ereignisbenachrichtigungen

Verwenden Sie den Befehl deregister-instance-event-notification-attributes und geben Sie die zu entfernenden Tags mithilfe des `InstanceTagKeys` Parameters an.

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_3"]'
```

PowerShell

So entfernen Sie alle Tags (Markierungen) aus Ereignisbenachrichtigungen:

Verwenden Sie das cmdlet Unregister-EC2InstanceEventNotificationAttribute.

```
Unregister-EC2InstanceEventNotificationAttribute `
    -InstanceTagAttribute_IncludeAllTagsOfInstance $false
```

So entfernen Sie ein Tag aus Ereignisbenachrichtigungen

Verwenden Sie das cmdlet Unregister-EC2InstanceEventNotificationAttribute.

```
Unregister-EC2InstanceEventNotificationAttribute `
    -InstanceTagAttribute_InstanceTagKey tag_key_3
```

Anzeigen der Tags (Markierungen), die in Ereignisbenachrichtigungen einzubeziehen sind

Sie können die in Ereignisbenachrichtigungen einzuschließende Tags anzeigen.

Console

So zeigen Sie die in Ereignisbenachrichtigungen einzuschließende Tags (Markierungen) an:

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Events.
3. Wählen Sie Actions (Aktionen), Manage event notifications (Ereignisbenachrichtigungen verwalten).

AWS CLI

So zeigen Sie die Tags an, die in Ereignisbenachrichtigungen einzuschließen sind

Verwenden Sie den Befehl describe-instance-event-notification-attributes.

```
aws ec2 describe-instance-event-notification-attributes
```

PowerShell

So zeigen Sie die Tags an, die in Ereignisbenachrichtigungen einzuschließen sind

Verwenden Sie das cmdlet Get-EC2InstanceEventNotificationAttribute.

```
Get-EC2InstanceEventNotificationAttribute
```

Planen Sie ein geplantes Ereignis für eine Instanz neu EC2

Sie können ein Ereignis so neu planen, dass es zu einem bestimmten Datum und einer Uhrzeit Ihrer Wahl erfolgt. Nachdem Sie ein Ereignis verschoben haben, kann es ein oder zwei Minuten dauern, bis das aktualisierte Datum angezeigt wird.

Einschränkungen

- Nur Ereignisse mit einem Ereignistermin können neu geplant werden. Der Zeitplan des Ereignisses kann bis hin zum Ablaufdatum der Ereignisfrist geändert werden. Die Spalte Frist (Konsole) und das Feld `NotBeforeDeadline` (AWS CLI) geben die Frist für das Ereignis an.
- Nur Ereignisse, die noch nicht gestartet wurden, können neu geplant werden. Die Spalte Startzeit (Konsole) und das Feld `NotBefore` (AWS CLI) geben die Startzeit des Ereignisses an. Ereignisse, die zum Start in den nächsten 5 Minuten geplant sind, können nicht verschoben werden.
- Die neue Startzeit muss mindestes 60 Minuten nach der aktuellen Uhrzeit liegen.
- Wenn Sie den Zeitplan mehrerer Ereignisse über die Konsole ändern, wird das Ablaufdatum der Ereignisfrist anhand des Ereignisses mit dem frühesten Ablaufdatum der Ereignisfrist bestimmt.

Console

So planen Sie ein Ereignis neu

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Events.
3. Wählen Sie Resource type: instance (Ressourcentyp: Instance) aus der Filterliste aus.
4. Wählen Sie eine oder mehrere Instances aus. Wählen Sie dann Actions (Aktionen), Schedule event (Ereignis planen).

Der Zeitplan kann nur für zeitlich befristete Ereignisse mit einem Wert für Deadline (Frist) geändert werden. Wenn eines der ausgewählten Ereignisse keinen Stichtag hat, ist Actions (Aktionen), Schedule event (Ereignis planen) deaktiviert.

5. Geben Sie für New start time (Neue Startzeit) ein neues Datum und eine neue Uhrzeit für das Ereignis ein. Das neue Datum und die neue Uhrzeit müssen vor dem Zeitpunkt von Event Deadline (Ereignisfrist) liegen.
6. Wählen Sie Speichern.

   Es kann ein oder zwei Minuten dauern, bis die aktualisierte Startzeit des Ereignisses in der Konsole angezeigt wird.

AWS CLI

So planen Sie ein Ereignis neu

Verwenden Sie den Befehl modify-instance-event-start-time.

```
aws ec2 modify-instance-event-start-time \
    --instance-id i-1234567890abcdef0 \
    --instance-event-id instance-event-0d59937288b749b32 \
    --not-before 2020-03-25T10:00:00.000
```

PowerShell

So planen Sie ein Ereignis neu

Verwenden Sie das cmdlet Edit-EC2InstanceEventStartTime.

```
Edit-EC2InstanceEventStartTime `
    -InstanceId i-1234567890abcdef0 `
    -InstanceEventId instance-event-0d59937288b749b32 `
    -NotBefore 2020-03-25T10:00:00.000
```

Erstellen Sie benutzerdefinierte Ereignisfenster für geplante Ereignisse, die sich auf Ihre EC2 Amazon-Instances auswirken

Sie können benutzerdefinierte Ereignisfenster definieren, die sich wöchentlich für geplante Ereignisse wiederholen, mit denen Ihre EC2 Amazon-Instances neu gestartet, gestoppt oder beendet werden.

Sie können einem Ereignisfenster eine oder mehrere Instances zuweisen. Wenn ein geplantes Ereignis für diese Instances geplant ist, plant AWS die Ereignisse innerhalb des zugehörigen Ereignisfensters.

Sie können Ereignisfenster verwenden, um die Verfügbarkeit von Workloads zu maximieren, indem Sie Ereignisfenster angeben, die in Zeiten mit geringer Auslastung für Ihre Workload auftreten. Sie können die Ereignisfenster auch an Ihren internen Wartungsplänen ausrichten.

Sie definieren ein Ereignisfenster, indem Sie einen Satz von Zeitbereichen angeben. Der minimale Zeitbereich beträgt 2 Stunden. Die kombinierten Zeitbereiche müssen mindestens 4 Stunden betragen.

Sie können einem Ereignisfenster eine oder mehrere Instances zuordnen, indem Sie entweder Instance IDs - oder Instance-Tags verwenden. Sie können Dedicated Hosts auch einem Ereignisfenster zuordnen, indem Sie die Host-ID verwenden.

> **Warning**
>
> Ereignisfenster gelten nur für geplante Ereignisse, die Instances anhalten, neu starten oder beenden.
> Ereignisfenster sind nicht anwendbar für:
>
> - Beschleunigte geplante Ereignisse und Netzwerkwartungsereignisse.
> - Außerplanmäßige Wartung wie die automatische Instance-Wiederherstellung und ungeplante Neustarts.

Arbeiten mit Ereignisfenstern

- Überlegungen
- Erstellen eines Ereignisfensters
- Zuordnen eines Ziels mit einem Ereignisfenster
- Ein Ziel von einem Ereignisfenster trennen
- Ein Ereignisfenster ändern
- Ein Ereignisfenster löschen

Überlegungen

- Alle Zeiträume des Ereignisfensters sind in UTC angegeben.
- Ein Ereignisfenster kann mehrere Zeitbereiche enthalten. Jeder einzelne Zeitbereich muss mindestens 2 Stunden lang sein, die Gesamtdauer für alle Bereiche muss jedoch mindestens 4 Stunden betragen.
- Einem Ereignisfenster kann nur ein Zieltyp (Instance-ID, Dedicated-Host-ID oder Instance-Tags (Markierungen)) zugeordnet werden.
- Ein Ziel (Instance-ID, Dedicated Host oder Instance-Tags (Markierungen)) kann nur einem Ereignisfenster zugeordnet werden.
- Einem Ereignisfenster können maximal 100 Instance IDs - oder 50 Dedicated Host IDs - oder 50 Instance-Tags zugeordnet werden. Die Instance-Tags (Markierungen) können beliebig vielen Instances zugeordnet werden.
- Pro AWS Region können maximal 200 Ereignisfenster erstellt werden.
- Bei mehreren Instances, die Ereignisfenstern zugeordnet sind, können möglicherweise gleichzeitig geplante Ereignisse auftreten.
- Wenn AWS bereits eine Veranstaltung geplant wurde, wirkt sich die Änderung eines Veranstaltungsfensters nicht auf die Uhrzeit der geplanten Veranstaltung aus. Wenn das Ereignis einen StichTags (Markierungen) hat, können Sie das Ereignis neu planen.
- Sie können eine Instance vor dem geplanten Ereignis anhalten und starten. Dadurch wird die Instance auf einen neuen Host migriert und das Ereignis gelöscht.

Erstellen eines Ereignisfensters

Sie können ein oder mehrere Ereignisfenster erstellen. Für jedes Ereignisfenster geben Sie einen oder mehrere Zeitblöcke an. Sie können beispielsweise ein Ereignisfenster mit Zeitblöcken erstellen, die jeden Tag um 4 Uhr morgens für 2 Stunden auftreten. Oder Sie erstellen ein Ereignisfenster mit Zeitblöcken, die sonntags von 2.00–4.00 Uhr und mittwochs von 3.00–5.00 Uhr stattfinden.

So lange werden die Ereignisfenster wöchentlich wiederholt, bis Sie sie löschen.

Console

So erstellen Sie ein Ereignisfenster

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Events.

3. Klicken Sie auf Aktionen, Verwalten von Ereignisfenstern.
4. Wählen Sie Instance-Ereignisfenster erstellen.
5. Geben Sie für Ereignisfenstername einen beschreibenden Namen für das Ereignisfenster ein.
6. Wählen Sie für Ereignisfensterzeitplan die Zeitblöcke im Ereignisfenster aus, indem Sie den Cron-Zeitplanersteller verwenden oder Zeitbereiche angeben.

   - Wenn Sie den Cron-Zeitplanersteller auswählen, geben Sie Folgendes an:
     1. Geben Sie für Tage (UTC) die Wochentage an, an denen das Ereignisfenster auftritt.
     2. Geben Sie für Startzeit (UTC) die Zeit an, zu der das Ereignisfenster beginnt.
     3. Geben Sie für Dauer die Dauer der Zeitblöcke im Ereignisfenster an. Die Mindestdauer pro Zeitblock beträgt 2 Stunden. Die Mindestdauer des Ereignisfensters muss insgesamt 4 Stunden betragen oder überschreiten. Alle Uhrzeiten sind in UTC angegeben.
   - Wenn Sie Zeitbereiche auswählen, wählen Sie Neuen Zeitbereich hinzufügen und geben Sie den Starttag und die Startzeit sowie den Endtag und die Endzeit an. Wiederholen Sie diesen Schritt für jeden Zeitraum. Die Mindestdauer pro Zeitbereich beträgt 2 Stunden. Die Mindestdauer für alle Zeitbereiche zusammen muss insgesamt 4 Stunden betragen oder überschreiten.
7. (Optional) Ordnen Sie für Zieldetails dem Ereignisfenster eine oder mehrere Instances zu. Verwenden Sie Instance IDs - oder Instance-Tags, um Instances zuzuordnen. Verwenden Sie host IDs , um Dedicated Hosts zuzuordnen. Wenn für diese Ziele Wartungsarbeiten geplant sind, tritt das Ereignis in diesem Ereignisfenster ein.

   Beachten Sie, dass Sie das Ereignisfenster erstellen können, ohne dem Fenster ein Ziel zuzuordnen. Später können Sie das Fenster ändern, um ein oder mehrere Ziele zu verknüpfen.
8. (Optional) Wählen Sie für Ereignisfenster-Tags (Markierungen) die Option Tags (Markierungen) hinzufügen und geben Sie den Schlüssel und den Wert für den Tag (Markierung) ein. Wiederholen Sie diesen Schritt für jeden Tag (Markierung).
9. Wählen Sie Ereignisfenster erstellen.

AWS CLI

So erstellen Sie ein Ereignisfenster mit einem Zeitbereich

Verwenden Sie den Befehl create-instance-event-window.

```
aws ec2 create-instance-event-window \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8 \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Es folgt eine Beispielausgabe.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

So erstellen Sie ein Ereignisfenster mit einem Cron-Ausdruck

Verwenden Sie den Befehl create-instance-event-window.

```
aws ec2 create-instance-event-window \
    --cron-expression "* 21-23 * * 2,3" \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Es folgt eine Beispielausgabe.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

PowerShell

So erstellen Sie ein Ereignisfenster mit einem Zeitbereich

Verwenden Sie das cmdlet New-EC2InstanceEventWindow.

```
$timeRange = New-Object Amazon.EC2.Model.InstanceEventWindowTimeRangeRequest
$timeRange.StartWeekDay = "monday"
$timeRange.EndWeekDay = "wednesday"
$timeRange.StartHour = 2
$timeRange.EndHour = 8
$tag = @{Key="key1"; Value="value1"}
$tagspec = New-Object Amazon.EC2.Model.TagSpecification
$tagspec.ResourceType = "instance-event-window"
$tagspec.Tags.Add($tag)
New-EC2InstanceEventWindow `
    -Name my-event-window `
    -TagSpecification $tagspec `
    -TimeRange @($timeRange)
```

Es folgt eine Beispielausgabe.

```
AssociationTarget     :
CronExpression        :
InstanceEventWindowId : iew-0abcdef1234567890
Name                  : my-event-window
State                 : creating
```

```
Tags                 : {key1}
TimeRanges           : {Amazon.EC2.Model.InstanceEventWindowTimeRange}
```

So erstellen Sie ein Ereignisfenster mit einem Cron-Ausdruck

Verwenden Sie das cmdlet New-EC2InstanceEventWindow.

```
$tag = @{Key="key1"; Value="value1"}
$tagspec = New-Object Amazon.EC2.Model.TagSpecification
$tagspec.ResourceType = "instance-event-window"
$tagspec.Tags.Add($tag)
New-EC2InstanceEventWindow `
    -Name my-event-window `
    -TagSpecification $tagspec`
    -CronExpression "* 21-23 * * 2,3"
```

Es folgt eine Beispielausgabe.

```
AssociationTarget     :
CronExpression        : * 21-23 * * 2,3
InstanceEventWindowId : iew-0abcdef1234567890
Name                  : my-event-window
State                 : creating
Tags                  : {key1}
TimeRanges            : {}
```

Zuordnen eines Ziels mit einem Ereignisfenster

Nachdem Sie ein Ereignisfenster erstellt haben, können Sie dem Ereignisfenster Ziele zuordnen. Sie können einem Ereignisfenster nur einen Zieltyp zuordnen. Sie können Instance- IDs, Dedicated Host IDs - oder Instance-Tags angeben.

Console

So ordnen Sie einem Ereignisfenster Ziele zu

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Events.
3. Wählen Sie das zu ändernde Ereignisfenster aus.

4. Wählen Sie Aktionen, Instance-Ereignisfenster ändern.

AWS CLI

So verknüpfen Sie Instance-Tags mit einem Ereignisfenster

Verwenden Sie den Befehl associate-instance-event-window.

```
aws ec2 associate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Es folgt eine Beispielausgabe.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [
                {
                    "Key": "k2",
                    "Value": "v2"
                },
                {
                    "Key": "k1",
                    "Value": "v1"
                }
            ],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Um eine Instance IDs einem Ereignisfenster zuzuordnen

Verwenden Sie den Befehl associate-instance-event-window.

```
aws ec2 associate-instance-event-window \
```

```
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Es folgt eine Beispielausgabe.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-1234567890abcdef0",
                "i-0598c7d356eba48d7"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

So verknüpfen Sie einen Dedicated Host mit einem Ereignisfenster

Verwenden Sie den Befehl associate-instance-event-window.

```
aws ec2 associate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "DedicatedHostIds=h-029fa35a02b99801d"
```

Es folgt eine Beispielausgabe.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": [
                "h-029fa35a02b99801d"
```

```
            ]
        },
        "State": "creating"
    }
}
```

PowerShell

So verknüpfen Sie Instance-Tags mit einem Ereignisfenster

Verwenden Sie das cmdlet Register-EC2InstanceEventWindow.

```
$tag1 = @{Key="key1"; Value="value1"}
$tag2 = @{Key="key2"; Value="value2"}
Register-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_InstanceTag @($tag1,$tag2)
```

Um eine Instanz IDs einem Ereignisfenster zuzuordnen

Verwenden Sie das cmdlet Register-EC2InstanceEventWindow.

```
Register-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_InstanceId i-1234567890abcdef0, i-0598c7d356eba48d7
```

So verknüpfen Sie einen Dedicated Host mit einem Ereignisfenster

Verwenden Sie das cmdlet Register-EC2InstanceEventWindow.

```
Register-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_DedicatedHostId h-029fa35a02b99801d
```

Ein Ziel von einem Ereignisfenster trennen

Console

So trennen Sie die Zuordnung von Zielen zu einem Ereignisfenster

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich die Option Events.
3. Wählen Sie das zu ändernde Ereignisfenster aus.
4. Wählen Sie Aktionen, Instance-Ereignisfenster ändern.

AWS CLI

So trennen Sie die Instance-Tags von einem Ereignisfenster

Verwenden Sie den Befehl disassociate-instance-event-window.

```
aws ec2 disassociate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Es folgt eine Beispielausgabe.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Um die Zuordnung einer Instance zu einem Ereignisfenster zu IDs trennen

Verwenden Sie den Befehl disassociate-instance-event-window.

```
aws ec2 disassociate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Es folgt eine Beispielausgabe.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

So trennen Sie einen Dedicated Host von einem Ereignisfenster

Verwenden Sie den Befehl disassociate-instance-event-window.

```
aws ec2 disassociate-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target DedicatedHostIds=h-029fa35a02b99801d
```

Es folgt eine Beispielausgabe.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

PowerShell

So trennen Sie die Instance-Tags von einem Ereignisfenster

Verwenden Sie das cmdlet Unregister-EC2InstanceEventWindow.

```
$tag1 = @{Key="key1"; Value="value1"}
$tag2 = @{Key="key2"; Value="value2"}
Unregister-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_InstanceTag @($tag1, $tag2)
```

Um die Zuordnung einer Instanz zu einem IDs Ereignisfenster zu trennen

Verwenden Sie das cmdlet Unregister-EC2InstanceEventWindow.

```
Unregister-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_InstanceId i-1234567890abcdef0, i-0598c7d356eba48d7
```

So trennen Sie einen Dedicated Host von einem Ereignisfenster

Verwenden Sie das cmdlet Unregister-EC2InstanceEventWindow.

```
Unregister-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -AssociationTarget_DedicatedHostId h-029fa35a02b99801d
```

Ein Ereignisfenster ändern

Sie können alle der Felder eines Ereignisfensters mit Ausnahme der ID ändern. Wenn beispielsweise die Sommerzeit beginnt, möchten Sie möglicherweise den Zeitplan für das Ereignisfenster ändern. Bei vorhandenen Ereignisfenstern empfiehlt es sich möglicherweise, Ziele hinzuzufügen oder zu entfernen.

Sie können beim Ändern des Ereignisfensters entweder einen Zeitbereich oder einen Cron-Ausdruck ändern, aber nicht beides.

Console

So ändern Sie ein Ereignisfenster

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich die Option Events.
3. Klicken Sie auf Aktionen, Verwalten von Ereignisfenstern.
4. Wählen Sie das zu ändernde Ereignisfenster aus und wählen Sie dann Aktionen, Instance-Ereignisfenster ändern.
5. Ändern Sie die Felder im Ereignisfenster und wählen Sie dann Ereignisfenster ändern.

AWS CLI

So ändern Sie den Zeitbereich eines Ereignisfensters

Verwenden Sie den Befehl modify-instance-event-window.

```
aws ec2 modify-instance-event-window
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8
```

Es folgt eine Beispielausgabe.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
```

```
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

So ändern Sie eine Reihe von Zeitbereichen für ein Ereignisfenster

Verwenden Sie den Befehl modify-instance-event-window.

```
aws ec2 modify-instance-event-window
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range '[{"StartWeekDay": "monday", "StartHour": 2, "EndWeekDay":
 "wednesday", "EndHour": 8},
   {"StartWeekDay": "thursday", "StartHour": 2, "EndWeekDay": "friday",
 "EndHour": 8}]'
```

Es folgt eine Beispielausgabe.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            },
            {
                "StartWeekDay": "thursday",
                "StartHour": 2,
                "EndWeekDay": "friday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
```

```
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

So ändern Sie den Cron-Ausdruck eines Ereignisfensters

Verwenden Sie den Befehl modify-instance-event-window.

```
aws ec2 modify-instance-event-window
    --instance-event-window-id iew-0abcdef1234567890 \
    --cron-expression "* 21-23 * * 2,3"
```

Es folgt eine Beispielausgabe.

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
```

```
        ]
    }
}
```

PowerShell

So ändern Sie den Zeitbereich eines Ereignisfensters

Verwenden Sie das cmdlet Edit-EC2InstanceEventWindow.

```
$timeRange1 = New-Object Amazon.EC2.Model.InstanceEventWindowTimeRangeRequest
$timeRange1.StartWeekDay = "monday"
$timeRange1.EndWeekDay = "wednesday"
$timeRange1.StartHour = 2
$timeRange1.EndHour = 8
$timeRange2 = New-Object Amazon.EC2.Model.InstanceEventWindowTimeRangeRequest
$timeRange2.StartWeekDay = "thursday"
$timeRange2.EndWeekDay = "friday"
$timeRange2.StartHour = 1
$timeRange2.EndHour = 6
Edit-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -TimeRange @($timeRange1, $timeRange2)
```

So ändern Sie den Cron-Ausdruck eines Ereignisfensters

Verwenden Sie das cmdlet Edit-EC2InstanceEventWindow.

```
Edit-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -CronExpression "* 21-23 * * 2,3"
```

Ein Ereignisfenster löschen

Sie können jeweils ein Ereignisfenster löschen.

Console

So löschen Sie ein Ereignisfenster

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich die Option Events.
3. Klicken Sie auf Aktionen, Verwalten von Ereignisfenstern.
4. Wählen Sie das zu löschende Ereignisfenster aus, und wählen Sie dann Aktionen, Instance-Ereignisfenster löschen.
5. Geben Sie bei der Aufforderung **`delete`** ein und klicken Sie dann auf Delete (Löschen).

AWS CLI

So löschen Sie ein Ereignisfenster

Verwenden Sie den delete-instance-event-windowBefehl und geben Sie das zu löschende Ereignisfenster an.

```
aws ec2 delete-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890
```

So erzwingen Sie das Löschen eines Ereignisfensters

Verwenden Sie den `--force-delete`-Parameter, wenn das Ereignisfenster derzeit mit Zielen verknüpft ist.

```
aws ec2 delete-instance-event-window \
    --instance-event-window-id iew-0abcdef1234567890 \
    --force-delete
```

PowerShell

So löschen Sie ein Ereignisfenster

Verwenden Sie das cmdlet Remove-EC2InstanceEventWindow.

```
Remove-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890
```

So erzwingen Sie das Löschen eines Ereignisfensters

Verwenden Sie das cmdlet Remove-EC2InstanceEventWindow.

```
Remove-EC2InstanceEventWindow `
    -InstanceEventWindowId iew-0abcdef1234567890 `
    -ForceDelete $true
```

Überwachen Sie Ihre Instances mit CloudWatch

Sie können Ihre Instances mithilfe von Amazon überwachen CloudWatch, das Rohdaten von Amazon sammelt und zu lesbaren, nahezu EC2 in Echtzeit verfügbaren Metriken verarbeitet. Diese Statistiken werden für einen Zeitraum von 15 Monaten aufgezeichnet, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden.

Standardmäßig EC2 sendet Amazon Metrikdaten innerhalb von 5 Minuten CloudWatch an. Um Metrikdaten für Ihre Instance innerhalb von 1 Minute CloudWatch an zu senden, können Sie die detaillierte Überwachung der Instance aktivieren. Weitere Informationen finden Sie unter Verwalte die detaillierte Überwachung deiner EC2 Instances.

Die EC2 Amazon-Konsole zeigt eine Reihe von Diagrammen an, die auf den Rohdaten von Amazon basieren CloudWatch. Je nach Ihren Anforderungen ziehen Sie es möglicherweise vor, Daten für Ihre Instances von Amazon CloudWatch anstelle der Diagramme in der Konsole zu beziehen.

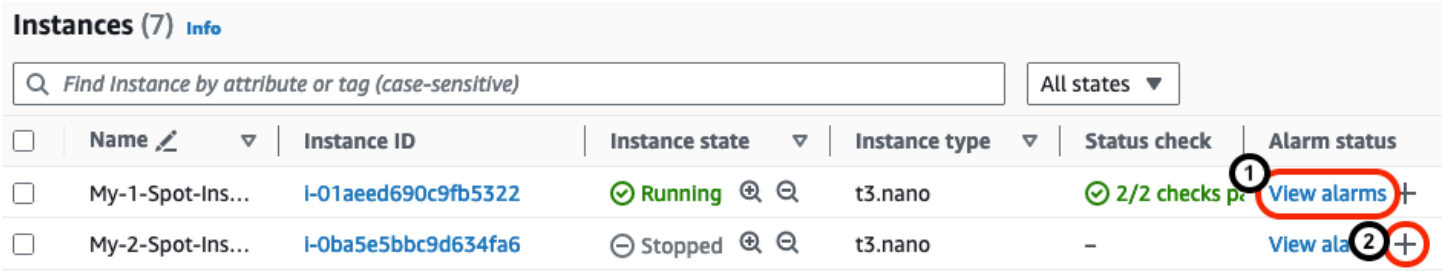
CloudWatch Abrechnungs- und Kosteninformationen von Amazon finden Sie unter CloudWatch Abrechnung und Kosten im CloudWatch Amazon-Benutzerhandbuch.

Inhalt

- CloudWatch Alarme für Ihre EC2 Instances in der EC2 Amazon-Konsole verwalten
- Verwalte die detaillierte Überwachung deiner EC2 Instances
- CloudWatch Metriken, die für Ihre Instances verfügbar sind
- Installieren und konfigurieren Sie den CloudWatch Agenten mithilfe der EC2 Amazon-Konsole, um zusätzliche Metriken hinzuzufügen
- Statistiken für CloudWatch Metriken für Ihre Instances
- Die Überwachungsdiagramme für Ihre Instance anzeigen
- Erstellen Sie einen CloudWatch Alarm für eine Instance
- Erstellen von Alarmen, mit denen eine Instance angehalten, beendet, neu gestartet oder wiederhergestellt wird

CloudWatch Alarme für Ihre EC2 Instances in der EC2 Amazon-Konsole verwalten

Auf dem Bildschirm Instances in der EC2 Amazon-Konsole können Sie die CloudWatch Amazon-Alarme für Ihre Instances verwalten. In der Instance-Tabelle bietet die Spalte Alarmstatus zwei Steuerelemente für die Konsole: eine Steuerung für die Anzeige von Alarmen und eine weitere für deren Erstellung oder Bearbeitung. Der folgende Screenshot zeigt diese Konsolensteuerungen mit den Nummern 1 (Alarme anzeigen) und 2 (ein Pluszeichen für das Erstellen oder Bearbeiten eines Alarms).



Alarme auf dem Instances-Bildschirm anzeigen

Sie können die Alarme jeder Instance auf dem Instances-Bildschirm einsehen.

So zeigen Sie den Alarm einer Instance auf dem Bildschirm Instances an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie in der Instances-Tabelle für die von Ihnen gewählte Instance die Option Alarme anzeigen aus (im vorherigen Screenshot mit 1 nummeriert).
4. Wählen Sie im *i-1234567890abcdef0* Fenster Alarm-Details für den Alarmnamen aus, um den Alarm in der CloudWatch Konsole anzuzeigen.

Alarme vom Instances-Bildschirm erstellen

Vom Bildschirm Instances können Sie für jede Instance einen Alarm erstellen.

So erstellen Sie einen Alarm für eine Instance über den Bildschirm Instances

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.

3. Wählen Sie in der Instances-Tabelle für die von Ihnen gewählte Instance die Option Alarme anzeigen aus (im vorherigen Screenshot mit 2 nummeriert).
4. Erstellen Sie auf dem Bildschirm „ CloudWatch Alarme verwalten“ Ihren Alarm. Weitere Informationen finden Sie unter Erstellen Sie einen CloudWatch Alarm für eine Instance.

Alarme vom Instances-Bildschirm bearbeiten

Vom Bildschirm Instances können Sie für jede Instance einen Alarm bearbeiten.

So bearbeiten Sie einen Alarm für eine Instance auf dem Bildschirm Instances

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie in der Instances-Tabelle für die von Ihnen gewählte Instance die Option Alarme anzeigen aus (im vorherigen Screenshot mit 2 nummeriert).
4. Bearbeiten Sie auf dem Bildschirm „ CloudWatch Alarme verwalten“ Ihren Alarm. Weitere Informationen finden Sie unter Bearbeiten oder Löschen eines CloudWatch Alarms im CloudWatch Amazon-Benutzerhandbuch.

Verwalte die detaillierte Überwachung deiner EC2 Instances

Amazon CloudWatch bietet zwei Überwachungskategorien: Basisüberwachung und detaillierte Überwachung. Standardmäßig ist für Ihre Instance die grundlegende Überwachung aktiviert. Sie können optional die detaillierte Überwachung aktivieren, um Probleme bei der Ausführung schneller zu identifizieren und zu beheben. Sie können die detaillierte Überwachung auf einer Instance ausschalten, während Sie sie starten bzw. während sie ausgeführt oder angehalten wird.

Das Aktivieren der detaillierten Überwachung für eine Instance wirkt sich nicht auf die Überwachung der EBS-Volumes aus, die mit der Instance verknüpft sind. Weitere Informationen finden Sie unter CloudWatch Amazon-Metriken für Amazon EBS.

In der folgenden Tabelle werden die Unterschiede zwischen der grundlegenden Überwachung und der detaillierten Überwachung von Instances beschrieben.

Überwachungstyp	Beschreibung	Gebühren
Grundlegende Überwachung	Metriken für die Statusprüfung sind in Zeitabständen von 1 Minute verfügbar. Alle anderen Metriken sind in 5-Minuten-Intervallen verfügbar.	Keine Gebühren.
Detaillierte Überwachung	Sie können Metriken in 1-Minuten-Intervallen abrufen, sofern Sie die detaillierte Überwachung für die Instance aktivieren. Wenn Sie die detaillierte Überwachung aktiviert haben, können Sie aggregierte Daten aus Gruppen mit ähnlichen Instances erhalten.	Ihnen wird pro Metrik berechnet, an die Amazon EC2 sendet CloudWatch. Die Datenspeicherung wird Ihnen nicht berechnet. Weitere Informationen finden Sie unter Tarif „Bezahlt“ auf der Seite mit den CloudWatch Amazon-Preisen.

Inhalt

- Erforderliche Berechtigungen
- Detaillierte Überwachung beim Start aktivieren
- Detaillierte Überwachung verwalten

Erforderliche Berechtigungen

Um die detaillierte Überwachung für eine Instance zu aktivieren, muss Ihr Benutzer über die Berechtigung zur Verwendung der MonitorInstances-API-Aktion verfügen. Um die detaillierte Überwachung für eine Instances zu deaktivieren, muss Ihr Benutzer über die Berechtigung zur Verwendung der UnmonitorInstances-API-Aktion verfügen.

Detaillierte Überwachung beim Start aktivieren

Verwenden Sie die folgenden Verfahren, um die detaillierte Überwachung beim Start zu aktivieren. Standardmäßig ist für Ihre Instance die grundlegende Überwachung aktiviert.

Console

Aktivieren der detaillierten Überwachung beim Starten einer Instance

Wenn Sie eine Instance über die EC2 Amazon-Konsole starten, aktivieren Sie unter Erweiterte Details das Kontrollkästchen Detaillierte CloudWatch Überwachung.

AWS CLI

Aktivieren der detaillierten Überwachung beim Starten einer Instance

Verwenden den Befehl run-instances mit der Option `--monitoring`.

```
--monitoring Enabled=true
```

PowerShell

Aktivieren der detaillierten Überwachung beim Starten einer Instance

Verwenden Sie das New-EC2InstanceCmdlet mit dem `-Monitoring` Parameter.

```
-Monitoring $true
```

Detaillierte Überwachung verwalten

Verwenden Sie die folgenden Verfahren, um die detaillierte Überwachung für eine laufende oder angehaltene Instance zu verwalten.

Console

So verwalten Sie die detaillierte Überwachung

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.
4. Wählen Sie Aktionen, Überwachung und Fehlerbehebung, Detaillierte Überwachung verwalten aus.
5. Führen Sie auf der Seite Detaillierte Überwachung unter Detaillierte Überwachung einen der folgenden Schritte aus:
   - Detaillierte Überwachung – Wählen Sie Aktivieren aus.

- Grundlegende Überwachung – Deaktivieren Sie die Option Aktivieren#.

6. Wählen Sie Bestätigen aus.

AWS CLI

So aktivieren Sie die detaillierte Überwachung

Verwenden Sie den Befehl monitor-instances.

```
aws ec2 monitor-instances --instance-ids i-1234567890abcdef0
```

So deaktivieren Sie die detaillierte Überwachung

Verwenden Sie den Befehl unmonitor-instances.

```
aws ec2 unmonitor-instances --instance-ids i-1234567890abcdef0
```

PowerShell

So aktivieren Sie die detaillierte Überwachung

Verwenden Sie das cmdlet Start-EC2InstanceMonitoring.

```
Start-EC2InstanceMonitoring -InstanceId i-1234567890abcdef0
```

So deaktivieren Sie die detaillierte Überwachung

Verwenden Sie das cmdlet Stop-EC2InstanceMonitoring.

```
Stop-EC2InstanceMonitoring -InstanceId i-1234567890abcdef0
```

CloudWatch Metriken, die für Ihre Instances verfügbar sind

Amazon EC2 sendet Messwerte an Amazon CloudWatch. Sie können die AWS-Managementkonsole, oder eine API verwenden AWS CLI, um die Metriken aufzulisten, an die Amazon EC2 sendet CloudWatch. Standardmäßig deckt jeder Datenpunkt die sich an die Startzeit anschließenden 5 Minuten an Aktivität für die Instance ab. Wenn Sie die detaillierte Überwachung aktiviert haben, deckt jeder Datenpunkt die nächste Minute an Aktivität ab der Startzeit ab. Beachten Sie, dass für

die Statistiken „Minimum“, „Maximum“ und „Durchschnitt“ die Mindestgranularität der bereitgestellten Metriken 1 Minute beträgt. EC2

Informationen darüber, wie Sie die verfügbaren Metriken mit dem AWS-Managementkonsole oder dem anzeigen können AWS CLI, finden Sie unter Verfügbare Metriken anzeigen im CloudWatch Amazon-Benutzerhandbuch.

Weitere Informationen zum Abrufen der Statistiken für diese Metriken erhalten Sie unter Statistiken für CloudWatch Metriken für Ihre Instances.

Inhalt

- Instance-Metriken
- Beschleuniger-Metriken
- CPU-Guthaben-Metriken
- Dedicated-Host-Metriken
- Amazon EBS-Metriken für Nitro-basierte Instances
- Statusprüfungsmetriken
- Metriken zur Spiegelung des Datenverkehrs
- Amazon EC2 Auto Scaling Scaling-Gruppenmetriken
- EC2 Metrische Abmessungen von Amazon
- EC2 Amazon-Nutzungsmetriken

Instance-Metriken

Der `AWS/EC2`-Namespace enthält die folgenden Instance-Metriken.

Metrik	Description	Einheit	Aussagekräftige Statistiken
`CPUUtilization`	Der Prozentsatz der physischen CPU-Zeit, die Amazon zum Ausführen der EC2 Instance EC2 verwendet, einschließlich der Zeit, die sowohl für die Ausführung des Benutzercodes als auch des EC2 Amazon-Codes aufgewendet wurde.	Percent	• Average • Minimum • Maximum

Metrik	Description	Einheit	Aussagekräftige Statistiken
	Auf einer sehr hohen Ebene ist `CPUUtilization` die Summe aus Gast `CPUUtilization` und Hypervisor `CPUUtilization`. Tools in Ihrem Betriebssystem können CloudWatch aufgrund von Faktoren wie Legacy-Gerätesimulation, Konfiguration von Geräten anderer Hersteller, Interrupt-intensive Workloads, Live-Migration und Live-Update einen anderen Prozentsatz anzeigen.		
`DiskReadOps`	Abgeschlossene Lesevorgänge von allen der Instance zu Verfügung stehenden Instance-Speicher-Volumes in einem angegebenen Zeitraum. Um die durchschnittlichen I/O Operationen pro Sekunde (IOPS) für den Zeitraum zu berechnen, dividieren Sie die Gesamtzahl der Vorgänge in dem Zeitraum durch die Anzahl der Sekunden in diesem Zeitraum. Wenn es keine Instance-Speicher-Volumes gibt, ist der Wert 0 oder die Metrik wird nicht angezeigt.	Count	• Sum • Average • Minimum • Maximum

Metrik	Description	Einheit	Aussagekräftige Statistiken
`DiskWriteOps`	Abgeschlossene Schreibvorgänge von allen der Instance zu Verfügung stehenden Instance-Speicher-Volumes in einem angegebenen Zeitraum. Um die durchschnittlichen I/O Operationen pro Sekunde (IOPS) für den Zeitraum zu berechnen, dividieren Sie die Gesamtzahl der Operationen in dem Zeitraum durch die Anzahl der Sekunden in diesem Zeitraum. Wenn es keine Instance-Speicher-Volumes gibt, ist der Wert 0 oder die Metrik wird nicht angezeigt.	Count	• Sum • Average • Minimum • Maximum

Metrik	Description	Einheit	Aussagekräftige Statistiken
`DiskReadBytes`	Von allen der Instance zu Verfügung stehenden Instance-Speicher-Volumes gelesene Byte. Diese Metrik wird verwendet, um das von der Festplatte der Instance gelesene Datenvolumen der Anwendung zu ermitteln. Damit kann die Geschwindigkeit der Anwendung bestimmt werden. Der ermittelte Wert ist die Anzahl der während des Zeitraums empfangenen Byte. Wenn Sie die grundlegende Überwachung (alle 5 Minuten) verwenden, können Sie diesen Wert durch 300 teilen, um die Byte/Sekunden zu ermitteln. Wenn Sie die detaillierte Überwachung (einminütig) verwenden, teilen Sie den Wert durch 60. Sie können auch die mathematische Funktion CloudWatch Metrik verwenden `DIFF_TIME` , um die Byte pro Sekunde zu ermitteln. Wenn Sie beispielsweise CloudWatch als grafisch dargestellt `DiskReadBytes` haben`m1`, gibt die mathematische Formel die Metrik in Byte/Sekunde `m1/(DIFF_TIME(m1))` zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie unter Verwenden von metrischer Mathematik im CloudWatch Amazon-Benutzerhandbuch. Wenn es keine Instance-Speicher-Volumes gibt, ist der Wert 0 oder die Metrik wird nicht angezeigt.	Bytes	• Sum • Average • Minimum • Maximum

Metrik	Description	Einheit	Aussagekräftige Statistiken
`DiskWriteBytes`	In alle der Instance zu Verfügung stehenden Instance-Speicher-Volumes geschriebene Byte. Diese Metrik wird verwendet, um das auf die Festplatte der Instance geschriebene Datenvolumen der Anwendung zu ermitteln . Damit kann die Geschwindigkeit der Anwendung bestimmt werden. Der ermittelte Wert ist die Anzahl der während des Zeitraums empfangenen Byte. Wenn Sie die grundlegende Überwachung (alle 5 Minuten) verwenden, können Sie diesen Wert durch 300 teilen, um die Byte/Sekunden zu ermitteln. Wenn Sie die detaillierte Überwachung (einminütig) verwenden, teilen Sie den Wert durch 60. Sie können auch die CloudWatch metrische mathematische Funktion verwenden `DIFF_TIME` , um die Byte pro Sekunde zu ermitteln. Wenn Sie beispielsweise CloudWatch als grafisch dargestellt `DiskWriteBytes` haben`m1`, gibt die mathematische Formel die Metrik in Byte/Sekunde `m1/(DIFF_TIME(m1))` zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie unter Verwenden von metrischer Mathematik im CloudWatch Amazon-Benutzerhandbuch. Wenn es keine Instance-Speicher-Volumes gibt, ist der Wert 0 oder die Metrik wird nicht angezeigt.	Bytes	• Sum • Average • Minimum • Maximum

Metrik	Description	Einheit	Aussagekräftige Statistiken
`MetadataNoToken`	Gibt an, wie oft erfolgreich auf den Instance Metadata Service (IMDS) mit einer Methode zugegriffen wurde, die kein Token verwendet. Diese Metrik wird verwendet, um festzustellen, ob es Prozesse gibt, die auf Instance-Metadaten zugreifen und die Version 1 (IMDSv1) für Instance-Metadaten verwenden, die kein Token verwendet. Wenn alle Anfragen tokengestützte Sitzungen verwenden, d. h. Instance Metadata Service Version 2 (IMDSv2), ist der Wert 0. Weitere Informationen finden Sie unter Übergang zur Verwendung von Instance-Metadatenservice Version 2.	Nitro-Instances: Keine Xen-Instances: Count	• Sum • Percentiles
`MetadataNoTokenRejected`	Gibt an, wie oft ein IMDSv1 Anruf versucht wurde, nachdem IMDSv1 er deaktiviert wurde. Wenn diese Metrik angezeigt wird, bedeutet dies, dass ein IMDSv1 Anruf versucht und abgelehnt wurde. Sie können es entweder wieder aktivieren IMDSv1 oder sicherstellen, dass alle Ihre Anrufe verwendet IMDSv2 werden. Weitere Informationen finden Sie unter Übergang zur Verwendung von Instance-Metadatenservice Version 2.	Nitro-Instances: Keine Xen-Instances: Count	• Sum • Percentiles

Metrik	Description	Einheit	Aussagekräftige Statistiken
`NetworkIn`	Anzahl der von der Instance auf allen Netzwerkschnittstellen empfangenen Byte. Diese Metrik gibt das an eine einzelne Instance eingehende Netzwerkdatenvolumen an. Der ermittelte Wert ist die Anzahl der während des Zeitraums empfangenen Byte. Wenn Sie eine grundlegene Überwachung (fünf Minuten) verwenden und die Statistik eine Summe ist, können Sie diese Zahl durch 300 teilen, um Bytes/Sekunde zu ermitteln. Wenn Sie eine detaillierte (einminütige) Überwachung haben und die Statistik eine Summe ist, teilen Sie sie durch 60.	Bytes	• Sum • Average • Minimum • Maximum
`NetworkOut`	Anzahl der von der Instance auf allen Netzwerkschnittstellen gesendeten Byte. Diese Metrik gibt das an eine einzelne Instance ausgehende Netzwerkdatenvolumen an. Der ermittelte Wert ist die Anzahl der während des Zeitraums gesendeten Bytes. Wenn Sie eine grundlegene Überwachung (fünf Minuten) verwenden und die Statistik eine Summe ist, können Sie diese Zahl durch 300 teilen, um Bytes/Sekunde zu ermitteln. Wenn Sie eine detaillierte (einminütige) Überwachung haben und die Statistik eine Summe ist, teilen Sie sie durch 60.	Bytes	• Sum • Average • Minimum • Maximum

Metrik	Description	Einheit	Aussagekräftige Statistiken
`NetworkPacketsIn`	Anzahl der von der Instance auf allen Netzwerkschnittstellen empfangenen Pakete. Diese Metrik gibt das an eine einzelne Instance eingehende Netzwerkdatenvolumen an, ausgedrückt in Anzahl an Paketen. Diese Metrik ist nur für die grundlegende Überwachung verfügbar (Fünf-Minuten-Intervalle). Um die Anzahl der Pakete pro Sekunde (PPS) zu berechnen, die Ihre Instance für die fünf Minuten erhalten hat, teilen Sie die Summe des Statistikwertes Sum durch 300.	Count	• Sum • Average • Minimum • Maximum
`NetworkPacketsOut`	Anzahl der von der Instance auf allen Netzwerkschnittstellen gesendeten Pakete. Diese Metrik gibt das von einer einzelnen Instance ausgehende Netzwerkdatenvolumen an, ausgedrückt in Anzahl an Paketen. Diese Metrik ist nur für die grundlegende Überwachung verfügbar (Fünf-Minuten-Intervalle). Um die Anzahl der Pakete pro Sekunde (PPS) zu berechnen, die Ihre Instance die fünf Minuten lang gesendet hat, teilen Sie die Summe des Statistikwertes durch 300.	Count	• Sum • Average • Minimum • Maximum

Beschleuniger-Metriken

Der `AWS/EC2` Namespace umfasst die folgende Beschleuniger-Metrik für Ihre beschleunigte Computing-Instances. Wird nur für eine Teilmenge der beschleunigte Computing-Instance-Typen unterstützt.

Metrik	Description	Einheit	Aussagekräftige Statistiken
`GPUPowerUtilization`	Wirkleistungsverbrauch als Prozentsatz der maximalen Wirkleistung.	Prozent	• Average • Minimum • Maximum

CPU-Guthaben-Metriken

Der `AWS/EC2`-Namespace enthält die folgenden CPU-Gutschriftmetriken für Ihre Instances mit Spitzenleistung.

Metrik	Description	Einheit	Aussagekräftige Statistiken
`CPUCreditUsage`	Die Anzahl der von der Instance für die CPU-Nutzung verbrauchten CPU-Guthaben. Ein CPU-Guthaben entspricht einer vCPU, die eine Minute lang bei 100% Auslastung läuft, oder einer äquivalenten Kombination aus vCPUs, Auslastung und Zeit (z. B. eine vCPU, die zwei Minuten lang mit 50% Auslastung läuft oder zwei v, die zwei Minuten lang mit 25% Auslastung CPUs laufen). Die Metriken für CPU-Guthaben sind nur mit einer fünfminütigen Frequenz verfügbar. Wenn Sie ein größeres Intervall als 5 Minuten angeben, verwenden Sie die Statistik `Sum` anstelle der Statistik `Average`.	Guthaben (vCPU-Minuten)	• Sum • Average • Minimum • Maximum
`CPUCreditBalance`	Die Anzahl verdienter CPU-Guthaben, die eine Instance angesammelt hat, seit sie gestartet wurde. Für T2 Standard beinhaltet `CPUCredit`	Guthaben (vCPU-Minuten)	• Sum • Average • Minimum

Metrik	Description	Einheit	Aussagekräftige Statistiken
	`Balance` auch die Anzahl der angesammelten Startguthaben. Guthaben werden auf dem Guthaben-Konto angesammelt, nachdem sie verdient wurden, und davon entfernt, wenn sie verbraucht werden. Der Guthaben-Kontostand hat ein maximales Limit, das anhand der Instance-Größe bestimmt wird. Nachdem das Limit erreicht ist, verfallen alle neu verdienten Guthabenpunkte. Für T2 Standard zählen Startguthaben nicht zum Limit. Die Guthaben in `CPUCreditBalance` sind verfügbar, um die Leistung der Instance über die Baseline ihrer CPU-Nutzung hinaus zu steigern. Wenn eine Instance ausgeführt wird, verfallen Guthaben im `CPUCreditBalance` nicht. Wenn eine T3- oder T3a-Instance angehalten wird, bleibt der `CPUCreditBalance` -Wert sieben Tage lang erhalten. Danach verfallen alle angesammelten Guthaben. Wenn eine T2-Instance beendet wird, bleibt der `CPUCreditBalance` -Wert nicht erhalten, und alle angesammelten Guthaben gehen verloren. Die Metriken für CPU-Guthaben sind nur mit einer fünfminütigen Frequenz verfügbar.		• Maximum

Metrik	Description	Einheit	Aussagekräftige Statistiken
`CPUSurplusCreditBalance`	Die Anzahl überzähliger Guthaben, die von einer `unlimited` -Instance verbraucht wurden, wenn ihr `CPUCreditBalance` -Wert null ist. Der `CPUSurplusCreditBalance` -Wert wird durch erworbene CPU-Guthaben abgezahlt. Wenn die Anzahl überzähliger Guthaben die Höchstzahl der Guthaben überschreitet, die die Instance in einem 24-Stunden-Zeitraum verdienen kann, fallen für die verbrauchten überzähligen Guthaben zusätzliche Gebühren an. Die Metriken für CPU-Guthaben sind nur mit einer fünfminütigen Frequenz verfügbar.	Guthaben (vCPU-Minuten)	• Sum • Average • Minimum • Maximum

Metrik	Description	Einheit	Aussagekräftige Statistiken
`CPUSurplusCreditsCharged`	Die Anzahl verbrauchter überzähliger Guthaben, die nicht durch verdiente CPU-Guthaben zurückgezahlt wurden, und für die deshalb eine zusätzliche Gebühr anfällt. Verbrauchte überzählige Guthaben werden in Rechnung gestellt, wenn einer der folgenden Fälle auftritt: • Die ausgegebenen überzähligen Guthaben überschreiten die maximale Anzahl an Guthaben, die die Instance in einem 24-Stunden-Zeitraum verdienen kann. Über das Maximum hinaus ausgegebene überzähli ge Guthaben werden am Ende der Stunde abgerechnet. • Die Instance wird angehalten oder beendet. • Die Instance wird von `unlimited` in `standard` geändert. Die Metriken für CPU-Guthaben sind nur mit einer fünfminütigen Frequenz verfügbar.	Guthaben (vCPU-Minuten)	• Sum • Average • Minimum • Maximum

Dedicated-Host-Metriken

Der `AWS/EC2`-Namespace enthält die folgenden Metriken für T3-Dedicated-Hosts.

Metrik	Description	Einheit	Aussagekräftige Statistiken
`DedicatedHostCPUUtilization`	Der Prozentsatz der zugewiesenen Rechenkapazität, die derzeit von den Instances verwendet wird, die auf dem Dedicated Host ausgeführt werden.	Percent	• Sum • Average • Minimum • Maximum

Amazon EBS-Metriken für Nitro-basierte Instances

Der `AWS/EC2`-Namespace beinhaltet zusätzliche Amazon EBS-Metriken für Volumes, die Nitro-basierten Instances angefügt sind, die keine Bare-Metal-Instances sind.

Metrik	Description	Einheit	Aussagekräftige Statistiken
`InstanceEBSIOPSExceededCheck`	Meldet, ob eine Anwendung innerhalb der letzten Minute versucht hat, IOPS zu treiben, die die maximalen EBS-IOPS-Limits für die Instance überschritten hat. Diese Metrik kann entweder `0` (IOPS nicht überschritten) oder 1 (IOPS überschritten) sein.	Keine	• Summe • Durchschnitt • Minimum • Maximum
`InstanceEBSThroughputExceededCheck`	Meldet, ob eine Anwendung innerhalb der letzten Minute versucht hat, einen Durchsatz zu treiben, der die maximalen EBS-Durchsatzlimits für die Instance überschreitet. Diese Metrik kann entweder `0` (Durchsatz nicht überschritten) oder 1 (Durchsatz überschritten) sein.	Keine	• Summe • Durchschnitt • Minimum • Maximum
`EBSReadOps`	Abgeschlossene Lesevorgänge von allen an die Instance angefügten Amazon EBS-Volumes in einem angegebenen Zeitraum.	Anzahl	• Summe • Durchschnitt • Minimum

Metrik	Description	Einheit	Aussagekräftige Statistiken
	Um die durchschnittlichen I/O Lesevorgänge pro Sekunde (Lese-IOPS) für den Zeitraum zu berechnen, dividieren Sie die Gesamtzahl der Vorgänge in diesem Zeitraum durch die Anzahl der Sekunden in diesem Zeitraum. Wenn Sie die grundlegende Überwachung (alle 5 Minuten) verwenden, können Sie diesen Wert durch 300 teilen, um die Lese-IOPS zu ermitteln. Wenn Sie die detaillierte Überwachung (einminütig) verwenden, teilen Sie den Wert durch 60. Sie können auch die CloudWatch metrische mathematische Funktion verwenden`DIFF_TIME` , um die Operationen pro Sekunde zu ermitteln. Wenn Sie beispielsweise CloudWatch als `m1` grafisch dargestellt `EBSReadOps` haben, gibt die metrische mathematische Formel die Metrik in Operationen/Sekunde `m1/(DIFF_TIME(m1))` zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie unter Verwenden von metrischer Mathematik im CloudWatch Amazon-Benutzerhandbuch.		• Maximum

Metrik	Description	Einheit	Aussagekräftige Statistiken
`EBSWriteOps`	Abgeschlossene Schreibvorgänge in alle an die Instance angehängten EBS-Volumes in einem angegebenen Zeitraum. Um die durchschnittlichen I/O Schreibvorgänge pro Sekunde (Schreib-IOPS) für den Zeitraum zu berechnen, dividieren Sie die Gesamtzahl der Operationen in dem Zeitraum durch die Anzahl der Sekunden in diesem Zeitraum. Wenn Sie die grundlegende Überwachung (alle 5 Minuten) verwenden, können Sie diesen Wert durch 300 teilen, um die Schreib-IOPS zu ermitteln. Wenn Sie die detaillierte Überwachung (einminütig) verwenden, teilen Sie den Wert durch 60. Sie können auch die CloudWatch metrische mathematische Funktion verwenden`DIFF_TIME` , um die Operationen pro Sekunde zu ermitteln. Wenn Sie beispielsweise CloudWatch als `m1` grafisch dargestellt `EBSWriteOps` haben, gibt die metrische mathematische Formel die Metrik in Operationen/Sekunde `m1/(DIFF_TIME(m1))` zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie unter Verwenden von metrischer Mathematik im CloudWatch Amazon-Benutzerhandbuch.	Anzahl	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Description	Einheit	Aussagekräftige Statistiken
`EBSReadBytes`	Die aus allen an die Instance angefügten EBS-Volumes gelesenen Bytes in einem angegebenen Zeitraum. Der ermittelte Wert ist die Anzahl der während des Zeitraums gelesenen Bytes. Wenn Sie die grundlegende Überwachung (alle 5 Minuten) verwenden, können Sie diesen Wert durch 300 teilen, um die Lese-Bytes/Sekunden zu ermitteln. Wenn Sie die detaillierte Überwachung (einminütig) verwenden, teilen Sie den Wert durch 60. Sie können auch die CloudWatch metrische mathematische Funktion verwenden `DIFF_TIME` , um die Byte pro Sekunde zu ermitteln. Wenn Sie beispielsweise CloudWatch als grafisch dargestellt `EBSReadBytes` haben`m1`, gibt die mathematische Formel die Metrik in Byte/Sekunde `m1/(DIFF_TIME(m1))` zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie unter Verwenden von metrischer Mathematik im CloudWatch Amazon-Benutzerhandbuch.	Bytes	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Description	Einheit	Aussagekräftige Statistiken
`EBSWriteBytes`	Die in alle an die Instance angefügten EBS-Volumes geschriebenen Bytes in einem angegebenen Zeitraum. Der ermittelte Wert ist die Anzahl der während des Zeitraums geschriebenen Bytes. Wenn Sie die grundlegende Überwachung (alle 5 Minuten) verwenden, können Sie diesen Wert durch 300 teilen, um die Schreib-Bytes/Sekunden zu ermitteln. Wenn Sie die detaillierte Überwachung (einminütig) verwenden, teilen Sie den Wert durch 60. Sie können auch die CloudWatch metrische mathematische Funktion verwenden`DIFF_TIME`, um die Byte pro Sekunde zu ermitteln. Wenn Sie beispielsweise CloudWatch als grafisch dargestellt `EBSWriteBytes` haben`m1`, gibt die mathematische Formel die Metrik in Byte/Sekunde `m1/(DIFF_TIME(m1))` zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie unter Verwenden von metrischer Mathematik im CloudWatch Amazon-Benutzerhandbuch.	Bytes	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Description	Einheit	Aussagekräftige Statistiken
`EBSIOBalance%`	Enthält Informationen über den Prozentsatz der verbleibenden I/O Credits im Burst-Bucket. Diese Metrik ist nur für die grundlegende Überwachung verfügbar. Diese Metrik ist nur für einige `*.4xlarge` -Instance-Größen und kleiner verfügbar, die mindestens einmal alle 24 Stunden für nur 30 Minuten ihre maximale Leistung erreichen. Die `Sum`-Statistik ist für diese Metrik nicht anwendbar.	Prozent	• Minimum • Maximum
`EBSByteBalance%`	Bietet Informationen über den Prozentanteil der verbleibenden Durchsatz-Guthaben im Burst-Bucket. Diese Metrik ist nur für die grundlegende Überwachung verfügbar. Diese Metrik ist nur für einige `*.4xlarge` -Instance-Größen und kleiner verfügbar, die mindestens einmal alle 24 Stunden für nur 30 Minuten ihre maximale Leistung erreichen. Die `Sum`-Statistik ist für diese Metrik nicht anwendbar.	Prozent	• Minimum • Maximum

Weitere Informationen zu den für Ihre EBS-Volumes verfügbaren Metriken erhalten Sie unter Metriken für Amazon-EBS-Volumes im Amazon-EBS-Benutzerhandbuch. Informationen zu den für Ihre EC2 Flotten und Spot-Flotten bereitgestellten Kennzahlen finden Sie unter. Überwachen Sie Ihre EC2 Flotte oder Spot-Flotte mit CloudWatch

Statusprüfungsmetriken

Standardmäßig sind die Metriken für Statusprüfungen mit einer einminütigen Frequenz kostenlos verfügbar. Für eine erneut gestartete Instance stehen Metrikdaten zu Statusprüfungen erst dann zur Verfügung, wenn die Instance den Initialisierungszustand abgeschlossen hat (innerhalb weniger Minuten wechselt die Instance in den Zustand „`running`“). Weitere Informationen zu EC2 Statuschecks finden Sie unter. Statuschecks für EC2 Amazon-Instances

Der `AWS/EC2`-Namespace enthält die folgenden Metriken zu Statusprüfungen.

Metrik	Description	Einheit	Aussagekräftige Statistiken
`StatusCheckFailed`	Berichtet, ob die Instance in der letzten Minute alle System-Statusprüfungen bestanden hat. Diese Metrik nimmt den Wert `0` (bestanden) oder 1 (fehlgeschlagen) an. Standardmäßig ist diese Metrik mit einer einminütigen Frequenz kostenlos verfügbar.	Count	• Average • Minimum • Maximum
`StatusCheckFailed_Instance`	Berichtet, ob die Instance in der letzten Minute die Instance-Statusprüfung bestanden hat. Diese Metrik nimmt den Wert `0` (bestanden) oder 1 (fehlgeschlagen) an. Standardmäßig ist diese Metrik mit einer einminütigen Frequenz kostenlos verfügbar.	Count	• Average • Minimum • Maximum
`StatusCheckFailed_System`	Berichtet, ob die Instance in der letzten Minute die System-Statusprüfung bestanden hat. Diese Metrik nimmt den Wert `0` (bestanden) oder 1 (fehlgeschlagen) an. Standardmäßig ist diese Metrik mit einer einminütigen Frequenz kostenlos verfügbar.	Count	• Average • Minimum • Maximum

Metrik	Description	Einheit	Aussagekräftige Statistiken
`StatusCheckFailed_AttachedEBS`	Berichtet, ob die Instance in der letzten Minute die verknüpfte EBS-Statusprüfung bestanden hat. Diese Metrik nimmt den Wert `0` (bestanden) oder 1 (fehlgeschlagen) an. Standardmäßig ist diese Metrik mit einer einminütigen Frequenz kostenlos verfügbar.	Count	• Average • Minimum • Maximum

Der `AWS/EBS`-Namespace enthält die folgenden Metriken zu Statusprüfungen.

Metrik	Description	Einheit	Aussagekräftige Statistiken
`VolumeStalledIOCheck`	Hinweis: Nur für Nitro-Instances. Nicht veröffentlicht für Bände, die Amazon ECS und AWS Fargate Aufgaben angehängt sind. Meldet, ob ein Volume in der letzten Minute eine unterbrochene E/A-Überprüfung bestanden hat. Diese Metrik nimmt den Wert `0` (bestanden) oder 1 (fehlgeschlagen) an.	Keine	• Average • Minimum • Maximum

Metriken zur Spiegelung des Datenverkehrs

Der `AWS/EC2`-Namespace enthält Metriken für gespiegelten Datenverkehr. Weitere Informationen finden Sie unter Überwachen von gespiegeltem Datenverkehr mithilfe von Amazon CloudWatch im Amazon VPC Traffic Mirroring Guide.

Amazon EC2 Auto Scaling Scaling-Gruppenmetriken

Der `AWS/AutoScaling` Namespace enthält Metriken für Amazon EC2 Auto Scaling Scaling-Gruppen. Weitere Informationen finden Sie unter Überwachen von CloudWatch Metriken für Ihre Amazon EC2 Auto Scaling Scaling-Gruppen und -Instances im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

EC2 Metrische Abmessungen von Amazon

Sie können die folgenden Dimensionen verwenden, um die in den vorherigen Tabellen aufgeführten Metriken zu verfeinern.

Dimension	Beschreibung
`AutoScalingGroupName`	Diese Dimension filtert die angeforderten Daten für alle Instances einer angegebenen Kapazitätsgruppe. Eine Auto Scaling-Gruppe ist eine Sammlung von Instances, die Sie definieren, wenn Sie Amazon EC2 Auto Scaling verwenden. Diese Dimension ist nur für EC2 Amazon-Metriken verfügbar, wenn sich die Instances in einer solchen Auto Scaling Scaling-Gruppe befinden. Verfügbar für Instances, für die die detaillierte oder die grundlegende Überwachung aktiviert ist.
`ImageId`	Diese Dimension filtert die Daten, die Sie für alle Instances anfordern, auf denen dieses Amazon EC2 Amazon Machine Image (AMI) ausgeführt wird. Verfügbar für Instances, für die die detaillierte Überwachung aktiviert ist.
`InstanceId`	Diese Dimension filtert die angeforderten Daten nur für die identifizierte Instance. So können Sie eine exakte Instance festlegen, von der aus die Daten überwacht werden sollen.
`InstanceType`	Diese Dimension filtert die angeforderten Daten für alle Instances, die mit diesem angegebenen Instance-Typ ausgeführt werden. So können Sie Ihre Daten nach dem Typ der ausgeführten Instance kategorisieren. Sie können beispielsweise Daten aus einer m1.small-Instance und einer m1.large-Instance vergleichen, um zu ermitteln, welche für

Dimension	Beschreibung
	Ihre Anwendung den größeren geschäftlichen Nutzen bietet. Verfügbar für Instances, für die die detaillierte Überwachung aktiviert ist.

EC2 Amazon-Nutzungsmetriken

Sie können CloudWatch Nutzungsmetriken verwenden, um einen Überblick über die Ressourcennutzung Ihres Kontos zu erhalten. Verwenden Sie diese Metriken, um Ihre aktuelle Servicenutzung in CloudWatch Diagrammen und Dashboards zu visualisieren.

Die EC2 Amazon-Nutzungskennzahlen entsprechen den AWS Servicekontingenten. Sie können Alarme konfigurieren, mit denen Sie benachrichtigt werden, wenn sich Ihre Nutzung einem Servicekontingent nähert. Weitere Informationen zur CloudWatch Integration mit Servicekontingenten finden Sie unter AWS Nutzungsmetriken im CloudWatch Amazon-Benutzerhandbuch.

Amazon EC2 veröffentlicht die folgenden Metriken im `AWS/Usage` Namespace.

Metrik	Beschreibung
`ResourceCount`	Die Anzahl der angegebenen Ressourcen, die in Ihrem Konto ausgeführt werden. Die Ressourcen werden durch die Dimensionen definiert, die der Metrik zugeordnet sind. Die nützlichste Statistik für diese Metrik ist `MAXIMUM`, die die maximale Anzahl der Ressourcen darstellt, die während des 1-Minuten-Zeitraums verwendet werden.

Die folgenden Dimensionen werden verwendet, um die von Amazon veröffentlichten Nutzungsmetriken zu verfeinern EC2.

Dimension	Description
`Service`	Der Name des AWS Dienstes, der die Ressource enthält. Für EC2 Amazon-Nutzungsmetriken ist der Wert für diese Dimension`EC2`.

Dimension	Description
`Type`	Der Typ von Entität, die gemeldet wird. Derzeit ist der einzig gültige Wert für EC2 Amazon-NutzungsmetrikenResource.
`Resource`	Der Typ der Ressource, die ausgeführt wird. Derzeit ist der einzig gültige Wert für EC2 Amazon-NutzungsmetrikenvCPU, der Informationen zu laufenden Instances zurückgibt.
`Class`	Die Klasse der nachverfolgten Ressource. Für EC2 Amazon-Nutzungsmetriken mit vCPU dem Wert der Resource Dimension sind die gültigen Werte Standard/OnDemand F/OnDemand ,G/OnDemand ,Inf/OnDemand ,P/OnDemand , undX/OnDemand . Die Werte für diese Dimension definieren den ersten Buchstaben der Instance-Typen, die von der Metrik gemeldet werden. Standard/OnDemand gibt beispielsweise Informationen über alle laufenden Instances mit Typen zurück, die mit A, C, D, H, I, M, R, T und Z beginnen, und G/OnDemand gibt Informationen über alle laufenden Instances mit Typen zurück, die mit G beginnen.

Installieren und konfigurieren Sie den CloudWatch Agenten mithilfe der EC2 Amazon-Konsole, um zusätzliche Metriken hinzuzufügen

Die Installation und Konfiguration des CloudWatch Agenten über die EC2 Amazon-Konsole befindet sich für Amazon in der Betaphase EC2 und kann sich ändern.

Standardmäßig CloudWatch stellt Amazon grundlegende Metriken wie CPUUtilization und NetworkIn für die Überwachung Ihrer EC2 Amazon-Instances bereit. Um zusätzliche Metriken zu sammeln, können Sie den CloudWatch Agenten auf Ihren EC2 Instances installieren und ihn dann so konfigurieren, dass er ausgewählte Metriken ausgibt. Anstatt den CloudWatch Agenten auf jeder EC2 Instance manuell zu installieren und zu konfigurieren, können Sie die EC2 Amazon-Konsole verwenden, um dies für Sie zu erledigen.

Sie können die EC2 Amazon-Konsole verwenden, um den CloudWatch Agenten auf Ihren Instances zu installieren und den Agenten so zu konfigurieren, dass er ausgewählte Metriken ausgibt.

Alternativ können Sie diesen Vorgang manuell abschließen, indem Sie den Artikel Installation des CloudWatch Agenten im CloudWatch Amazon-Benutzerhandbuch nachlesen. Weitere Informationen über den CloudWatch Agenten finden Sie unter Erfassung von Metriken, Protokollen und Traces mithilfe des CloudWatch Agenten.

Inhalt

- Voraussetzungen
- Funktionsweise
- Kosten
- Installieren und konfigurieren Sie den CloudWatch Agenten

Voraussetzungen

EC2 Um Amazon für die Installation und Konfiguration des CloudWatch Agenten zu verwenden, müssen Sie die in diesem Abschnitt beschriebenen Benutzer- und Instance-Voraussetzungen erfüllen.

> **Tip**
>
> Diese Funktion ist nicht in allen verfügbar AWS-Regionen. Wenn das im Installationsverfahren auf dieser Seite beschriebene Menüelement nicht in der EC2 Amazon-Konsole vorhanden ist und Sie flexibel entscheiden können, wo Ihre Instances ausgeführt werden, versuchen Sie es mit einer anderen Region. Andernfalls können Sie die manuellen Anweisungen im CloudWatch Amazon-Benutzerhandbuch verwenden, um den Agenten zu installieren und zu konfigurieren.

Voraussetzungen für den Benutzer

Um diese Funktion nutzen zu können, muss Ihr IAM-Konsolenbenutzer oder Ihre IAM-Rolle über die für die Nutzung von Amazon erforderlichen Berechtigungen EC2 und die folgenden IAM-Berechtigungen verfügen:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter",
                "ssm:PutParameter"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/EC2-Custom-Metrics-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:ListCommandInvocations",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetInstanceProfile",
                "iam:SimulatePrincipalPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Voraussetzungen für Instance

- Instance-Status: `running`
- Unterstütztes Betriebssystem: Linux
- AWS Systems Manager Agent (SSM-Agent): Installiert. Zwei Hinweise zum SSM-Agenten:

  - Der SSM-Agent ist auf einigen Amazon Machine Images (AMIs) vorinstalliert, die von vertrauenswürdigen Drittanbietern AWS bereitgestellt werden. Informationen zu den unterstützten Programmen AMIs und Anweisungen zur Installation des SSM-Agenten finden Sie unter Amazon Machine Images (AMIs) with SSM Agent preinstalled im AWS Systems Manager Benutzerhandbuch.
  - Wenn Sie Probleme mit dem SSM-Agenten haben, finden Sie weitere Informationen unter Problembehandlung beim SSM-Agenten im AWS Systems Manager -Benutzerhandbuch.
- IAM-Berechtigungen für die Instance: Die folgenden AWS verwalteten Richtlinien müssen einer IAM-Rolle hinzugefügt werden, die der Instance zugeordnet ist:
  - Amazon SSMManaged InstanceCore — Ermöglicht einer Instance, Systems Manager zur Installation und Konfiguration des CloudWatch Agenten zu verwenden.
  - CloudWatchAgentServerPolicy— Ermöglicht einer Instance, den CloudWatch Agenten zum Schreiben von Daten zu verwenden CloudWatch.

  Informationen zum Hinzufügen von IAM-Berechtigungen zu Ihrer Instance finden Sie unter Verwenden von Instance-Profilen im IAM-Benutzerhandbuch.

Funktionsweise

Bevor Sie die EC2 Amazon-Konsole zur Installation und Konfiguration des CloudWatch Agenten verwenden können, müssen Sie sicherstellen, dass Ihr IAM-Benutzer oder Ihre IAM-Rolle und die Instances, auf denen Sie Metriken hinzufügen möchten, bestimmte Voraussetzungen erfüllen. Anschließend können Sie die EC2 Amazon-Konsole verwenden, um den CloudWatch Agenten auf Ihren ausgewählten Instances zu installieren und zu konfigurieren.

Erfüllen Sie zunächst die Voraussetzungen

- Sie benötigen die erforderlichen IAM-Berechtigungen – Bevor Sie beginnen, stellen Sie sicher, dass Ihr Konsolenbenutzer oder Ihre Rolle über die erforderlichen IAM-Berechtigungen für die Verwendung dieses Features verfügt.
- Instances — Um die Funktion nutzen zu können, müssen Ihre EC2 Instances Linux-Instances sein, auf denen der SSM-Agent installiert ist, über die erforderlichen IAM-Berechtigungen verfügen und ausgeführt werden.

Dann können Sie das Feature verwenden

1. Wählen Sie Ihre Instances aus — In der EC2 Amazon-Konsole wählen Sie die Instances aus, auf denen der CloudWatch Agent installiert und konfiguriert werden soll. Anschließend starten Sie den Vorgang, indem Sie „ CloudWatch Agent konfigurieren“ wählen.
2. SSM-Agent validieren — Amazon EC2 überprüft, ob der SSM-Agent auf jeder Instance installiert und gestartet ist. Alle Instances, die diese Prüfung nicht bestehen, werden vom Prozess ausgeschlossen. Der SSM-Agent wird verwendet, um während dieses Prozesses Aktionen auf der Instance auszuführen.
3. IAM-Berechtigungen validieren — Amazon EC2 prüft, ob jede Instance über die erforderlichen IAM-Berechtigungen für diesen Prozess verfügt. Alle Instances, die diese Prüfung nicht bestehen, werden vom Prozess ausgeschlossen. Die IAM-Berechtigungen ermöglichen es dem CloudWatch Agenten, Metriken von der Instance zu sammeln und ihn AWS Systems Manager zur Verwendung des SSM-Agenten zu integrieren.
4. CloudWatch Agent validieren — Amazon EC2 überprüft, ob der CloudWatch Agent auf jeder Instance installiert ist und ausgeführt wird. Wenn eine Instanz diese Prüfung nicht besteht, EC2 bietet Amazon an, den CloudWatch Agenten für Sie zu installieren und zu starten. Sobald dieser Vorgang abgeschlossen ist, erfasst der CloudWatch Agent die ausgewählten Metriken für jede Instance.
5. Metrikkonfiguration auswählen — Sie wählen die Metriken aus, die der CloudWatch Agent von Ihren Instances ausgeben soll. Nach der Auswahl EC2 speichert Amazon eine Konfigurationsdatei im Parameter Store, wo sie verbleibt, bis der Vorgang abgeschlossen ist. Amazon EC2 löscht die Konfigurationsdatei aus dem Parameter Store, sofern der Vorgang nicht unterbrochen wird. Beachten Sie, dass, wenn Sie keine Metrik auswählen, sie aber zuvor zu Ihrer Instance hinzugefügt haben, diese nach Abschluss dieses Vorgangs aus Ihrer Instance entfernt wird.
6. CloudWatch Agentenkonfiguration aktualisieren — Amazon EC2 sendet die Metrikkonfiguration an den CloudWatch Agenten. Dies ist der letzte Schritt in diesem Prozess. Wenn dies erfolgreich ist, können Ihre Instances Daten für die ausgewählten Metriken ausgeben und Amazon EC2 löscht die Konfigurationsdatei aus dem Parameter Store.

Kosten

Zusätzliche Metriken, die Sie während dieses Vorgangs hinzufügen, werden als benutzerdefinierte Metriken abgerechnet. Weitere Informationen zu den Preisen von CloudWatch Metriken finden Sie unter CloudWatch Amazon-Preise.

Installieren und konfigurieren Sie den CloudWatch Agenten

Sie können die EC2 Amazon-Konsole verwenden, um den CloudWatch Agenten zu installieren und zu konfigurieren, um zusätzliche Metriken hinzuzufügen.

> **Note**
>
> Jedes Mal, wenn Sie dieses Verfahren ausführen, überschreiben Sie die bestehende CloudWatch Agentenkonfiguration. Wenn Sie keine Metrik auswählen, die zuvor ausgewählt wurde, wird sie aus der Instance entfernt.

Um den CloudWatch Agenten mit der EC2 Amazon-Konsole zu installieren und zu konfigurieren

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instances aus, auf denen der CloudWatch Agent installiert und konfiguriert werden soll.
4. Wählen Sie Aktionen, Überwachung und Fehlerbehebung, CloudWatch Agent konfigurieren aus.
5. Lesen Sie für jeden Schritt des Vorgangs den Konsolentext und wählen Sie dann Weiter.
6. Um den Vorgang abzuschließen, wählen Sie im letzten Schritt Vollständig aus.

Um die von der EC2 Amazon-Konsole erstellte Agentenkonfiguration zu aktualisieren

Sie können die Konfiguration, die die EC2 Konsole erstellt hat, manuell anpassen. Weitere Informationen finden Sie unter Manuelles Erstellen oder Bearbeiten der CloudWatch Agenten-Konfigurationsdatei im CloudWatch Amazon-Benutzerhandbuch.

Statistiken für CloudWatch Metriken für Ihre Instances

Sie können Statistiken für die CloudWatch Metriken für Ihre Instances abrufen. Statistiken sind Aggregationen von Metrikdaten über bestimmte Zeiträume. CloudWatch stellt Statistiken bereit, die auf den metrischen Datenpunkten basieren, die durch Ihre benutzerdefinierten Daten oder durch andere Dienste bereitgestellt werden. AWS CloudWatch Für die Aggregationen werden der Namespace, der Metrikname, die Dimensionen und die Datenpunkt-Maßeinheit innerhalb des von Ihnen angegebenen Zeitraums verwendet. Die folgende Tabelle beschreibt die verfügbaren Statistiken.

Statistik	Beschreibung
`Minimum`	Der niedrigste beobachtete Wert während eines angegebenen Zeitraums. Sie können diesen Wert verwenden, um für Ihre Anwendung Aktivitäten geringen Umfangs zu bestimmen.
`Maximum`	Der höchste beobachtete Wert während eines angegebenen Zeitraums. Sie können diesen Wert verwenden, um für Ihre Anwendung Aktivitäten hohen Umfangs zu bestimmen.
`Sum`	Alle für die passende Metrik übermittelten Werte werden addiert. Diese Statistik kann nützlich sein, um das Gesamtvolumen einer Metrik zu ermitteln.
`Average`	Der Wert von `Sum`/`SampleCount` während eines angegebenen Zeitraums. Wenn Sie diese Statistik mit dem `Minimum` und dem `Maximum` vergleichen, können Sie den vollen Umfang einer Metrik bestimmen und feststellen, wie nahe die durchschnittliche Nutzung an das `Minimum` und `Maximum` heranreicht. Dank dieses Vergleichs wissen Sie dann, wann Sie Ihre Ressourcen je nach Bedarf erhöhen oder verringern sollten.
`SampleCount`	Die Anzahl der für die statistische Berechnung verwendeten Datenpunkte.
`pNN.NN`	Der Wert des angegebenen Perzentils. Sie können ein beliebiges Perzentil mit bis zu zwei Dezimalstellen (z. B. p95,45) angeben.

Inhalt

- Abrufen von Statistiken für eine bestimmte Instance
- Aggregieren von Statistiken auf allen Instances
- Aggregierte Statistiken nach Amazon EC2 Auto Scaling Scaling-Gruppe
- Aggregieren von Statistiken nach AMI

Abrufen von Statistiken für eine bestimmte Instance

Sie können das AWS-Managementkonsole oder das verwenden AWS CLI , um Statistiken für eine bestimmte Instanz abzurufen. Die folgenden Beispiele zeigen Ihnen, wie Sie mit AWS-

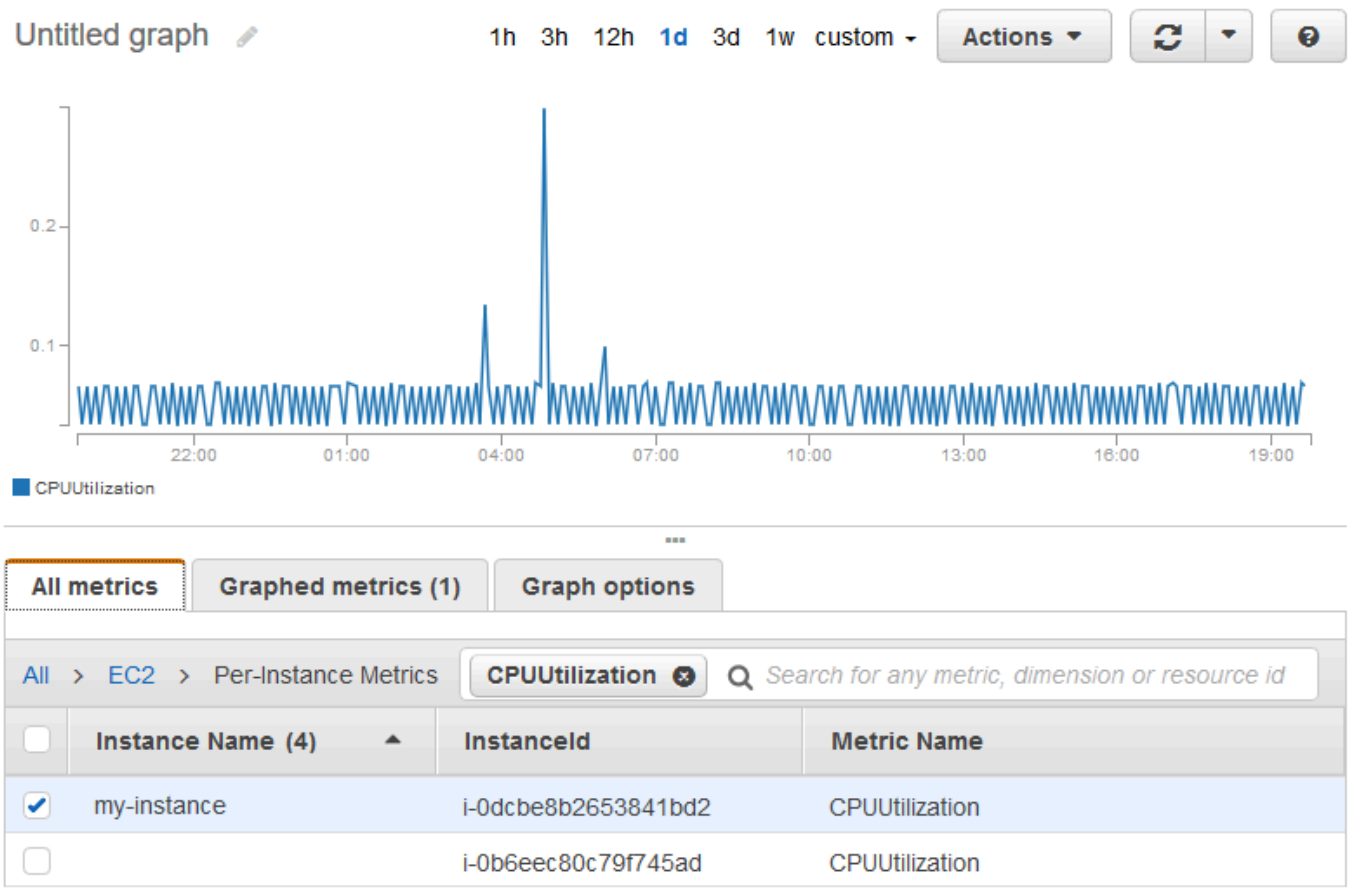
Managementkonsole oder die AWS CLI die maximale CPU-Auslastung einer bestimmten EC2 Instanz ermitteln können.

Voraussetzungen

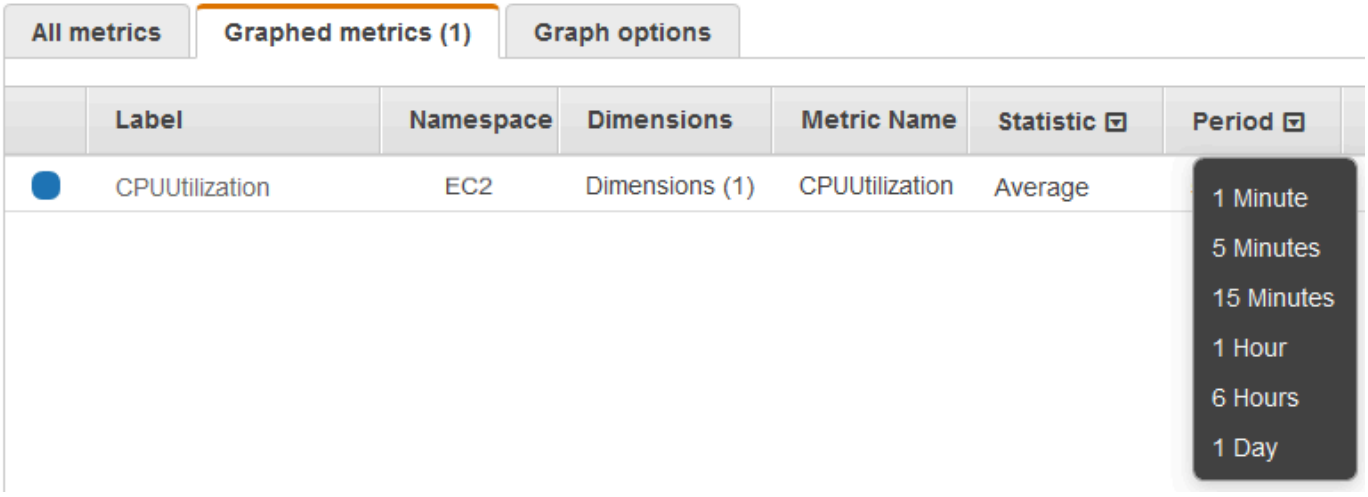
- Sie müssen die ID der Instance kennen. Sie können die Instance-ID mit der AWS-Managementkonsole oder mit dem Befehl describe-instances abrufen.
- Standardmäßig ist die grundlegende Überwachung aktiviert. Sie können aber auch eine detaillierte Überwachung aktivieren. Weitere Informationen finden Sie unter Verwalte die detaillierte Überwachung deiner EC2 Instances.

So zeigen Sie die CPU-Auslastung für eine bestimmte Instance an (Konsole)

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den EC2Metrik-Namespace aus.
4. Wählen Sie die Dimension Per-Instance Metrics (Metriken pro Instance) aus.
5. Geben Sie **`CPUUtilization`** in das Suchfeld ein und drücken Sie die Eingabetaste. Wählen Sie die Zeile für die spezifische Instance aus, in der ein Diagramm für die CPUUtilizationMetrik für die Instance angezeigt wird. Wählen Sie das Stiftsymbol aus, um das Diagramm zu benennen. Wenn Sie den Zeitraum ändern möchten, müssen Sie einen der vordefinierten Werte oder custom (benutzerdefiniert) auswählen.



6. Um die Statistik oder den Zeitraum der Metrik zu ändern, müssen Sie die Registerkarte Graphed metrics (Grafisch dargestellte Metriken) auswählen. Wählen Sie die Spaltenüberschrift oder einen einzelnen Wert und anschließend einen anderen Wert aus.



So rufen Sie die CPU-Auslastung für eine bestimmte Instance ab (AWS CLI)

Verwenden Sie den folgenden get-metric-statisticsBefehl, um die CPUUtilizationMetrik für die angegebene Instance unter Verwendung des angegebenen Zeitraums und Zeitintervalls abzurufen:

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
 --period 3600 \
--statistics Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
--start-time 2022-10-18T23:18:00 --end-time 2022-10-19T23:18:00
```

Es folgt eine Beispielausgabe. Jeder Wert steht für den maximalen Prozentsatz der CPU-Auslastung für eine einzelne EC2 Instance.

```
{
    "Datapoints": [
        {
            "Timestamp": "2022-10-19T00:18:00Z",
            "Maximum": 0.33000000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T03:18:00Z",
            "Maximum": 99.670000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T07:18:00Z",
            "Maximum": 0.34000000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T12:18:00Z",
            "Maximum": 0.34000000000000002,
            "Unit": "Percent"
        }
    ],
    "Label": "CPUUtilization"
}
```

Aggregieren von Statistiken auf allen Instances

Sie können verfügbare Statistiken für die Instances aggregieren, für die die detaillierte Überwachung aktiviert ist. Instances, die die grundlegende Überwachung verwenden, sind nicht in den Zusammenfassungen enthalten. Bevor Sie die Statistiken abrufen können, die für alle Instances

aggregiert wurden, müssen Sie die detaillierte Überwachung (gegen Aufpreis) aktivieren, bei der Daten in 1-Minuten-Intervallen bereitgestellt werden.

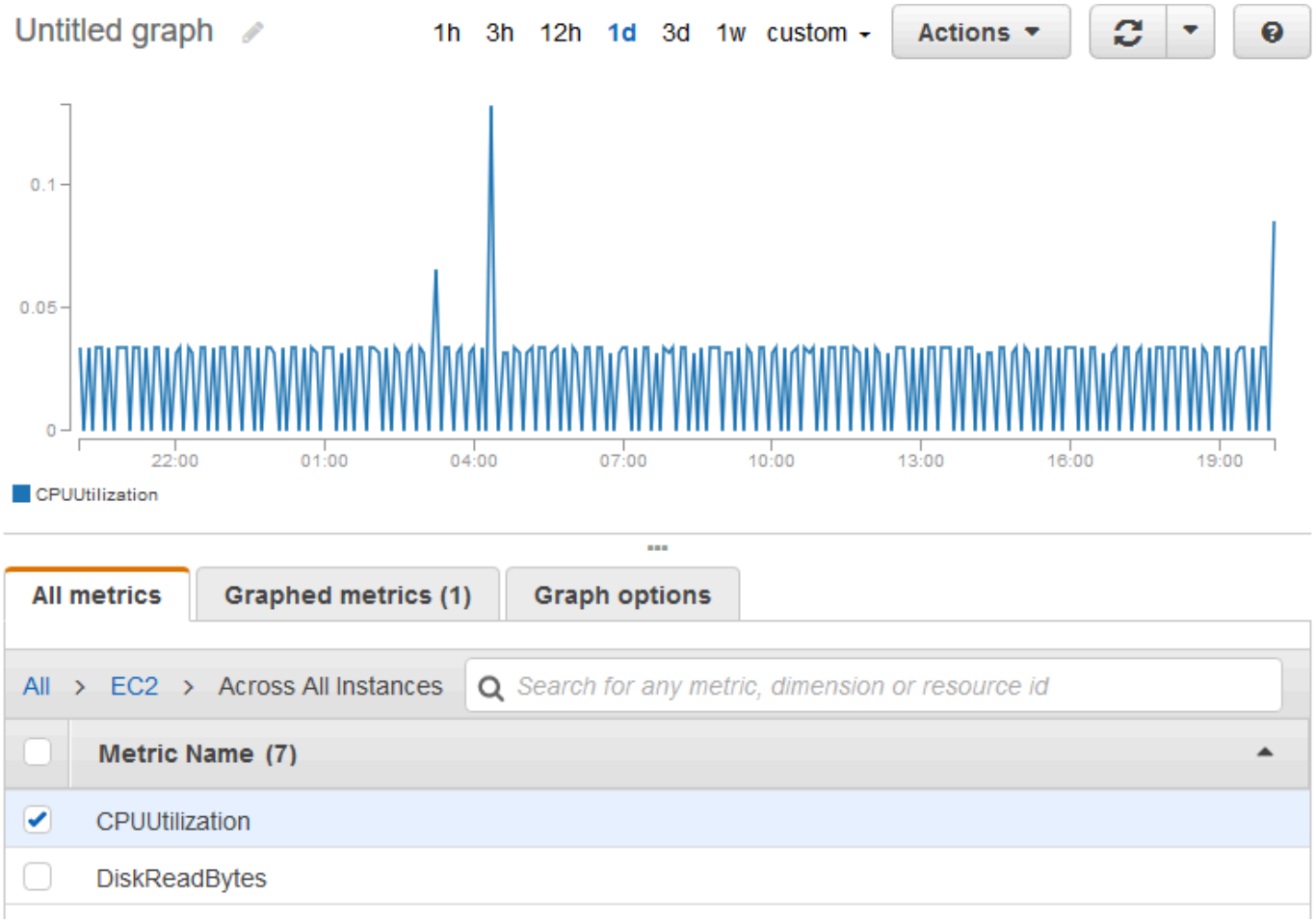
Beachten Sie, dass Amazon CloudWatch keine Daten regionsübergreifend AWS aggregieren kann. Die Metriken sind zwischen Regionen vollständig voneinander getrennt.

Dieses Beispiel zeigt Ihnen, wie Sie mithilfe einer detaillierten Überwachung die durchschnittliche CPU-Auslastung Ihrer EC2 Instances ermitteln können. Da keine Dimension angegeben ist, werden Statistiken für alle Dimensionen im `AWS/EC2` Namespace CloudWatch zurückgegeben.

> **Important**
>
> Diese Technik zum Abrufen aller Dimensionen in einem AWS Namespace funktioniert nicht für benutzerdefinierte Namespaces, die Sie auf Amazon veröffentlichen. CloudWatch Bei benutzerdefinierten Namespaces müssen Sie die vollständige Palette von Dimensionen angeben, die im Zusammenhang mit einem bestimmten Datenpunkt stehen, um Statistiken zu diesem Datenpunkt abzurufen.

So zeigen Sie die durchschnittliche CPU-Auslastung für Ihre gesamten Instances an (Konsole)

1. Öffnen Sie die Konsole unter. CloudWatch https://console.aws.amazon.com/cloudwatch/
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den EC2Namespace und dann Across All Instances aus.
4. Wählen Sie die Zeile aus CPUUtilization, die ein Diagramm für die Metrik für all Ihre EC2 Instances enthält. Wählen Sie das Stiftsymbol aus, um das Diagramm zu benennen. Wenn Sie den Zeitraum ändern möchten, müssen Sie einen der vordefinierten Werte oder custom (benutzerdefiniert) auswählen.



5. Um die Statistik oder den Zeitraum der Metrik zu ändern, müssen Sie die Registerkarte Graphed metrics (Grafisch dargestellte Metriken) auswählen. Wählen Sie die Spaltenüberschrift oder einen einzelnen Wert und anschließend einen anderen Wert aus.

So rufen Sie die durchschnittliche CPU-Auslastung für Ihre gesamten Instances ab (AWS CLI)

Verwenden Sie den get-metric-statisticsBefehl wie folgt, um den Durchschnitt der CPUUtilizationMetrik für Ihre Instances zu ermitteln.

```
aws cloudwatch get-metric-statistics \
    --namespace AWS/EC2 \
    --metric-name CPUUtilization \
    --period 3600  --statistics "Average" "SampleCount" \
    --start-time 2022-10-11T23:18:00 \
    --end-time 2022-10-12T23:18:00
```

Das Folgende ist eine Beispielausgabe:

```
{
    "Datapoints": [
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-12T07:18:00Z",
            "Average": 0.038235294117647062,
            "Unit": "Percent"
        },
        {
            "SampleCount": 240.0,
            "Timestamp": "2022-10-12T09:18:00Z",
            "Average": 0.16670833333333332,
            "Unit": "Percent"
        },
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-11T23:18:00Z",
            "Average": 0.041596638655462197,
            "Unit": "Percent"
        }
    ],
    "Label": "CPUUtilization"
}
```


Aggregierte Statistiken nach Amazon EC2 Auto Scaling Scaling-Gruppe

Sie können Statistiken für die EC2 Instances in einer Amazon EC2 Auto Scaling Scaling-Gruppe aggregieren. Beachten Sie, dass Amazon CloudWatch keine Daten regionsübergreifend AWS aggregieren kann. Die Metriken sind zwischen Regionen vollständig voneinander getrennt.

Dieses Beispiel zeigt Ihnen, wie Sie die Gesamtzahl der auf die Festplatte geschriebenen Byte für eine Amazon EC2 Auto Scaling Scaling-Gruppe abrufen. Die Summe wird für Zeiträume von 1 Minute für ein 24-Stunden-Intervall für alle EC2 Instances in der angegebenen Amazon EC2 Auto Scaling Scaling-Gruppe berechnet.

Zur Anzeige DiskWriteBytes für die Instances in einer Amazon EC2 Auto Scaling Scaling-Gruppe (Konsole)

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den EC2Namespace und dann Nach Auto Scaling Scaling-Gruppe.

4. Wählen Sie die Zeile für die DiskWriteBytesMetrik und die spezifische Amazon EC2 Auto Scaling Scaling-Gruppe aus, in der ein Diagramm für die Metrik für die Instances in der Amazon EC2 Auto Scaling Scaling-Gruppe angezeigt wird. Wählen Sie das Stiftsymbol aus, um das Diagramm zu benennen. Wenn Sie den Zeitraum ändern möchten, müssen Sie einen der vordefinierten Werte oder custom (benutzerdefiniert) auswählen.
5. Um die Statistik oder den Zeitraum der Metrik zu ändern, müssen Sie die Registerkarte Graphed metrics (Grafisch dargestellte Metriken) auswählen. Wählen Sie die Spaltenüberschrift oder einen einzelnen Wert und anschließend einen anderen Wert aus.

Zur Anzeige DiskWriteBytes für die Instances in einer Amazon EC2 Auto Scaling Scaling-Gruppe (AWS CLI)

Verwenden Sie den get-metric-statistics-Befehl wie folgt:

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name DiskWriteBytes
 --period 360 \
--statistics "Sum" "SampleCount" --dimensions Name=AutoScalingGroupName,Value=my-asg --
start-time 2022-10-16T23:18:00 --end-time 2022-10-18T23:18:00
```

Das Folgende ist eine Beispielausgabe:

```
{
    "Datapoints": [
        {
            "SampleCount": 18.0,
            "Timestamp": "2022-10-19T21:36:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "SampleCount": 5.0,
            "Timestamp": "2022-10-19T21:42:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        }
    ],
    "Label": "DiskWriteBytes"
}
```

Aggregieren von Statistiken nach AMI

Sie können Statistiken für Ihre Instances aggregieren, für die die detaillierte Überwachung aktiviert ist. Instances, die die grundlegende Überwachung verwenden, sind nicht in den Zusammenfassungen enthalten. Bevor Sie die Statistiken abrufen können, die für alle Instances aggregiert wurden, müssen Sie die detaillierte Überwachung (gegen Aufpreis) aktivieren, bei der Daten in 1-Minuten-Intervallen bereitgestellt werden.

Beachten Sie, dass Amazon CloudWatch keine Daten regionsübergreifend AWS aggregieren kann. Die Metriken sind zwischen Regionen vollständig voneinander getrennt.

Dieses Beispiel zeigt, wie Sie die durchschnittliche CPU-Auslastung für alle Instances abrufen, die ein bestimmtes Amazon Machine Image (AMI) verwenden. Der Durchschnitt wird über 60-Sekunden-Intervalle für einen Zeitraum von einem Tag berechnet.

So zeigen Sie die durchschnittliche CPU-Auslastung nach AMI an (Konsole)

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den EC2Namespace und dann Nach Bild-ID (AMI) aus.
4. Wählen Sie die Zeile für die CPUUtilizationMetrik und das spezifische AMI aus, wodurch ein Diagramm für die Metrik für das angegebene AMI angezeigt wird. Wählen Sie das Stiftsymbol aus, um das Diagramm zu benennen. Wenn Sie den Zeitraum ändern möchten, müssen Sie einen der vordefinierten Werte oder custom (benutzerdefiniert) auswählen.
5. Um die Statistik oder den Zeitraum der Metrik zu ändern, müssen Sie die Registerkarte Graphed metrics (Grafisch dargestellte Metriken) auswählen. Wählen Sie die Spaltenüberschrift oder einen einzelnen Wert und anschließend einen anderen Wert aus.

So rufen Sie die durchschnittliche CPU-Auslastung für eine Image-ID ab (AWS CLI)

Verwenden Sie den get-metric-statistics-Befehl wie folgt:

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
 --period 3600 \
--statistics Average --dimensions Name=ImageId,Value=ami-3c47a355 --start-
time 2022-10-10T00:00:00 --end-time 2022-10-11T00:00:00
```

Es folgt eine Beispielausgabe. Jeder Wert stellt einen durchschnittlichen Prozentsatz der CPU-Auslastung für die EC2 Instances dar, auf denen das angegebene AMI ausgeführt wird.


```
{
    "Datapoints": [
        {
            "Timestamp": "2022-10-10T07:00:00Z",
            "Average": 0.041000000000000009,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T14:00:00Z",
            "Average": 0.079579831932773085,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T06:00:00Z",
            "Average": 0.036000000000000011,
            "Unit": "Percent"
        }
    ],
    "Label": "CPUUtilization"
}
```


Die Überwachungsdiagramme für Ihre Instance anzeigen

Nachdem Sie eine Instance gestartet haben, können Sie die EC2 Amazon-Konsole öffnen und die Monitoring-Graphen für die Instance auf der Registerkarte Monitoring anzeigen. Jedes Diagramm basiert auf einer der verfügbaren EC2 Amazon-Metriken.

Folgende Diagramme sind verfügbar:

- Durchschnittliche CPU-Auslastung (in Prozent)
- Durchschnittliche Lesevorgänge (in Byte)
- Durchschnittliche Schreibvorgänge (in Byte)
- Maximaler Netzwerkeingang (in Byte)
- Maximaler Netzwerkausgang (in Byte)
- Zusammenfassung der Datenträger-Lesevorgänge (Anzahl)
- Zusammenfassung der Datenträger-Schreibvorgänge (Anzahl)

- Statuszusammenfassung (Beliebig)
- Statuszusammenfassung Instance (Anzahl)
- Statuszusammenfassung System (Anzahl)

Weitere Informationen zu den für die Diagramme bereitgestellten Metriken und Daten erhalten Sie unter CloudWatch Metriken, die für Ihre Instances verfügbar sind.

Stellen Sie Metriken mithilfe der CloudWatch Konsole grafisch dar

Sie können die CloudWatch Konsole auch verwenden, um von Amazon EC2 und anderen AWS Diensten generierte Metrikdaten grafisch darzustellen. Weitere Informationen finden Sie unter Metriken grafisch darstellen im CloudWatch Amazon-Benutzerhandbuch.

Erstellen Sie einen CloudWatch Alarm für eine Instance

Sie können einen CloudWatch Alarm erstellen, der die CloudWatch Metriken für eine Ihrer Instanzen überwacht. CloudWatchsendet Ihnen automatisch eine Benachrichtigung, wenn die Metrik einen von Ihnen angegebenen Schwellenwert erreicht. Sie können einen CloudWatch Alarm mit der EC2 Amazon-Konsole oder mit den erweiterten Optionen der CloudWatch Konsole erstellen.

Um einen Alarm mit der CloudWatch Konsole zu erstellen

Beispiele finden Sie unter CloudWatchAmazon-Alarme erstellen im CloudWatch Amazon-Benutzerhandbuch.

Um einen Alarm mit der EC2 Amazon-Konsole zu erstellen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und wählen Sie Aktionen, Überwachung und Fehlerbehebung, CloudWatch Alarme verwalten aus.
4. Wählen Sie auf der Detailseite CloudWatch Alarme verwalten unter Alarm hinzufügen oder bearbeiten die Option Alarm erstellen aus.
5. Wählen Sie unter Alarmbenachrichtigung, ob Sie Amazon Simple Notification Service (Amazon SNS)-Benachrichtigungen konfigurieren möchten. Geben Sie ein vorhandenes Amazon SNS-Thema ein oder geben Sie einen Namen ein, um ein neues Thema zu erstellen.
6. Wählen Sie unter Alarmaktion, ob Sie eine Aktion angeben möchten, die beim Auslösen des Alarms ausgeführt werden soll. Wählen Sie eine Aktion aus der Liste aus.

7. Wählen Sie unter Alarmschwellenwerte die Metrik und Kriterien für den Alarm aus. Wenn Sie beispielsweise einen Alarm erstellen möchten, der ausgelöst wird, wenn die CPU-Auslastung für einen Zeitraum von fünf Minuten 80 % erreicht, gehen Sie wie folgt vor:

   a. Behalten Sie die Standardeinstellung für Stichproben gruppieren nach (Durchschnitt) und Art der abzufragenden Daten (CPU-Auslastung) bei.

   b. Wählen Sie für Alarm bei die Option **>=** aus und geben Sie unter Prozent den Wert **`0.80`** ein.

   c. Geben unter Aufeinanderfolgender Zeitraum den Wert **1** ein und wählen Sie unter Zeitraum die Option 5 Minuten.

8. (Optional) Wählen Sie für Beispiel-Metrikdaten die Option Zu Dashboard hinzufügen aus.

9. Wählen Sie Erstellen aus.

Sie können Ihre CloudWatch Alarmeinstellungen von der EC2 Amazon-Konsole oder der CloudWatch Konsole aus bearbeiten. Wenn Sie Ihren Alarm löschen möchten, können Sie dies von der CloudWatch Konsole aus tun. Weitere Informationen finden Sie unter Bearbeiten oder Löschen eines CloudWatch Alarms im CloudWatch Amazon-Benutzerhandbuch.

Erstellen von Alarmen, mit denen eine Instance angehalten, beendet, neu gestartet oder wiederhergestellt wird

Mithilfe von CloudWatch Amazon-Alarmaktionen können Sie Alarme erstellen, die Ihre Instances automatisch stoppen, beenden, neu starten oder wiederherstellen. Sie können die Aktionen zum Anhalten oder Beenden nutzen, um Geld zu sparen, wenn eine Instance über einen längeren Zeitraum nicht ausgeführt werden muss. Sie können die Aktionen zum Neustarten oder Wiederherstellen verwenden, um diese Instances automatisch neu zu starten oder um sie – für den Fall, dass eine Systembeeinträchtigung eintritt – auf einer neuen Hardware wiederherzustellen.

> **Note**
>
> Abrechnungs- und Preisinformationen für Amazon CloudWatch Alarms finden Sie unter CloudWatch Abrechnung und Kosten im CloudWatch Amazon-Benutzerhandbuch.

Die `AWSServiceRoleForCloudWatchEvents` dienstbezogene Rolle ermöglicht es AWS , Alarmaktionen in Ihrem Namen durchzuführen. Wenn Sie zum ersten Mal einen Alarm in der AWS-

Managementkonsole, der oder der AWS CLI IAM-API erstellen, CloudWatch wird die dienstbezogene Rolle für Sie erstellt.

Es gibt eine Reihe von Szenarien, bei denen Sie Ihre Instance möglicherweise automatisch anhalten oder beenden möchten. Beispielsweise verwenden Sie Instances für die Stapelverarbeitung von Gehaltsabrechnungen oder wissenschaftliche Datenverarbeitungsaufgaben, die für einen bestimmten Zeitraum ausgeführt werden und ihre Arbeit anschließend abschließen. Anstatt diese Instances im Leerlauf beizubehalten (und damit Kosten anfallen zu lassen), können Sie sie auch anhalten oder beenden und so Geld sparen. Der Hauptunterschied zwischen der Verwendung einer Alarmaktion zum Anhalten und einer Alarmaktion zum Beenden besteht darin, dass Sie eine angehaltene Instance problemlos wieder neu starten können, wenn sie später wieder ausgeführt werden soll, und Sie dieselbe Instance-ID und dasselbe Stamm-Volume beibehalten können. Eine beendete Instance können Sie dagegen nicht neu starten. Stattdessen müssen Sie eine neue Instance starten. Wenn eine Instance angehalten oder beendet wird, gehen Daten auf Instance-Speicher-Volumes verloren.

Sie können die Aktionen Beenden, Beenden, Neustarten oder Wiederherstellen zu jedem Alarm hinzufügen, der für eine EC2 Amazon-spezifische Instanz-Metrik festgelegt ist, einschließlich grundlegender und detaillierter Überwachungsmetriken, die von Amazon CloudWatch (im `AWS/EC2` Namespace) bereitgestellt werden, sowie allen benutzerdefinierten Metriken, die die `InstanceId` Dimension enthalten, sofern sich ihr Wert auf eine gültige laufende EC2 Amazon-Instance bezieht.

> **Important**
>
> Alarme bei Statusprüfungen können vorübergehend in den `INSUFFICIENT_DATA`-Status wechseln, wenn metrische Datenpunkte fehlen. Dies ist zwar selten, kann aber passieren, wenn es zu einer Unterbrechung der metrischen Berichtssysteme kommt, selbst wenn eine Instance fehlerfrei ist. Wir empfehlen, den `INSUFFICIENT_DATA`-Status als fehlende Daten und nicht als Alarmverletzung zu behandeln, insbesondere wenn der Alarm so konfiguriert wird, dass eine Instance gestoppt, beendet, neu gestartet oder wiederhergestellt wird.

Konsolenunterstützung

Sie können Alarme mit der EC2 Amazon-Konsole oder der CloudWatch Konsole erstellen. Die Verfahren in dieser Dokumentation verwenden die EC2 Amazon-Konsole. Verfahren, die die CloudWatch Konsole verwenden, finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen von Alarmen, die eine Instance stoppen, beenden, neu starten oder wiederherstellen.

Berechtigungen

Sie benötigen die Möglichkeit, einen Alarm `iam:CreateServiceLinkedRole` zu erstellen oder zu ändern, der EC2 Alarmaktionen ausführt. Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

Inhalt

- Stoppaktionen zu CloudWatch Amazon-Alarmen hinzufügen
- Beendenaktionen zu CloudWatch Amazon-Alarmen hinzufügen
- Neustartaktionen zu CloudWatch Amazon-Alarmen hinzufügen
- Wiederherstellungsaktionen zu CloudWatch Amazon-Alarmen hinzufügen
- CloudWatch Amazon-Alarmaktionsszenarien

Stoppaktionen zu CloudWatch Amazon-Alarmen hinzufügen

Sie können einen Alarm erstellen, der eine EC2 Amazon-Instance stoppt, wenn ein bestimmter Schwellenwert erreicht wurde. Es kann beispielsweise sein, dass Sie Entwicklungs- oder Test-Instances ausführen und gelegentlich vergessen, diese herunterzufahren. Sie können einen Alarm einrichten, der ausgelöst wird, wenn die durchschnittliche prozentuale CPU-Auslastung 24 Stunden lang unter 10 Prozent fällt. Dies signalisiert, dass sich die Instance im Leerlauf befindet und nicht mehr verwendet wird. Sie können den Schwellenwert, die Dauer und den Zeitraum an Ihre Anforderungen anpassen. Außerdem haben Sie die Möglichkeit, eine Amazon-Simple-Notification-Service (Amazon SNS)-Benachrichtigung hinzuzufügen, damit Sie eine E-Mail erhalten, sobald der Alarm ausgelöst wird.

Instances, die ein Amazon-EBS-Volume als Root-Volume verwenden, können angehalten oder beendet werden. Instances, die den Instance-Speicher als Root-Volume verwenden, können dagegen nur beendet werden. Daten auf Instance-Speicher-Volumes gehen verloren, wenn die Instance beendet oder gestoppt wird.

Um einen Alarm zum Stoppen einer Instance im Leerlauf zu erstellen (EC2 Amazon-Konsole)

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und wählen Sie Aktionen, Überwachung und Fehlerbehebung, CloudWatch Alarme verwalten aus.

Alternativ können Sie das Pluszeichen (

) in der Spalte Alarm status (Alarmstatus) auswählen.

4. Gehen Sie auf der Seite „ CloudWatch Alarme verwalten“ wie folgt vor:

   a. Wählen Sie Create an alarm (Einen Alarm erstellen).

   b. Um eine E-Mail zu erhalten, wenn der Alarm ausgelöst wird, wählen Sie für Alarm notification (Alarmbenachrichtigung) ein vorhandenes Amazon SNS-Thema aus. Sie müssen zuerst mit der Amazon-SNS-Konsole ein Amazon-SNS-Thema erstellen. Weitere Informationen finden Sie unter Verwenden von Amazon SNS für application-to-person (A2P) -Messaging im Amazon Simple Notification Service Developer Guide.

   c. Schalten Sie die Alarm action (Alarmaktion) ein und wählen Sie Stop (Anhalten).

   d. Wählen Sie für Group samples by (Beispiele gruppieren nach) und Type of data to sample (Datentypen, die in Beispielen aufgeführt werden sollen) eine Statistik und eine Metrik. Wählen Sie in diesem Beispiel die Optionen Average und CPU Utilization (CPU-Nutzung).

   e. Geben Sie für Alarm When (Alarm bei) und Percent (Prozent) den metrischen Schwellenwert an. In diesem Beispiel geben Sie <= und 10 Prozent an.

   f. Geben Sie für Consecutive period (Aufeinanderfolgender Zeitraum) und Period (Zeitraum) den Bewertungszeitraum für den Alarm an. Geben Sie in diesem Beispiel 1 aufeinanderfolgende Periode von 5 Minuten an.

   g. Amazon erstellt CloudWatch automatisch einen Alarmnamen für Sie. Um den Namen zu ändern, geben Sie für Alarm name (Alarmname) einen neuen Namen ein. Alarmnamen dürfen nur ASCII-Zeichen enthalten.

      > **Note**
      >
      > Sie können die Alarmkonfiguration vor dem Erstellen des Alarms gemäß Ihren eigenen Anforderungen anpassen oder diese später ändern. Dies umfasst die Einstellungen für Metrik, Schwellenwert, Dauer, Aktion und Benachrichtigung. Nachdem Sie einen Alarm erstellt haben, können Sie seinen Namen aber nicht mehr bearbeiten.

   h. Wählen Sie Erstellen aus.

Beendenaktionen zu CloudWatch Amazon-Alarmen hinzufügen

Sie können einen Alarm erstellen, der eine EC2 Instance automatisch beendet, wenn ein bestimmter Schwellenwert erreicht wurde (sofern der Kündigungsschutz für die Instance nicht aktiviert ist). Es kann beispielsweise sein, dass Sie eine Instance beenden möchten, sobald diese ihre Arbeit abgeschlossen hat, und dass Sie die Instance nicht noch einmal benötigen. Wenn Sie die Instance unter Umständen später noch einmal verwenden möchten, sollten Sie die Instance nur anhalten, anstatt sie zu beenden. Daten auf Instance-Speicher-Volumes gehen verloren, wenn die Instance beendet wird. Informationen zum Aktivieren und Deaktivieren des Beendigungsschutzes für eine Instance finden Sie unter Beendigungsschutz für Instances ändern.

Um einen Alarm zu erstellen, um eine Instance im Leerlauf zu beenden (EC2 Amazon-Konsole)

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und wählen Sie Aktionen, Überwachung und Fehlerbehebung, CloudWatch Alarme verwalten aus.

   Alternativ können Sie das Pluszeichen (

) in der Spalte Alarm status (Alarmstatus) auswählen.
4. Gehen Sie auf der Seite „ CloudWatch Alarme verwalten“ wie folgt vor:

   a. Wählen Sie Create an alarm (Einen Alarm erstellen).

   b. Um eine E-Mail zu erhalten, wenn der Alarm ausgelöst wird, wählen Sie für Alarm notification (Alarmbenachrichtigung) ein vorhandenes Amazon SNS-Thema aus. Sie müssen zuerst mit der Amazon-SNS-Konsole ein Amazon-SNS-Thema erstellen. Weitere Informationen finden Sie unter Verwenden von Amazon SNS für application-to-person (A2P) -Messaging im Amazon Simple Notification Service Developer Guide.

   c. Schalten Sie die Alarm action (Alarmaktion) ein und wählen Sie Terminate (Beenden).

   d. Wählen Sie für Group samples by (Beispiele gruppieren nach) und Type of data to sample (Datentypen, die in Beispielen aufgeführt werden sollen) eine Statistik und eine Metrik. Wählen Sie in diesem Beispiel die Optionen Average und CPU Utilization (CPU-Nutzung).

   e. Geben Sie für Alarm When (Alarm bei) und Percent (Prozent) den metrischen Schwellenwert an. In diesem Beispiel geben Sie => und 10 Prozent an.

f. Geben Sie für Consecutive period (Aufeinanderfolgender Zeitraum) und Period (Zeitraum) den Bewertungszeitraum für den Alarm an. Geben Sie in diesem Beispiel 24 aufeinanderfolgende Perioden von 1 Hour (einer Stunde) an.

g. Amazon erstellt CloudWatch automatisch einen Alarmnamen für Sie. Um den Namen zu ändern, geben Sie für Alarm name (Alarmname) einen neuen Namen ein. Alarmnamen dürfen nur ASCII-Zeichen enthalten.

> **Note**
>
> Sie können die Alarmkonfiguration vor dem Erstellen des Alarms gemäß Ihren eigenen Anforderungen anpassen oder diese später ändern. Dies umfasst die Einstellungen für Metrik, Schwellenwert, Dauer, Aktion und Benachrichtigung. Nachdem Sie einen Alarm erstellt haben, können Sie seinen Namen aber nicht mehr bearbeiten.

h. Wählen Sie Erstellen aus.

Neustartaktionen zu CloudWatch Amazon-Alarmen hinzufügen

Sie können einen CloudWatch Amazon-Alarm erstellen, der eine EC2 Amazon-Instance überwacht und die Instance automatisch neu startet. Die Alarmaktion zum Neustarten wird für Instance-Zustandsprüfungsfehler empfohlen (im Gegensatz zur Alarmaktion zum Wiederherstellen, die sich für System-Zustandsprüfungsfehler eignet). Ein Neustart einer Instance entspricht einem Neustart des Betriebssystems. In den meisten Fällen dauert es nur wenige Minuten, um die Instance neu zu starten. Wenn Sie eine Instance neu starten, verbleibt sie auf demselben physischen Host, sodass die Instance ihren öffentlichen DNS- Namen, ihre private IP-Adresse sowie alle Daten auf ihren Instance-Speicher-Volumes behält.

Im Gegensatz zum Anhalten und erneuten Starten der Instance beginnt mit dem erneuten Hochfahren einer Instance kein neuer Instance-Abrechnungszeitraum (mit einer minimalen 1-Minuten-Abrechnung). Daten auf Instance-Speicher-Volumes werden beibehalten, wenn die Instance neu gestartet wird. Die Instance-Speicher-Volumes müssen nach einem Neustart erneut in das Dateisystem gemountet werden. Weitere Informationen finden Sie unter Eine Amazon-EC2-Instance neu starten.

> **Important**
>
> Um eine Race-Bedingung zwischen der Neustart- und der Wiederherstellungsaktion zu vermeiden, sollten Sie für den Neustartalarm und den Wiederherstellungsalarm nicht die gleiche Anzahl von Auswertungszeiträumen festlegen. Wir empfehlen, dass Sie Neustartalarme zu drei Auswertungszeiträumen von jeweils einer Minute festlegen. Weitere Informationen finden Sie unter Auswertung eines Alarms im CloudWatch Amazon-Benutzerhandbuch.

Um einen Alarm für den Neustart einer Instance zu erstellen (EC2 Amazon-Konsole)

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und wählen Sie Aktionen, Überwachung und Fehlerbehebung, CloudWatch Alarme verwalten aus.

   Alternativ können Sie das Pluszeichen (

) in der Spalte Alarm status (Alarmstatus) auswählen.
4. Gehen Sie auf der Seite „ CloudWatch Alarme verwalten“ wie folgt vor:

   a. Wählen Sie Create an alarm (Einen Alarm erstellen).

   b. Um eine E-Mail zu erhalten, wenn der Alarm ausgelöst wird, wählen Sie für Alarm notification (Alarmbenachrichtigung) ein vorhandenes Amazon SNS-Thema aus. Sie müssen zuerst mit der Amazon-SNS-Konsole ein Amazon-SNS-Thema erstellen. Weitere Informationen finden Sie unter Verwenden von Amazon SNS für application-to-person (A2P) -Messaging im Amazon Simple Notification Service Developer Guide.

   c. Schalten Sie die Alarm action (Alarmaktion) ein und wählen Sie Reboot (Neustart).

   d. Wählen Sie für Group samples by (Beispiele gruppieren nach) und Type of data to sample (Datentypen, die in Beispielen aufgeführt werden sollen) eine Statistik und eine Metrik. In diesem Beispiel wählen Sie Average (Durchschnitt) und Status check failed: instance (Statusprüfung fehlgeschlagen: Instance).

   e. Geben Sie für Consecutive period (Aufeinanderfolgender Zeitraum) und Period (Zeitraum) den Bewertungszeitraum für den Alarm an. Geben Sie in diesem Beispiel 3

aufeinanderfolgende Perioden von 1 Minute an. Wenn 1 Minute deaktiviert ist, müssen Sie die detaillierte Überwachung aktivieren, oder Sie können stattdessen 5 Minuten wählen.

f. Amazon erstellt CloudWatch automatisch einen Alarmnamen für Sie. Um den Namen zu ändern, geben Sie für Alarm name (Alarmname) einen neuen Namen ein. Alarmnamen dürfen nur ASCII-Zeichen enthalten.

g. Wählen Sie Erstellen aus.

Wiederherstellungsaktionen zu CloudWatch Amazon-Alarmen hinzufügen

Sie können einen CloudWatch Amazon-Alarm erstellen, der eine EC2 Amazon-Instance überwacht. Wenn die Instance aufgrund eines zugrunde liegenden Hardwarefehlers oder eines Problems, das eine Reparatur AWS erfordert, beeinträchtigt wird, können Sie die Instance automatisch wiederherstellen. Beendete Instances können nicht wiederhergestellt werden. Eine wiederhergestellte Instance ist mit der ursprünglichen Instance identisch. Dies schließt auch die Instance-ID, private IP-Adressen, Elastic IP-Adressen und alle Instance-Metadaten mit ein.

CloudWatch verhindert, dass Sie eine Wiederherstellungsaktion zu einem Alarm hinzufügen, der sich auf einer Instance befindet, die keine Wiederherstellungsaktionen unterstützt.

Wird der Alarm `StatusCheckFailed_System` ausgelöst und die Aktion zum Wiederherstellen initiiert, werden Sie über das Amazon SNS-Thema, das Sie bei der Erstellung des Alarms gewählt haben und das mit der Aktion zum Wiederherstellen verknüpft ist, darüber benachrichtigt. Während der Instance-Wiederherstellung wird die Instance bei einem Instance-Neustart migriert und alle im Speicher befindlichen Daten gehen verloren. Wenn der Vorgang abgeschlossen ist, wird die Information in dem SNS-Thema, das Sie für den Alarm konfiguriert haben, veröffentlicht. Alle Personen, die das SNS-Thema abonniert haben, erhalten eine Benachrichtigung per E-Mail, in der auch der Status des Wiederherstellungsversuchs und weitere Anweisungen enthalten sind. Sie bemerken, dass auf der wiederhergestellten Instance ein Instance-Neustart durchgeführt wird.

> **Note**
>
> Die Aktion zum Wiederherstellen kann nur mit `StatusCheckFailed_System` verwendet werden, nicht mit `StatusCheckFailed_Instance`.

Hier sind die Probleme aufgeführt, die dazu führen können, dass System-Statusprüfungen fehlschlagen:

- Verlust der Netzwerkverbindung
- Systemstromausfall
- Softwareprobleme auf dem physischen Host
- Hardwareprobleme auf dem physischen Host, die die Erreichbarkeit des Netzwerks beeinträchtigen

Die Wiederherstellungsaktion wird nur auf Instances unterstützt, die bestimmte Kriterien erfüllen. Weitere Informationen finden Sie unter Automatische Instance-Wiederherstellung.

Wenn Ihre Instance über eine öffentliche IP-Adresse verfügt, wird diese nach der Wiederherstellung beibehalten.

> **Important**
>
> Um eine Race-Bedingung zwischen der Neustart- und der Wiederherstellungsaktion zu vermeiden, sollten Sie für den Neustartalarm und den Wiederherstellungsalarm nicht die gleiche Anzahl von Auswertungszeiträumen festlegen. Wir empfehlen, dass Sie Wiederherstellungsalarme zu zwei Auswertungszeiträumen von jeweils einer Minute festlegen. Weitere Informationen finden Sie unter Auswertung eines Alarms im CloudWatch Amazon-Benutzerhandbuch.

Um einen Alarm zur Wiederherstellung einer Instance zu erstellen (EC2 Amazon-Konsole)

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und wählen Sie Aktionen, Überwachung und Fehlerbehebung, CloudWatch Alarme verwalten aus.

   Alternativ können Sie das Pluszeichen (

) in der Spalte Alarm status (Alarmstatus) auswählen.
4. Gehen Sie auf der Seite „ CloudWatch Alarme verwalten“ wie folgt vor:

   a. Wählen Sie Create an alarm (Einen Alarm erstellen).

   b. Um eine E-Mail zu erhalten, wenn der Alarm ausgelöst wird, wählen Sie für Alarm notification (Alarmbenachrichtigung) ein vorhandenes Amazon SNS-Thema aus. Sie

müssen zuerst mit der Amazon-SNS-Konsole ein Amazon-SNS-Thema erstellen. Weitere Informationen finden Sie unter Verwenden von Amazon SNS für application-to-person (A2P) -Messaging im Amazon Simple Notification Service Developer Guide.

> **Note**
>
> Benutzer müssen das angegebene SNS-Thema abonnieren, um E-Mail-Benachrichtigungen zu erhalten, wenn der Alarm ausgelöst wird. The erhält Root-Benutzer des AWS-Kontos immer E-Mail-Benachrichtigungen, wenn automatische Aktionen zur Instance-Wiederherstellung ausgeführt werden, auch wenn kein SNS-Thema angegeben ist oder der Root-Benutzer das angegebene SNS-Thema nicht abonniert hat.

c. Schalten Sie die Alarm action (Alarmaktion) ein und wählen Sie Recover (Wiederherstellen).

d. Wählen Sie für Group samples by (Beispiele gruppieren nach) und Type of data to sample (Datentypen, die in Beispielen aufgeführt werden sollen) eine Statistik und eine Metrik. In diesem Beispiel wählen Sie Average (Durchschnitt) und Status check failed: system (Statusprüfung fehlgeschlagen: System).

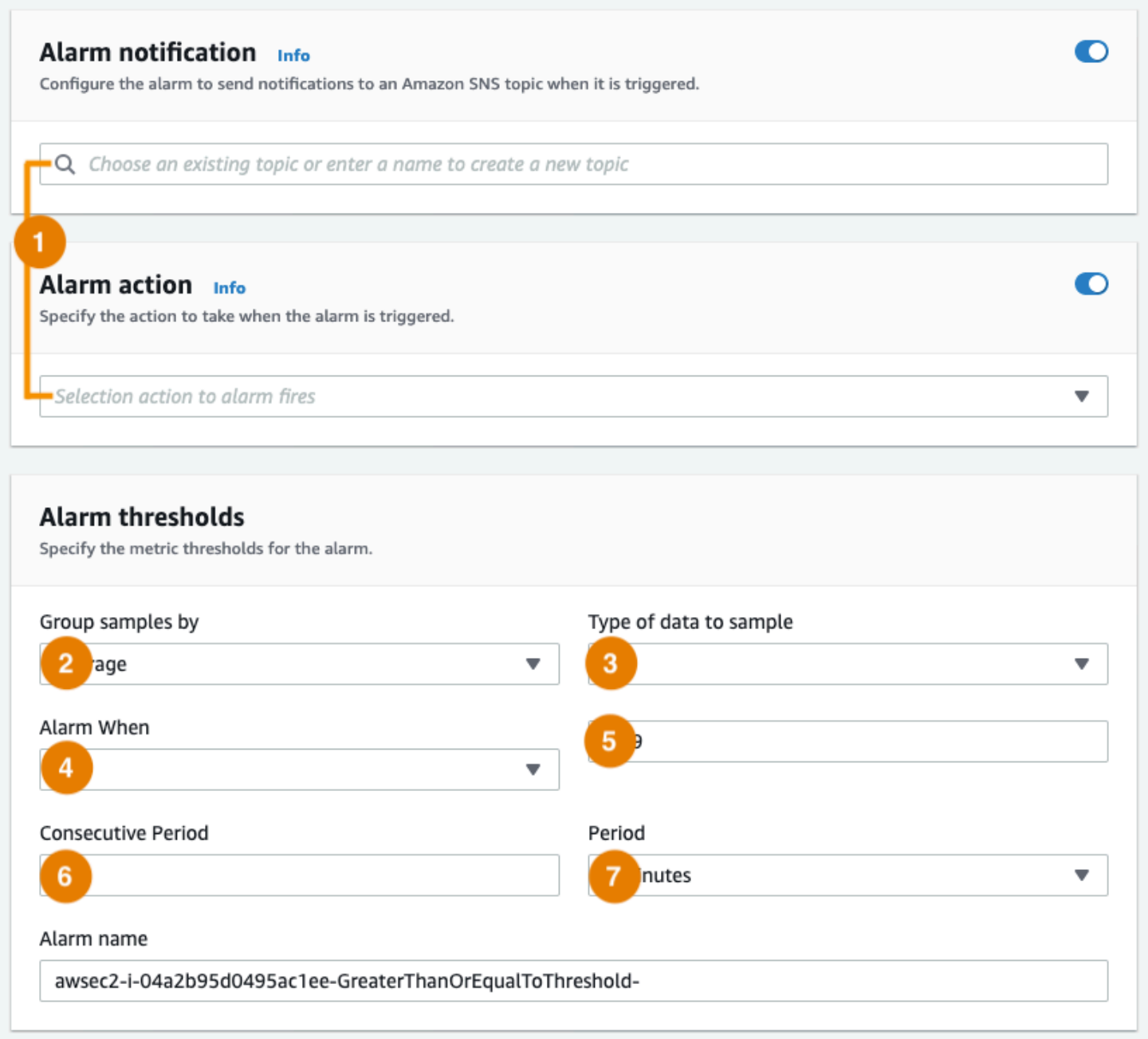
e. Geben Sie für Consecutive period (Aufeinanderfolgender Zeitraum) und Period (Zeitraum) den Bewertungszeitraum für den Alarm an. Geben Sie in diesem Beispiel 2 aufeinanderfolgende Perioden von 1 Minute an. Wenn 1 Minute deaktiviert ist, müssen Sie die detaillierte Überwachung aktivieren, oder Sie können stattdessen 5 Minuten wählen.

f. Amazon erstellt CloudWatch automatisch einen Alarmnamen für Sie. Um den Namen zu ändern, geben Sie für Alarm name (Alarmname) einen neuen Namen ein. Alarmnamen dürfen nur ASCII-Zeichen enthalten.

g. Wählen Sie Erstellen aus.

CloudWatch Amazon-Alarmaktionsszenarien

Sie können die EC2 Amazon-Konsole verwenden, um Alarmaktionen zu erstellen, die eine EC2 Amazon-Instance stoppen oder beenden, wenn bestimmte Bedingungen erfüllt sind. In den folgenden Screenshots der Konsolenseite, auf der Sie die Alarmaktionen festlegen, haben wir die Einstellungen nummeriert. Wir haben auch die Einstellungen in den darauffolgenden Szenarien nummeriert, damit Sie die entsprechenden Aktionen leichter erstellen können.



Szenario 1: Anhalten von im Leerlauf befindlichen Entwicklungs- und Test-Instances

Erstellen Sie einen Alarm, mit dem eine für die Software-Entwicklung oder das Testing bestimmte Instance angehalten wird, wenn sie sich seit mindestens einer Stunde im Leerlauf befindet.

Einstellung	Wert
1	Stoppen

Einstellung	Wert
2	Maximum
3	CPU-Auslastung
4	<=
5	10 %
6	1
7	1 Stunde

Szenario 2: Anhalten von im Leerlauf befindlichen Instances

Erstellen Sie einen Alarm, mit dem eine Instance angehalten und eine E-Mail gesendet wird, wenn sich die Instance seit 24 Stunden im Leerlauf befindet.

Einstellung	Wert
1	Anhalten und Senden einer E-Mail
2	Durchschnitt
3	CPU-Auslastung
4	<=
5	5 %
6	24
7	1 Stunde

Szenario 3: Senden von E-Mails zu Webservern mit ungewöhnlich hohem Datenverkehrsaufkommen

Erstellen Sie einen Alarm, mit dem eine E-Mail gesendet wird, wenn für eine Instance pro Tag der Grenzwert von 10 GB an ausgehendem Netzwerkdatenverkehr überschritten wird.

Einstellung	Wert
1	E-Mail
2	Summe
3	Netzwerkausgang
4	>
5	10 GB
6	24
7	1 Stunde

Szenario 4: Anhalten von Webservern mit ungewöhnlich hohem Datenverkehrsaufkommen

Erstellen Sie einen Alarm, mit dem eine Instance angehalten und eine Textnachricht (SMS) gesendet wird, wenn der ausgehende Datenverkehr den Grenzwert von 1 GB pro Stunde überschreitet.

Einstellung	Wert
1	Anhalten und Senden einer SMS
2	Summe
3	Netzwerkausgang
4	>
5	1 GB
6	1
7	1 Stunde

Szenario 5: Anhalten einer beeinträchtigten Instance

Erstellen Sie einen Alarm, mit dem eine Instance angehalten wird, die drei aufeinander folgende Statusprüfungen (im Abstand von 5 Minuten) nicht bestanden hat.

Einstellung	Wert
1	Stoppen
2	Durchschnitt
3	Statusprüfung fehlgeschlagen: System
4	-
5	-
6	1
7	15 Minuten

Szenario 6: Beenden von Instances nach dem Abschluss von Stapelverarbeitungsaufträgen

Erstellen Sie einen Alarm, mit dem eine Instance für Stapelaufträge beendet wird, wenn keine Ergebnisdaten mehr gesendet werden.

Einstellung	Wert
1	Beenden
2	Maximum
3	Netzwerkausgang
4	<=
5	100 000 Bytes
6	1

Einstellung	Wert
7	5 Minuten

Automatisieren von Amazon EC2 mithilfe von EventBridge

Sie können Amazon EventBridge verwenden, um Ihr AWS-Services zu automatisieren und automatisch auf Systemereignisse zu reagieren, wie z. B. Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen. Ereignisse von AWS-Services werden in EventBridge nahezu in Echtzeit bereitgestellt. Sie können Regeln erstellen, um anzugeben, an welchen Ereignissen Sie interessiert sind, und welche Aktionen auszuführen sind, wenn ein Ereignis mit einer Regel übereinstimmt. Die folgenden Aktionen können beispielsweise automatisch ausgelöst werden:

- Aufrufen einer AWS Lambda-Funktion
- Aufrufen eines Amazon-EC2-Ausführungsbefehls
- Weitergabe des Ereignisses an Amazon Kinesis Data Streams
- Aktivieren eines AWS Step Functions-Status-Automaten
- Benachrichtigen eines Amazon-SNS-Themas
- Benachrichtigen einer Amazon-SQS-Warteschlange

Die folgenden Beispiele zeigen, wie Sie EventBridge mit Amazon EC2 verwenden können:

- Aktivieren Sie eine Lambda-Funktion immer dann, wenn eine Instance in den Ausführungsstatus übergeht.
- Benachrichtigen Sie ein Amazon-SNS-Thema, wenn ein Amazon-EBS-Volume erstellt oder geändert wird.
- Senden Sie mit Amazon-EC2-Ausführungsbefehl einen Befehl an eine oder mehrere Amazon-EC2-Instances, wenn ein bestimmtes Ereignis in einem anderen AWS-Service eintritt.

Weitere Informationen finden Sie im Benutzerhandbuch für Amazon EventBridge.

Amazon-EC2-Ereignistypen

Amazon EC2 unterstützt die folgenden Ereignistypen:

- EC2-AMI-Statusänderung
- EC2 Schnellstart Benachrichtigung über Statusänderungen
- EC2-Flotten-Fehler
- Informationen zur EC2-Flotte
- Ändern der EC2-Flotten-Instance
- Ändern der Anforderung der EC2-Flotte-Spot-Instance
- Verändern des EC2-Flottenzustand
- Empfehlung zum Ausgleich einer EC2-Instance
- Benachrichtigung über die Statusänderung für eine EC2-Instance
- EC2-Spot-Flottenfehler
- Informationen zur EC2-Spot-Flotte
- Ändern der EC2-Spot-Flotten-Instance
- Ändern der Anforderung der EC2-Spot-Flotten-Spot-Instance
- Verändern des EC2-Spot-Flottenzustands
- Unterbrechungswarnung zur EC2-Spot-Instance
- Erfüllung einer EC2-Spot-Instance-Anforderung
- Benachrichtigung zur EC2-ODCR-Nichtauslastung

Weitere Informationen zu den von Amazon EBS unterstützten Ereignistypen finden Sie unter Amazon EventBridge für Amazon EBS.

Amazon-EC2-API-Aufrufe mit AWS CloudTrail protokollieren

Die Amazon-EC2-API ist in AWS CloudTrail integriert, einem Service, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS-Service durchgeführten Aktionen bereitstellt. CloudTrail erfasst alle Amazon-EC2-API-Aufrufe als Ereignisse. Die erfassten Aufrufe umfassen von der Konsole ausgeführte Aufrufe. Anhand der von CloudTrail gesammelten Informationen können Sie feststellen, welche Anfrage an die Amazon-EC2-API gestellt wurde, von welcher IP-Adresse aus die Anfrage gestellt wurde und wann sie gestellt wurde.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Anmeldeinformationen des Root-Benutzers oder des Benutzers gestellt wurde.

- Die Anforderung wurde im Namen eines IAM-Identity-Center-Benutzers erstellt.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen gesendet wurde AWS-Service.

Bei Kontoerstellung ist CloudTrail standardmäßig in AWS-Konto aktiviert und Sie haben automatisch Zugriff auf den CloudTrail-Ereignisverlauf. Der CloudTrail-Ereignisverlauf stellt eine anzeigbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der Verwaltungsereignisse der letzten 90 Tage in einer AWS-Region bereit. Weitere Informationen finden Sie unter Arbeiten mit dem CloudTrail-Ereignisverlauf im AWS CloudTrail-Benutzerhandbuch. Für die Anzeige des Eventverlaufs fallen keine CloudTrail-Gebühren an.

Erstellen Sie einen Trail oder einen Ereignisdatenspeicher in CloudTrail Lake, um Aktivitäten und Ereignisse in Ihrer AWS-Konto über 90 Tage hinaus fortlaufend aufzuzeichnen.

CloudTrail-Trails

Ein Trail ermöglicht es CloudTrail, Protokolldateien in einem Amazon-S3-Bucket bereitzustellen. Trails, die mit der AWS-Managementkonsole erstellt wurden, sind multiregional. Sie können mithilfe von AWS CLI einen Einzel-Region- oder einen Multi-Region-Trail erstellen. Das Erstellen eines Multi-Region-Trails wird empfohlen, da Sie so die Aktivitäten in allen AWS-Regionen in Ihrem Konto erfassen. Wenn Sie einen Einzel-Region-Trail erstellen, können Sie nur die Ereignisse anzeigen, die im AWS-Region des Trails protokolliert wurden. Weitere Informationen zu Trails finden Sie unter Erstellen eines Trails für Ihr AWS-Konto und Erstellen eines Trails für eine Organisation im AWS CloudTrail-Benutzerhandbuch.

Sie können eine Kopie Ihrer laufenden Verwaltungsereignisse kostenlos von CloudTrail an Ihren Amazon-S3-Bucket senden, indem Sie einen Trail erstellen. Es fallen jedoch Speichergebühren für Amazon S3 an. Weitere Informationen zu CloudTrail-Preisen finden Sie unter AWS CloudTrail – Preise. Informationen zu Amazon-S3-Preisen finden Sie unter Amazon S3 – Preise.

CloudTrail-Lake-Ereignisdatenspeicher

Mit CloudTrail Lake können Sie SQL-basierte Abfragen zu Ihren Ereignissen ausführen. CloudTrail Lake konvertiert vorhandene Ereignisse im zeilenbasierten JSON-Format in das Apache ORC-Format. ORC ist ein spaltenförmiges Speicherformat, das für den schnellen Abruf von Daten optimiert ist. Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien

basieren, die Sie mit Hilfe von erweiterten Ereignisselektoren auswählen. Die Selektoren, die Sie auf einen Ereignisdatenspeicher anwenden, steuern, welche Ereignisse bestehen bleiben und für Sie zur Abfrage verfügbar sind. Weitere Informationen zu CloudTrail Lake finden Sie unter Arbeiten mit AWS CloudTrail-Lake im AWS CloudTrail-Benutzerhandbuch.

Für CloudTrail-Lake-Ereignisdatenspeicher und -abfragen fallen Gebühren an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die Preisoption aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Weitere Informationen zu CloudTrail-Preisen finden Sie unter AWS CloudTrail – Preise.

Amazon-EC2-API-Verwaltungsereignisse in CloudTrail

Verwaltungsereignisse liefern Informationen zu Verwaltungsvorgängen, die für Ressourcen in Ihrem AWS-Konto ausgeführt werden. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. CloudTrail protokolliert standardmäßig Verwaltungsereignisse.

Alle Amazon-EC2-API-Aktionen werden als Verwaltungsereignisse protokolliert. Eine Liste der API-Aktionen, die von CloudTrail protokolliert werden, finden Sie in der Amazon-EC2-API-Referenz. Beispielsweise werden Aufrufe der RunInstances, DescribeInstances und StopInstances-Aktionen als Verwaltungsereignisse protokolliert.

Amazon-EC2-API-Ereignisbeispiele

Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte API-Aktion, das Datum und die Uhrzeit der Operation, Anforderungsparameter usw. CloudTrail-Protokolldateien sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und Ereignisse und erscheinen daher in keiner bestimmten Reihenfolge.

Der folgende Protokolldatensatz zeigt, dass ein Benutzer eine Instance beendet hat.

```
{
   "Records":[
      {
         "eventVersion":"1.03",
         "userIdentity":{
            "type":"Root",
            "principalId":"123456789012",
```

```
            "arn":"arn:aws:iam::123456789012:root",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"user"
         },
         "eventTime":"2016-05-20T08:27:45Z",
         "eventSource":"ec2.amazonaws.com",
         "eventName":"TerminateInstances",
         "awsRegion":"us-west-2",
         "sourceIPAddress":"198.51.100.1",
         "userAgent":"aws-cli/1.10.10 Python/2.7.9 Windows/7botocore/1.4.1",
         "requestParameters":{
            "instancesSet":{
               "items":[{
                  "instanceId":"i-1a2b3c4d"
               }]
            }
         },
         "responseElements":{
            "instancesSet":{
               "items":[{
                  "instanceId":"i-1a2b3c4d",
                  "currentState":{
                     "code":32,
                     "name":"shutting-down"
                  },
                  "previousState":{
                     "code":16,
                     "name":"running"
                  }
               }]
            }
         },
         "requestID":"be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
         "eventID":"6e12345-2a4e-417c-aa78-7594fEXAMPLE",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```


Informationen zu den Inhalten von CloudTrail-Datensätzen finden Sie unter CloudTrail-Datensatzinhalte im AWS CloudTrail-Benutzerhandbuch.

Prüfung von Verbindungen, die über EC2-Instance-Connect hergestellt wurden

Verwenden Sie AWS CloudTrail, um die Benutzer zu prüfen, die sich über EC2-Instance-Connect mit Ihren Instances verbinden.

Prüfen der SSH-Aktivität über EC2 Instance Connect mit der AWS CloudTrail-Konsole

1. Öffnen Sie die CloudTrail-Konsole unter https://console.aws.amazon.com/cloudtrail/.
2. Stellen Sie sicher, dass Sie sich in der korrekten Region befinden.
3. Wählen Sie im Navigationsbereich Event history (Ereignisverlauf) aus.
4. Wählen Sie für Filter Event source (Ereignisquelle), ec2-instance-connect.amazonaws.com aus.
5. (Optional) Wählen Sie für Time range (Zeitraum) einen Zeitraum aus.
6. Wählen Sie das Symbol Refresh events (Ereignisse aktualisieren) aus.
7. Die Seite zeigt die Ereignisse, die den SendSSHPublicKey-API-Aufrufen entsprechen. Erweitern Sie ein Ereignis mit dem Pfeil, um zusätzliche Details anzuzeigen, wie den Benutzernamen und AWS-Zugriffsschlüssel, der für die Herstellung der SSH-Verbindung verwendet wurde, und die Quell-ID-Adresse.
8. Zum Anzeigen der vollständigen Ereignisinformationen im JSON-Format wählen Sie View event (Ereignis anzeigen). Das Feld requestParameters enthält die Ziel-Instance-ID, den Benutzernamen für das Betriebssystem und den öffentlichen Schlüssel, der zur Herstellung der SSH-Verbindung verwendet wurde.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
        "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
        "accountId": "123456789012",
        "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
        "userName": "IAM-friendly-name",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-09-21T21:37:58Z"}
        }
    },
```

```
    "eventTime": "2018-09-21T21:38:00Z",
    "eventSource": "ec2-instance-connect.amazonaws.com",
    "eventName": "SendSSHPublicKey ",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "123.456.789.012",
    "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
    "requestParameters": {
        "instanceId": "i-0123456789EXAMPLE",
        "osUser": "ec2-user",
        "SSHKey": {
            "publicKey": "ssh-rsa ABCDEFGHIJKLMNO01234567890EXAMPLE"
        }
     },
    "responseElements": null,
    "requestID": "1a2s3d4f-bde6-11e8-a892-f7ec64543add",
    "eventID": "1a2w3d4r5-a88f-4e28-b3bf-30161f75be34",
    "eventType": "AwsApiCall",
    "recipientAccountId": "0987654321"
}
```


Wenn Sie Ihr AWS-Konto so konfiguriert haben, dass es CloudTrail-Ereignisse in einem S3-Bucket erfasst, können Sie die Informationen herunterladen und programmatisch prüfen. Weitere Informationen finden Sie unter Abrufen und Anzeigen der CloudTrail-Protokolldateien im AWS CloudTrail-Benutzerhandbuch.

Überwachen Sie .NET- und SQL Server-Anwendungen mithilfe von CloudWatch Application Insights

CloudWatch Application Insights unterstützt Sie bei der Überwachung Ihrer .NET- und SQL Server-Anwendungen, die EC2 Amazon-Instances zusammen mit anderen AWS Anwendungsressourcen verwenden. Der Service identifiziert Schlüsselmetrikprotokolle und Alarme und richtet diese für Ihre Anwendungsressourcen und Ihren Technologie-Stack ein (z. B. Ihre Microsoft-SQL-Server-Datenbank, Web (IIS)- und Anwendungsserver, Betriebssystem, Load Balancer und Warteschlangen). Es überwacht kontinuierlich die Metriken und Protokolle, um Anomalien und Fehler zu erkennen und zu korrelieren. Wenn Fehler und Anomalien erkannt werden, generiert Application Insights Ereignisse, mit denen Sie Benachrichtigungen einrichten oder Aktionen ausführen können. Um die Fehlersuche zu erleichtern, erstellt es automatisierte Dashboards für die erkannten Probleme, die korrelierte Metrikanomalien und Protokollfehler sowie zusätzliche Erkenntnisse enthalten, die Sie auf die mögliche Ursache hinweisen. Die automatisierten Dashboards helfen Ihnen, schnell

Abhilfemaßnahmen zu ergreifen, um Ihre Anwendungen funktionstüchtig zu halten und Auswirkungen auf die Endbenutzer Ihrer Anwendung zu vermeiden.

Informationen über erkannte Probleme:

- Eine kurze Zusammenfassung des Problems.
- Die Startzeit und das Datum des Problems.
- Der Schweregrad des Problems: High/Medium/Low
- Der Status des erkannten Problems: in Bearbeitung/gelöst.
- Einblicke: Automatisch generierte Erkenntnisse über das erkannte Problem und die mögliche Hauptursache.
- Feedback zu Erkenntnissen: Feedback, das Sie zur Nützlichkeit der mit CloudWatch Application Insights für .NET und SQL Server generierten Erkenntnisse gegeben haben
- Verwandte Beobachtungen: Eine detaillierte Übersicht über die Metrikanomalien und Fehlerausschnitte relevanter Protokolle im Zusammenhang mit dem Problem über verschiedene Anwendungskomponenten hinweg.

Feedback

Sie können Feedback zu den automatisch generierten Erkenntnissen über erkannte Probleme geben, indem Sie sie als nützlich oder nicht nützlich einstufen. Ihr Feedback zu den Erkenntnissen sowie Ihre Anwendungsdiagnose (Metrikanomalien und Protokollausnahmen) werden genutzt, um die zukünftige Erkennung ähnlicher Probleme zu verbessern.

Weitere Informationen finden Sie in der CloudWatchApplication Insights-Dokumentation im CloudWatch Amazon-Benutzerhandbuch.

Verfolgen Sie Ihre Nutzung des kostenlosen Kontingents für Amazon EC2

Wenn Sie Ihre erstellen AWS-Konto, können Sie mit dem kostenlosen Kontingent EC2 AWS kostenlos mit Amazon beginnen. Ihre Vorteile im Rahmen des kostenlosen Kontingents hängen davon ab, ob Sie Ihr Konto vor dem 15. Juli 2025 oder am oder nach dem 15. Juli 2025 erstellt haben. Weitere Informationen finden Sie im AWS Billing Benutzerhandbuch unter Entdecken Sie AWS Services mit AWS kostenlosem Kontingent.

Vorteile des kostenlosen Kontingents vor und nach dem 15. Juli 2025

In der folgenden Tabelle werden die Vorteile des kostenlosen Kontingents anhand des Erstellungsdatums Ihres AWS-Konto verglichen:

Vorteil des kostenlosen Kontingents	Konto vor dem 15. Juli 2025 erstellt	Konto am oder nach dem 15. Juli 2025 erstellt
Instance-Typen, die für das kostenlose Kontingent berechtigt sind	`t2.micro`, `t3.micro`	`t3.micro`, `t3.small`, `t4g.micro` , `t4g.small` , `c7i-flex.large` , `m7i-flex.large`
Amazon-EBS-Volume-Typen, die für das kostenlose Kontingent berechtigt sind	`standard`, `st1`, `sc1`, `gp2`, und `gp3`	`standard`, `st1`, `sc1`, `gp2`, und `gp3`
AMIs als „Kostenloses Kontingent berechtigt“ gekennzeichnet	Suchen Sie nach, ob das kostenlose Kontingent als berechtigt AMIs markiert ist.	Suchen Sie nach, ob das kostenlose Kontingent als berechtigt AMIs markiert ist.
Nutzungslimit	Beschränkt auf Nutzungslimits. Danach werden Ihnen pay-as-you-go Tarife in Rechnung gestellt.	Sie erhalten ein Anmeldeguthaben in Höhe von 100 USD und können bis zu 100 USD an zusätzlichem Guthaben verdienen.
Dauer des kostenlosen Kontingents	Ihr kostenloses Kontingent gilt für 12 Monate ab dem Datum, an dem Sie Ihr Konto erstellen. Wenn Sie während dieser Zeit Ihre Nutzungslimits im Rahmen des kostenlosen Kontingents überschreiten, werden Ihnen Tarife in Rechnung gestellt pay-as-you-go.	Ihr kostenloses Kontingent gilt für 6 Monate ab dem Datum, an dem Sie Ihr Konto erstellt haben, oder wenn Ihr Guthaben aufgebraucht ist, je nachdem, was zuerst eintritt. Sie können Ihr Limit für das kostenlose Kontingent nicht überschreiten.

So listen Sie die Instance-Typen auf, die für das kostenlose Kontingent berechtigt sind

Verwenden Sie den Befehl describe-instance-types mit dem Filter `free-tier-eligible`.

```
aws ec2 describe-instance-types \
    --filters Name=free-tier-eligible,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

Um diejenigen aufzulisten AMIs , für die das kostenlose Kontingent in Frage kommt

Verwenden Sie den Befehl describe-images mit dem `free-tier-eligible`-Filter.

```
aws ec2 describe-images \
    --filters Name=free-tier-eligible,Values=true \
    --query "Images[*].[ImageId]" \
    --output text | sort
```

Die Nutzung des kostenlosen Kontingents für Konten nachverfolgen, die vor dem 15. Juli 2025 erstellt wurden

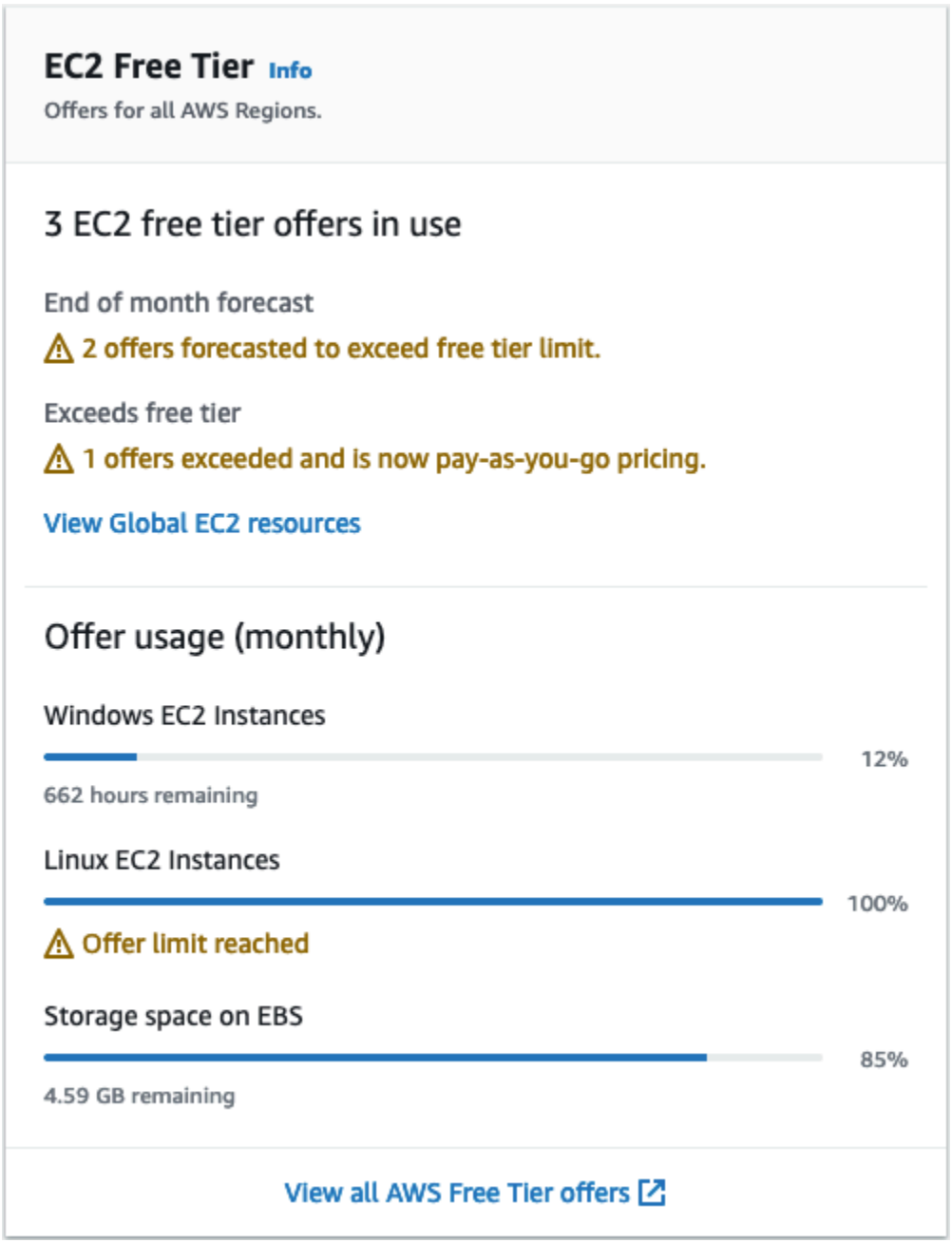
> **Note**
>
> Dieser Abschnitt gilt nur für Nutzer des kostenlosen Kontingents, die AWS-Konten vor dem 15. Juli 2025 ein Konto erstellt haben. Wenn Sie Ihr Konto am oder nach dem 15. Juli 2025 erstellt haben, finden Sie im AWS Billing Benutzerhandbuch Informationen zur Nachverfolgung Ihrer Nutzung des AWS kostenlosen Kontingents.

Wenn Sie Ihr Konto vor dem 15. Juli 2025 erstellt haben, können EC2 Sie Amazon kostenlos nutzen, wenn Sie seit weniger als 12 Monaten AWS Kunde sind und die Kostenloses AWS-Kontingent Nutzungslimits einhalten. Es ist wichtig, dass Sie Ihre Nutzung des kostenlosen Kontingents nachverfolgen, um Überraschungen bei der Rechnungsstellung zu vermeiden. Wenn Sie die Limits des kostenlosen Kontingents überschreiten, fallen Standardgebühren an. pay-as-go Weitere Informationen finden Sie unter Kostenloses AWS-Kontingent.

> **Note**
>
> Wenn Sie seit mehr als 12 Monaten AWS Kunde sind, haben Sie keinen Anspruch mehr auf das kostenlose Kontingent und das Feld „EC2Kostenloses Kontingent“, das im folgenden Verfahren beschrieben wird, wird nicht angezeigt.

So können Sie Ihre Nutzung des kostenlosen Kontingents nachverfolgen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich EC2 Dashboard (Dashboard).
3. Suchen Sie das Feld „EC2 Kostenloses Kontingent“ (oben rechts).



4. Prüfen Sie im Feld EC2 Kostenloses Kontingent wie folgt Ihre Nutzung des kostenlosen Kontingents:

   - Beachten EC2 Sie unter „In Anspruch genommenes kostenloses Kontingent“ die folgenden Warnhinweise:
     - Prognose zum Monatsende – Diese Warnung gibt an, dass in diesem Monat Gebühren anfallen werden, wenn Sie Ihr derzeitiges Nutzungsmuster beibehalten.
     - Überschreitet das kostenlose Kontingent – Diese Warnung gibt an, dass Sie Ihr Limit für das kostenlose Kontingent überschritten haben und bereits Gebühren anfallen.

- Notieren Sie sich unter Nutzung des Angebots (monatlich) Ihre Nutzung von Linux-Instances, Windows-Instances und EBS-Speicher. Der Prozentsatz gibt an, wie viele der Limits Ihres kostenlosen Kontingents Sie in diesem Monat genutzt haben. Wenn Sie bei 100 % angelangt sind, fallen Gebühren für die weitere Nutzung an.

> **Note**
>
> Diese Informationen werden erst angezeigt, nachdem Sie eine Instance erstellt haben. Die Nutzungsinformationen werden jedoch nicht in Echtzeit aktualisiert, sondern dreimal täglich.

5. Um weitere Gebühren zu vermeiden, löschen Sie alle Ressourcen, für die entweder jetzt Gebühren anfallen oder für die Gebühren anfallen, wenn Sie Ihr Nutzungslimit für das kostenlose Kontingent überschreiten.

   - Eine Anleitung zum Löschen Ihrer Instance finden Sie unter EC2 Amazon-Instances beenden.
   - Um zu überprüfen, ob Sie über Ressourcen in anderen Regionen verfügen, für die möglicherweise Gebühren anfallen, wählen Sie im Feld EC2 Kostenloses Kontingent die Option Globale EC2 Ressourcen anzeigen aus, um die EC2 globale Ansicht zu öffnen. Weitere Informationen finden Sie unter Mit AWS Global View können Sie Ressourcen regionsübergreifend anzeigen.

6. Wählen Sie unten im Feld „EC2 Kostenloses Kontingent AWS-Services “ die Kostenloses AWS-Kontingent Option „Alle Angebote anzeigen“ aus, um Ihren Ressourcenverbrauch für alle Kostenloses AWS-Kontingent einzusehen. Weitere Informationen finden Sie unter Testen von Services mithilfe von Kostenloses AWS-Kontingent im Benutzerhandbuch zur AWS - Fakturierung.

Die Codes für Amazon EC2 in Fakturierungs- und Nutzungsberichten verstehen

Wenn Sie Amazon EC2 verwenden, nehmen wir entsprechende Codes in Ihre AWS-Fakturierungs- und Nutzungsberichte auf. Die Überprüfung dieser Codes hilft Ihnen, Ihre Kosten und Nutzungsmuster für Amazon EC2 zu verstehen. Die Nachverfolgung und Verwaltung Ihrer Ausgaben ist für die Optimierung Ihrer Kosten unerlässlich.

Die folgenden Tabellen beschreiben die Codes für Amazon EC2, die in Ihren Fakturierungs- und Nutzungsberichten vorkommen. Eine Liste der Regionscodes in den Fakturierungs- und Nutzungsberichten finden Sie unter AWSRegions-Fakturierungscodes.

Fakturierungscodes für:

- Instances
- Bare Metal-Instances
- Dedicated Hosts
- Dedicated Instances
- EBS-Optimierung
- Capacity Reservations

Zugehörige Ressourcen

- the section called “Abrechnungs- und Kaufoptionen”
- the section called “Verstehen der AMI-Fakturierung”
- Amazon EC2 – Preise

Instances

Code	Beschreibung	Einheiten
region-BoxUsage :*instance-type*	Die Laufzeit für On-Demand-Instances.	Stunden
region-HostBoxUsage :*instance-type*	Die Laufzeit für Instances auf Dedicated Hosts.	Stunden
region-SpotUsage :*instance-type*	Die Laufzeit für Spot Instances.	Stunden

Bare Metal-Instances

Code	Beschreibung	Einheiten
region-BoxUsage :*instance-family* .metal	Die Laufzeit für Bare-Metal-On-Demand-Instances.	Stunden
region-HostBoxUsage :*instance-family* .metal	Die Laufzeit für Bare-Metal-Instances auf Dedicated Hosts.	Stunden
region-SpotUsage :*instance-family* .metal	Die Laufzeit für Bare-Metal-Spot-Instances.	Stunden

Dedicated Hosts

Code	Beschreibung	Einheiten
region-HostUsage :*Host-Typ*	Der Zeitpunkt, zu dem Dedicated Hosts bereitgestellt werden.	Stunden
region-ReservedHostUsage :*Host-Typ*	Der Zeitpunkt, zu dem Dedicated-Host-Reservierungen gelten.	Stunden

Dedicated Instances

Code	Beschreibung	Einheiten
region-DedicatedUsage :*instance-type*	Die Laufzeit für Dedicated Instances.	Stunden + Gebühr pro Region

EBS-Optimierung

Code	Beschreibung	Einheiten
region-EBSOptimized :*instance-type*	Der Zeitpunkt, zu dem die EBS-Optimierung aktiviert ist.	Stunden

Capacity Reservations

Code	Beschreibung	Einheiten
region-Reservation :*instance-type*	Die reservierte Instance-Zeit für Kapazitätsreservierungen.	Stunden
region-UnusedBox :*instance-type*	Die ungenützte reservierte Instance-Zeit für Kapazitätsreservierungen.	Stunden
region-DedicatedRes :*instance-type*	Die reservierte Instance-Zeit für dedizierte Kapazitätsreservierungen.	Stunden
region-UnusedDed :*instance-type*	Die ungenutzte reservierte Instance-Zeit für dedizierte Kapazitätsreservierungen.	Stunden

Eine Bestandsaufnahme Ihrer EC2-Instances erstellen

Amazon EC2 stellt skalierbare On-Demand-Rechenkapazität bereit. Eine EC2-Instance ist ein virtueller Server, der im AWS-Netzwerk ausgeführt wird.

In der folgenden Tabelle werden die wichtigsten Merkmale einer EC2-Instance beschrieben. Ein Systemadministrator kann anhand der in diesem Handbuch enthaltenen Anleitungen Informationen zu diesen Merkmalen abrufen und anhand dieser Informationen funktionsgleiche

Server konfigurieren, die On-Premises oder im Netzwerk eines anderen Cloud-Anbieters ausgeführt werden.

Merkmal	Beschreibung
Geografischer Standort	Amazon EC2 wird in allen AWS-Regionen weltweit gehostet. Sie wählen Standorte für Ihre Instances aus, die sich in der Nähe Ihrer Kunden befinden. Sie können Instances an mehreren Standorten starten.
Hardwarespezifikationen	Amazon EC2 bietet eine große Auswahl an Instance-Typen, die für verschiedene Anwendungsfälle optimiert sind. Die Instance-Typen, die Sie für Ihre Instances auswählen, bestimmen deren Rechen-, Arbeitsspeicher-, Netzwerk- und Speicherressourcen.
Bilder	Ein Amazon Machine Image (AMI) enthält die Software, die Sie beim Start auf Ihrer Instance installieren müssen. Dazu gehören das Betriebssystem, Softwarepakete und benutzerdefinierte Konfigurationen.
IP-Adressen und DNS-Hostnamen	Instances erhalten private IP-Adressen und einen privaten DNS-Hostnamen. Wenn Sie eine öffentliche IP-Adresse für eine Instance konfigurieren, erhält sie auch einen öffentlichen DNS-Hostnamen.
Sicherheitsgruppenregeln	Die Ihren Instances zugeordneten Sicherhei tsgruppenregeln legen fest, welcher eingehend e und ausgehende Datenverkehr zulässig ist.
Benutzerdaten	Benutzerdaten werden den Instances beim Start zur Verfügung gestellt. Diese Daten bestehen aus Shell-Skripten (Linux) oder PowerShell-Skripten (Windows).

Geografischer Standort

Amazon EC2 ist in allen AWS-Regionen weltweit verfügbar. Jede Region ist ein separater geografischer Bereich. Sie können die Netzwerklatenz verringern, wenn Sie Regionen für Ihre Server auswählen, die sich in der Nähe der Mehrheit Ihrer Benutzer befinden.

Sie können Amazon EC2 Global View verwenden, um Ihre Amazon-EC2-Instances in allen Regionen aufzulisten. Mit der AWS-Managementkonsole und der API müssen Sie die Instances für jede Region einzeln auflisten.

Warum das wichtig ist

Nachdem Sie ermittelt haben, wo sich Ihre Instances befinden, können Sie je nach Ihren Anforderungen entscheiden, ob Sie funktionell gleichwertige Server an denselben Standorten oder an verschiedenen Standorten bereitstellen möchten.

So erhalten Sie eine Zusammenfassung Ihrer EC2-Instances in allen Regionen

1. Öffnen Sie die Amazon EC2 Global View-Konsole unter https://console.aws.amazon.com/ec2globalview/home.
2. Überprüfen Sie auf der Registerkarte Region Explorer unter Zusammenfassung die Ressourcenanzahl für Instances, die die Anzahl der Instances und die Anzahl der Regionen umfasst. Wählen Sie den unterstrichenen Text, um zu sehen, wie sich die Anzahl der Instances auf die Regionen verteilt.
3. Wählen Sie auf der Registerkarte Globale Suche den Client-Filter Ressourcentyp = Instance aus. Sie können die Ergebnisse weiter filtern, indem Sie eine Region oder ein Tag angeben.

So rufen Sie die Anzahl der EC2-Instances in einer Region mit der AWS CLI ab

Verwenden Sie den Befehl describe-instances, um die Instances in der aktuellen Region zu zählen. Sie müssen diesen Befehl in jeder Region ausführen, in der Sie Instances haben.

```
aws ec2 describe-instances \
    --region us-east-2 \
    --query "length(Reservations[*].Instances[])"
```

Es folgt eine Beispielausgabe.

```
27
```

Verwenden Sie stattdessen den folgenden `--query`-Parameter, um eine Liste der Instance-IDs anstelle der Anzahl der Instances zu erhalten.

```
--query "Reservations[*].Instances[].InstanceId"
```

Hardwarespezifikationen

Der Instance-Typ, den Sie für eine EC2-Instance angeben, bestimmt die Rechen-, Arbeitsspeicher-, Speicher- und Netzwerkressourcen, die ihr zur Verfügung stehen. Jeder Instance-Typ bietet ein anderes Verhältnis in Bezug auf Datenverarbeitung, Arbeitsspeicher, Speicher und Netzwerkfunktionen. Weitere Informationen finden Sie unter Amazon-EC2-Instance-Typen.

Warum diese wichtig sind

Nachdem Sie die Hardwarespezifikationen für Ihre Instances festgelegt haben, können Sie festlegen, welche Mindestspezifikationen für funktionsgleiche Server erforderlich sind.

So rufen Sie eine Zusammenfassung der von Ihren Instances verwendeten Instance-Typen ab

Verwenden Sie den folgenden describe-instances-Befehl. Der sed-Befehl entfernt Zeilen mit Klammern und Leerzeilen. Sie müssen diesen Befehl in jeder Region ausführen, in der Sie Instances haben.

```
aws ec2 describe-instances \
    --query "Reservations[*].Instances[].InstanceType" | sed 's/[][]//g;/^$/d' | sort |
 uniq -c | sort -nr
```

Es folgt eine Beispielausgabe.

```
  20    "c6i.4xlarge",
   5    "t2.micro",
   2    "g6e.2xlarge",
```

So rufen Sie Informationen zu bestimmten Instance-Typen ab

Verwenden Sie den Befehl describe-instance-types, um die Instance-Typen zu beschreiben. Der `--query`-Parameter umfasst nur die angegebenen Felder in der Ausgabe. Dies sind die grundlegenden Eigenschaften. Sie können alle zusätzlichen Felder angeben, die Sie benötigen, oder Sie können die Spezifikationen für Amazon-EC2-Instance-Typen im Leitfaden für Amazon-EC2-Instance-Typen nachschlagen.

```
aws ec2 describe-instance-types \
    --instance-types c6i.4xlarge t2.micro g6e.2xlarge \
    --query "InstanceTypes[*].
[InstanceType,VCpuInfo.DefaultVCpus,MemoryInfo.SizeInMiB,NetworkInfo.NetworkPerformance]"
 \
    --output table
```

Es folgt eine Beispielausgabe. Die Spalten lauten Instance-Typ, vCPUs, Arbeitsspeicher (GiB) und Netzwerkbandbreite (Gbit/s).

```
-----------------------------------------------------
|               DescribeInstanceTypes               |
+--------------+-----+--------+----------------------+
|  t2.micro    |  1  |  1024  |  Low to Moderate     |
|  c6i.4xlarge |  16 |  32768 |  Up to 12.5 Gigabit  |
|  g6e.2xlarge |  8  |  65536 |  Up to 20 Gigabit    |
+--------------+-----+--------+----------------------+
```

Bilder

Ein Amazon Machine Image (AMI) stellt die Software bereit, die beim Start auf Ihrer Instance installiert wird, z. B. das Betriebssystem, Services, Entwicklungstools und Anwendungen. Sie können ein AMI in andere Formate exportieren, um es mit anderen Servern zu verwenden.

Warum diese wichtig sind

Nachdem Sie die AMIs für Ihre Instances festgelegt haben, können Sie die Images planen, die für funktionsgleiche Server erforderlich sind. Möglicherweise können Sie Ihre AMIs in ein Format exportieren, das Sie an anderer Stelle verwenden können. Alternativ müssen Sie möglicherweise eine Verbindung zu einer Instance herstellen, die Sie von jedem AMI aus gestartet haben, überprüfen, was installiert und wie sie konfiguriert ist, und sicherstellen, dass Sie über eine Kopie von allem verfügen, was Sie benötigen.

So rufen Sie die AMIs für Ihre Instances ab

Verwenden Sie den folgenden describe-instances-Befehl. Der sed-Befehl entfernt Zeilen mit Klammern und Leerzeilen. Sie müssen diesen Befehl in jeder Region ausführen, in der Sie Instances haben.

```
aws ec2 describe-instances \
```

```
    --query "Reservations[*].Instances[].ImageId" | sed 's/[][]//g;/^$/d' | sort | uniq
 -c | sort -nr
```

Es folgt eine Beispielausgabe.

```
20     "ami-0a70b9d193ae8a79",
 5     "ami-07d9cf938edb0739b",
 2     "ami-09245d5773578a1d6",
```

So rufen Sie Informationen zu bestimmten AMIs auf

Verwenden Sie den Befehl describe-images. Der `--query`-Parameter umfasst nur die angegebenen Felder in der Ausgabe. Sie können alle zusätzlichen Felder hinzufügen, die Sie benötigen.

```
aws ec2 describe-images \
    --image-id ami-0a70b9d193ae8a79 ami-07d9cf938edb0739b ami-09245d5773578a1d6 \
    --query "Images[*].
{ID:ImageId,CreateDate:CreationDate,Name:Name,Description:Description}"
```

Es folgt eine Beispielausgabe.

```
[
    {
        "ID": "ami-0a70b9d193ae8a799",
        "CreateDate": "2025-03-01T02:22:41.000Z",
        "Name": "web-server-3.1",
        "Description": "Image for web servers"
    },
    {
        "ID": "ami-07d9cf938edb0739b",
        "CreateDate": "2025-02-01T23:59:03.000Z",
        "Name": "awesome-application-11.5",
        "Description": "Image for Awesome Application"
    },
    {
        "ID": "ami-09245d5773578a1d6",
        "CreateDate": "2025-01-31T02:22:41.000Z",
        "Name": "monitoring-4.2",
        "Description": "Monitoring software"
    }
]
```

So erstellen Sie eine VM-Datei aus einem AMI

Verwenden Sie den Befehl export-image. Die unterstützten Image-Formate sind VHD (kompatibel mit Citrix Xen und Microsoft Hyper-V), VMDK (kompatibel mit VMware ESX und VMware vSphere) und Rohformat (kompatibel mit KVM- und Xen-Hypervisoren). Informationen zu den Anforderungen und Einschränkungen von VM Import/Export finden Sie unter Anforderungen für VM Import/Export.

IP-Adressen und DNS-Hostnamen

Ihre Benutzer stellen über das Internet mithilfe ihrer öffentlichen DNS-Hostnamen eine Verbindung zu Ihren EC2-Instances her. Der öffentliche DNS-Hostname einer EC2-Instance wird in ihre öffentliche IP-Adresse aufgelöst. EC2-Instances können über ihre private IP-Adressen miteinander kommunizieren.

Warum diese wichtig sind

IP-Adressen ermöglichen es Geräten, über ein lokales Netzwerk oder das Internet miteinander zu kommunizieren. Indem Sie sich die IP-Adressen und DNS-Namen Ihrer Instances notieren, können Sie sicherstellen, dass funktionell gleichwertige Server mit denselben Clients oder Geräten wie Ihre Instances kommunizieren können. Sie können beispielsweise Ihre Load Balancer-Konfiguration oder die DNS-Datensätze, die Sie für Ihren DNS-Anbieter erstellt haben, aktualisieren.

So rufen Sie die IP-Adressen und DNS-Hostnamen für Ihre Instances ab

Verwenden Sie den folgenden describe-instances-Befehl. Sie müssen diesen Befehl in jeder Region ausführen, in der Sie Instances haben. Der `--query`-Parameter umfasst nur die angegebenen Felder in der Ausgabe. Sie können alle zusätzlichen Felder hinzufügen, die Sie benötigen.

```
aws ec2 describe-instances \
    --query "Reservations[*].Instances[].[InstanceId,PrivateIpAddress,PublicDnsName]" \
    --output table
```

Es folgt eine Beispielausgabe. Die Spalten lauten Instance-ID, private IPv4-Adresse und öffentlicher IPv4-DNS-Name.

```
----------------------------------------------------------------------------------
|                                DescribeInstances                               |
 |
+---------------------+------------+-------------------------------------------------
+
```

```
| i-0bac57d7472c89bac | 10.0.2.139 | ec2-192-0-2-142.us-east-2.compute.amazonaws.com
 |
| i-0fa8b7678975a3fff | 10.0.14.85 | ec2-198-51-100-56.us-east-2.compute.amazonaws.com
 |
  ...
  ...
| i-08fd74f3f1595fdbd | 10.0.1.241 | ec2-203.0.113.13.us-east-2.compute.amazonaws.com
 |
+---------------------+------------+-------------------------------------------------
+
```

Sicherheitsgruppenregeln

Eine Sicherheitsgruppe fungiert als virtuelle Firewall. Nachdem Sie eine Sicherheitsgruppe einer EC2-Instance zugeordnet haben, lassen ihre Regeln ein- und ausgehenden Datenverkehr für die EC2-Instance über bestimmte Ports und Protokolle zu.

Warum diese wichtig sind

Nachdem Sie den eingehenden Datenverkehr festgelegt haben, der Ihren Server erreichen darf, und den ausgehenden Datenverkehr, der Ihren Server verlassen darf, können Sie die Firewall-Regeln planen, die für funktionsgleiche Server erforderlich sind.

So rufen Sie die Sicherheitsgruppen für Ihre Instances ab

Verwenden Sie den folgenden describe-instances-Befehl. Der sed-Befehl entfernt Zeilen mit Klammern und Leerzeilen. Sie müssen diesen Befehl in jeder Region ausführen, in der Sie Instances haben.

```
aws ec2 describe-instances \
    --query "Reservations[*].Instances[].SecurityGroups[].GroupId" | sed 's/[][]//g;/^
$/d' | sort | uniq -c | sort -nr
```

Es folgt eine Beispielausgabe.

```
27     "sg-01dd3383691d02f42",
10     "sg-08c77cc910c0b3b2c",
 2     "sg-00f4e409629f1a42d",
```

So rufen Sie die Regeln einer Sicherheitsgruppe für den eingehenden Datenverkehr ab

Verwenden Sie den Befehl describe-security-group-rules, um die Regeln für die angegebene Sicherheitsgruppe anzuzeigen, wobei `IsEgress` den Wert `false` hat.

```
aws ec2 describe-security-group-rules \
    --filters Name=group-id,Values=sg-01dd3383691d02f42 \
    --query 'SecurityGroupRules[?IsEgress==`false`]'
```

Es folgt eine Beispielausgabe. Die erste Regel ist die Standardregel für eingehenden Datenverkehr, die eingehenden Datenverkehr von allen Ressourcen zulässt, die dieser Sicherheitsgruppe zugewiesen sind. Die andere Regel erlaubt SSH-Verkehr von den IP-Adressen in der angegebenen Präfixliste. Verwenden Sie den Befehl describe-prefix-lists, um die CIDR-Blöcke in einer Präfixliste zu beschreiben.

```
[
    {
        "SecurityGroupRuleId": "sgr-06c8b42574a91db1b",
        "GroupId": "sg-01dd3383691d02f42",
        "GroupOwnerId": "123456789012",
        "IsEgress": false,
        "IpProtocol": "-1",
        "FromPort": -1,
        "ToPort": -1,
        "ReferencedGroupInfo": {
            "GroupId": "sg-01dd3383691d02f42",
            "UserId": "123456789012"
        },
        "Tags": [],
        "SecurityGroupRuleArn": "arn:aws:ec2:us-west-2:123456789012:security-group-
rule/sgr-06c8b42574a91db1b"
    },
    {
        "SecurityGroupRuleId": "sgr-0886a5d46afcd1758",
        "GroupId": "sg-01dd3383691d02f42",
        "GroupOwnerId": "123456789012",
        "IsEgress": false,
        "IpProtocol": "tcp",
        "FromPort": 22,
        "ToPort": 22,
        "PrefixListId": "pl-f8a6439125e7bf465",
        "Tags": [],
        "SecurityGroupRuleArn": "arn:aws:ec2:us-east-2:123456789012:security-group-
rule/sgr-0886a5d46afcd1758"
```

```
    }
]
```

So rufen Sie die Regeln einer Sicherheitsgruppe für den ausgehenden Datenverkehr ab

Verwenden Sie den Befehl describe-security-group-rules, um die Regeln für die angegebene Sicherheitsgruppe anzuzeigen, wobei `IsEgress` den Wert `true` hat.

```
aws ec2 describe-security-group-rules \
    --filters Name=group-id,Values=sg-01dd3383691d02f42 \
    --query 'SecurityGroupRules[?IsEgress==`true`]'
```

Es folgt eine Beispielausgabe. Darin ist nur die Standardregel für ausgehenden Datenverkehr enthalten, die den gesamten ausgehenden IPv4-Datenverkehr erlaubt.

```
[
    {
        "SecurityGroupRuleId": "sgr-048f09a719247dce7",
        "GroupId": "sg-01dd3383691d02f42",
        "GroupOwnerId": "123456789012",
        "IsEgress": true,
        "IpProtocol": "-1",
        "FromPort": -1,
        "ToPort": -1,
        "CidrIpv4": "0.0.0.0/0",
        "Tags": [],
        "SecurityGroupRuleArn": "arn:aws:ec2:us-east-2:123456789012:security-group-
rule/sgr-048f09a719247dce7"
    }
]
```

Benutzerdaten

Wenn Sie eine EC2-Instance starten, können Sie mithilfe von Benutzerdaten ein Shell-Skript an die Instance übergeben. Beachten Sie, dass Benutzerdaten base64-codiert sind. Sie müssen also die Benutzerdaten dekodieren, um das Skript lesen zu können.

Warum das wichtig ist

Wenn Sie beim Start im Rahmen der Einrichtung Ihrer Instances Befehle ausführen, müssen Sie möglicherweise dieselben Aufgaben ausführen, wenn Sie funktionsgleiche Server einrichten.

So zeigen Sie die dekodierten Benutzerdaten für eine Instance an

Verwenden Sie den Befehl describe-instance-attribute. Der Befehl base64 dekodiert die Benutzerdaten.

```
aws ec2 describe-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --attribute userData \
    --output text \
    --query "UserData.Value" | base64 --decode
```

Es folgt eine Beispielausgabe.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Zugehörige Ressourcen

Im Folgenden sind weitere Merkmale von EC2-Instances aufgeführt:

- Schlüsselpaare
- Speicher
- Tags

Sie können überprüfen, ob Sie Folgendes verwenden, um EC2-Instances zu starten oder den Datenverkehr zwischen Ihren EC2-Instances zu verteilen:

- Auto-Scaling-Gruppen
- EC2-Flotte
- Elastic Load Balancing

Probleme mit EC2 Amazon-Instances beheben

Die folgenden Verfahren und Tipps können Ihnen bei der Behebung von Problemen mit Ihren EC2 Amazon-Instances helfen.

Problembereiche

- Fehlerbehebung bei Amazon-EC2-Instances
- Beheben Sie Probleme beim Anhalten von Amazon-EC2-Instances
- Probleme mit der Kündigung von EC2 Amazon-Instances beheben
- Problembehandlung bei unerreichbaren Amazon-EC2-Instances
- Fehlersuche bei Verbindungsproblemen mit Ihrer Amazon-EC2-Linux-Instance
- Problembehandlung bei Amazon EC2 Linux-Instances mit fehlgeschlagenen Statusprüfungen
- Fehlerbehebung bei einer Amazon EC2 Linux-Instance, die von einem falschen Volume gestartet wurde
- Verbindungsprobleme mit Ihrer Amazon-EC2-Windows-Instance beheben
- Problembehebung bei Startproblemen von Amazon-EC2-Windows-Instance
- Probleme bei Amazon-EC2-Windows-Instances beheben
- Zurücksetzen des Windows-Administratorpassworts für eine Amazon-EC2-Windows-Instance
- Behebung von Sysprep-Problemen mit Amazon Windows-Instances EC2
- Fehlerbehebung einer beeinträchtigten Amazon-EC2-Linux-Instance mithilfe von EC2Rescue
- Problembehebung einer beeinträchtigten Amazon EC2 Windows-Instance mithilfe von EC2 Rescue
- EC2 Serielle Konsole für Instanzen
- Senden Sie einen Diagnose-Interrupt, um eine nicht erreichbare Amazon-Instance zu debuggen EC2

Fehlerbehebung bei Amazon-EC2-Instances

Mithilfe der folgenden Tipps können Sie Probleme beheben, die beim Starten einer Amazon-EC2-Instance auftreten können.

Startprobleme

- Ungültiger Gerätename

- Instance-Limit überschritten
- Ungenügend Kapazität der Instance
- Die angefragte Konfiguration wird derzeit nicht unterstützt. Bitte überprüfen Sie die Dokumentation auf unterstützte Konfigurationen.
- Die Instance wird sofort beendet
- Unzureichende Berechtigungen
- Hohe CPU-Auslastung kurz nach dem Windows-Start (Nur Windows-Instances)

Ungültiger Gerätename

Beschreibung

Sie erhalten den `Invalid device name` *`device_name`*-Fehler, wenn Sie versuchen, eine neue Instance zu starten.

Ursache

Wenn Sie diesen Fehler erhalten, wenn Sie versuchen, eine Instance zu starten, hat der in der Anfrage für ein oder mehrere Volumes angegebene Gerätename einen ungültigen Gerätenamen. Mögliche Gründe hierfür sind:

- Der Gerätename wird möglicherweise vom ausgewählten AMI verwendet.
- Der Gerätename ist möglicherweise für Root-Volumes reserviert.
- Der Gerätename wird in der Anforderung möglicherweise für ein anderes Volume verwendet.
- Der Gerätename ist möglicherweise für das Betriebssystem nicht gültig.

Lösung

So beheben Sie das Problem:

- Stellen Sie sicher, dass der Gerätename nicht in dem ausgewählten AMI verwendet wird. Führen Sie den folgenden Befehl aus, um die Gerätename anzuzeigen, die vom AMI verwendet werden.

```
aws ec2 describe-images --image-id ami-0abcdef1234567890 --query
 'Images[*].BlockDeviceMappings[].DeviceName'
```

- Stellen Sie sicher, dass Sie keinen Gerätenamen verwenden, der für Root-Volumes reserviert ist. Weitere Informationen finden Sie unter Verfügbare Gerätenamen.
- Stellen Sie sicher, dass jedes in Ihrer Anfrage angegebene Volume einen eindeutigen Gerätenamen hat.
- Stellen Sie sicher, dass die von Ihnen angegebenen Gerätenamen das richtige Format haben. Weitere Informationen finden Sie unter Verfügbare Gerätenamen.

Instance-Limit überschritten

Beschreibung

Die Fehlermeldung `InstanceLimitExceeded` wird angezeigt, wenn Sie versuchen, eine neue Instance zu starten oder eine angehaltene Instance erneut zu starten.

Ursache

Wenn beim Versuch, eine neue Instance zu starten oder eine angehaltene Instance erneut zu starten, die Fehlermeldung `InstanceLimitExceeded` angezeigt wird, haben Sie die maximal zulässige Anzahl von Instances erreicht, die Sie in einer Region starten können. Wenn Sie Ihr AWS-Konto erstellen, legen wir Standardlimits für die Anzahl von Instances fest, die sie abhängig von der jeweiligen Region ausführen können.

Lösung

Sie können eine Erhöhung des Instance-Limits für die jeweilige Region anfordern. Weitere Informationen finden Sie unter EC2 Amazon-Servicekontingente.

Ungenügend Kapazität der Instance

Beschreibung

Die Fehlermeldung `InsufficientInstanceCapacity` wird angezeigt, wenn Sie versuchen, eine neue Instance zu starten oder eine angehaltene Instance erneut zu starten.

Ursache

Wenn bei dem Versuch, eine Instance zu starten oder eine angehaltene Instance erneut zu starten, diese Fehlermeldung angezeigt wird, verfügt AWS aktuell nicht über genügend On-Demand-Kapazität, um Ihre Anforderung zu erfüllen.

Lösung

Versuchen Sie, das Problem wie folgt zu beheben:

- Warten Sie einige Minuten und senden Sie Ihre Anfrage erneut. Die Kapazität kann häufig schwanken.
- Senden Sie eine neue Anfrage mit einer geringeren Anzahl von Instances. Wenn Sie z. B. eine einzelne Anfrage zum Starten von 15 Instances senden möchten, versuchen Sie stattdessen, 3 Anfragen für 5 Instances oder 15 Anfragen für 1 Instance zu erstellen.
- Wenn Sie eine Instance starten, senden Sie eine neue Anfrage ohne Angabe einer Availability Zone.
- Wenn Sie eine Instance starten, senden Sie eine neue Anfrage unter Verwendung eines anderen Instance-Typs (die Größe können Sie später anpassen). Weitere Informationen finden Sie unter Änderungen des EC2 Amazon-Instanztyps.
- Wenn Sie Instances in einer Cluster Placement-Gruppe starten, kann es zu einem Fehler wegen unzureichender Kapazität kommen.

Die angefragte Konfiguration wird derzeit nicht unterstützt. Bitte überprüfen Sie die Dokumentation auf unterstützte Konfigurationen.

Beschreibung

Die Fehlermeldung `Unsupported` wird angezeigt, wenn Sie versuchen, eine neue Instance zu starten, da die Instance-Konfiguration nicht unterstützt wird.

Ursache

Die Fehlermeldung enthält zusätzliche Details. Beispielsweise wird ein Instance-Typ oder eine Instance-Kaufoption in der angegebenen Region oder Availability Zone möglicherweise nicht unterstützt.

Lösung

Versuchen Sie es mit einer anderen Instance-Konfiguration. Informationen zum Suchen nach einem Instance-Typ, der Ihren Anforderungen entspricht, finden Sie unter Suchen eines Amazon EC2-Instance-Typs.

Die Instance wird sofort beendet

Beschreibung

Ihre Instance wechselt vom Status `pending` in den Status `terminated`.

Ursache

Nachfolgend sind einige Gründe genannt, warum eine Instance sofort beendet werden kann:

- Sie haben Ihre EBS-Volumenlimits überschritten. Weitere Informationen finden Sie unter Amazon EBS-Volumenlimits für Amazon-Instances EC2 .
- Ein EBS-Snapshot ist beschädigt.
- Das EBS-Stamm-Volume ist verschlüsselt und Sie sind nicht berechtigt, auf den Verschlüsselung zur Entschlüsselung zuzugreifen.
- Ein Snapshot, der in der Blockgerätezuordnung für das AMI angegeben ist, ist verschlüsselt, und Sie haben keine Berechtigungen für den Zugriff auf den Verschlüsselung für die Entschlüsselung oder Sie haben keinen Zugriff auf den Verschlüsselung für die Verschlüsselung der wiederhergestellten Volumes.
- Dem Amazon-S3-gestützten AMI, das Sie zum Starten der Instance verwendet haben, fehlt eine erforderliche Komponente (eine image.part.xx-Datei).

Um weitere Informationen zu erhalten, fordern Sie mit einer der folgenden Methoden den Beendigungsgrund an.

So verwenden Sie die Amazon EC2-Konsole, um den Grund für die Beendigung zu erfahren

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie die Instance aus.
3. Suchen Sie auf der ersten Registerkarte neben Grund für den Zustandsübergang nach dem Grund.

So verwenden Sie die , um den Grund für die Beendigung zu erfahre AWS CLI

1. Führen Sie den Befehl describe-instances aus und geben Sie die Instance-ID an.

```
aws ec2 describe-instances --instance-id i-1234567890abcdef0
```

2. Sehen Sie sich die von dem Befehl zurückgegebene JSON-Antwort an und notieren Sie die Werte im `StateReason`-Antwortelement.

   Der folgende Codeblock zeigt ein Beispiel für ein `StateReason`-Antwortelement.

```
"StateReason": {
  "Message": "Client.VolumeLimitExceeded: Volume limit exceeded",
  "Code": "Server.InternalError"
},
```

So verwenden Sie die , um den Grund für die Beendigung zu erfahre AWS CloudTrail

Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-Ereignisverlauf im AWS CloudTrail-Benutzerhandbuch.

Lösung

Führen Sie abhängig von dem notierten Beendigungsgrund eine der folgenden Aktionen aus:

- **`Client.VolumeLimitExceeded: Volume limit exceeded`** — Löschen Sie nicht verwendete Volumes. Sie können einen Antrag zum Erhöhen Ihres Volume-Limits absenden.
- **`Client.InternalError: Client error on launch`** – Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen für den Zugriff auf die AWS KMS keys verfügen, die zum Entschlüsseln und Verschlüsseln von Volumes verwendet werden. Weitere Informationen finden Sie unter Verwenden von Schlüsselrichtlinien in AWS KMS im Entwicklerhandbuch für AWS Key Management Service.

Unzureichende Berechtigungen

Beschreibung

Sie erhalten den `"errorMessage": "You are not authorized to perform this operation."`-Fehler, wenn Sie versuchen, eine neue Instance zu starten, und der Startvorgang ist nicht erfolgreich.

Ursache

Falls beim Versuch, eine Instance zu starten, dieser Fehler auftritt, verfügen Sie nicht über die erforderlichen IAM-Berechtigungen, um die Instance zu starten.

Mögliche fehlende Berechtigungen:

- `ec2:RunInstances`
- `iam:PassRole`

Unter Umständen sind auch noch weitere Berechtigungen erforderlich. Die Liste der Berechtigungen, die zum Starten einer Instance erforderlich sind, finden Sie in den exemplarischen IAM-Richtlinien unter Beispiel: Verwenden Sie den EC2 Launch-Instance-Assistenten und Instanzen starten (RunInstances).

Lösung

So beheben Sie das Problem:

- Wenn Sie Anforderungen als IAM-Benutzer erstellen, vergewissern Sie sich, dass Sie über die folgenden Berechtigungen verfügen:
  - `ec2:RunInstances` mit einer Platzhalterressource ("*")
  - `iam:PassRole` mit der Ressource entsprechend dem ARN der Rolle (z. B, `arn:aws:iam::999999999999:role/ExampleRoleName`)
- Sollten Sie nicht über die oben genannten Berechtigungen verfügen, bearbeiten Sie die IAM-Richtlinie, die der IAM-Rolle oder dem IAM-Benutzer zugeordnet ist, um die fehlenden erforderlichen Berechtigungen hinzuzufügen.

Falls Ihr Problem dadurch nicht behoben wird und Sie weiterhin einen Fehler beim Starten erhalten, können Sie die im Fehler enthaltene Autorisierungsfehlermeldung decodieren. Die decodierte Meldung enthält die Berechtigungen, die in der IAM-Richtlinie fehlen. Weitere Informationen finden Sie unter Wie kann ich eine Meldung über einen Autorisierungsfehler entschlüsseln, nachdem ich beim Start einer EC2-Instance den Fehler „UnauthorizedOperation“ erhalten habe?

Hohe CPU-Auslastung kurz nach dem Windows-Start (Nur Windows-Instances)

> **Note**
>
> Dieser Tipp zur Fehlerbehebung gilt nur für Windows-Instances.

Wenn Sie für Windows Update die Option Nach Updates suchen, aber Zeitpunkt zum Herunterladen und Installieren manuell festlegen (Standardeinstellung für Instances) auswählen, kann diese Überprüfung auf Updates zwischen 50 % und 99 % der CPU-Ressourcen in der Instance beanspruchen. Wenn diese CPU-Auslastung für Ihre Anwendungen problematisch ist, können Sie die Windows Update-Einstellungen in der Systemsteuerung ändern oder das folgende Script im Amazon EC2-Dialogfeld „View/Change User Data“ verwenden:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v
 AUOptions /t REG_DWORD /d 3 /f net stop wuauserv net start wuauserv
```

Wenn Sie dieses Script ausführen, geben Sie einen Wert für die Option „/d“ an. Der Standardwert ist 3. Die folgenden Werte sind möglich:

1. Nie nach Updates suchen
2. Nach Updates suchen, aber Zeitpunkt zum Herunterladen und Installieren manuell festlegen
3. Updates herunterladen, aber Installation manuell durchführen
4. Updates automatisch installieren

Nachdem Sie die Benutzerdaten für Ihre Instance geändert haben, können Sie die Instance ausführen. Weitere Informationen finden Sie unter Ausführen von Befehlen auf Ihrer Windows-Instance beim Start.

Beheben Sie Probleme beim Anhalten von Amazon-EC2-Instances

Wenn Sie Ihre Amazon-EBS-gestützte Instance angehalten haben und sie im Status `stopping` hängen bleibt, hängt das Problem möglicherweise mit dem zugrunde liegenden Host-Computer vor.

Um dieses Problem zu beheben, führen Sie die folgenden Schritte aus:

1. Erzwungenes Anhalten der Instance

   Verwenden Sie die Amazon-EC2-Konsole oder die AWS CLI, um das Anhalten der Instance zu erzwingen. Die Schritte finden Sie in Erzwingung des Stopps einer Instance.

   Die Instance versucht zunächst, das System ordnungsgemäß herunterzufahren. Dabei werden auch Dateisystem-Caches und Metadaten geleert (obwohl Sie optional das ordnungsgemäße Herunterfahren umgehen können).. Wenn das ordnungsgemäße Herunterfahren nicht

innerhalb des Timeout-Zeitraums abgeschlossen werden kann, wird die Instance gewaltsam heruntergefahren, ohne die Dateisystem-Caches und Metadaten zu leeren.

2. Nach dem erzwungenen Anhalten

   Führen Sie Verfahren zur Überprüfung und Reparatur des Dateisystems durch.

   > **Important**
   >
   > Die Durchführung dieser Verfahren ist von entscheidender Bedeutung, da ein erzwungenes Anhalten das Leeren von Dateisystemcaches und Metadaten verhindert.

3. Wenn das erzwungene Anhalten fehlschlägt

   Wenn die Instance nach 10 Minuten nicht angehalten wurde, gehen Sie wie folgt vor:

   a. Stellen Sie eine Hilfeanfrage an AWS re:Post. Um schneller eine Lösung zu erhalten, geben Sie die Instance-ID dabei an und beschreiben Sie die Schritte, die Sie unternommen haben.
   b. Wenn Sie einen Supportplan haben, können Sie auch einen technischen Support-Fall im Support Center erstellen.
   c. Während Sie auf Unterstützung warten, können Sie bei Bedarf eine Ersatz-Instance erstellen. Die Schritte finden Sie in (Optional) Eine Ersatz-Instance erstellen.

Während sich eine Instance im Status `stopping` oder einem anderen Status außer `running` befindet, entstehen keine Kosten für die Instance-Nutzung. Ihnen wird die Instance-Nutzung nur in Rechnung gestellt, wenn sich eine Instance im `running`-Status befindet.

Inhalt

- Erzwingung des Stopps einer Instance
- (Optional) Eine Ersatz-Instance erstellen

Erzwingung des Stopps einer Instance

Sie können das Anhalten einer Instance erzwingen. Wenn die Instance nach 10 Minuten nicht gestoppt wurde, posten Sie eine Hilfeanforderung im AWS re:Post. Um schneller eine Lösung zu erhalten, geben Sie die Instance-ID dabei an und beschreiben Sie die Schritte, die Sie unternommen haben. Wenn Sie einen Supportplan haben, können Sie auch einen technischen Support-Fall im Support Center erstellen.

> **Note**
>
> Mit der Konsole können Sie nur dann das Anhalten einer Instance erzwingen, wenn sich die Instance im Status `stopping` befindet. Mit der AWS CLI können Sie nur dann das Anhalten einer Instance erzwingen, wenn sich die Instance im Status `pending`, `running` oder `stopping` befindet.

Console

So erzwingen Sie das Anhalten einer Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie die hängen gebliebene Instance aus.
3. Wählen Sie Instance-Status, Anhalten der Instance erzwingen.

   Beachten Sie, dass Force stop instance (Anhalten der Instance erzwingen) nur dann in der Konsole verfügbar ist, wenn sich Ihre Instance im Zustand `stopping` befindet. Wenn Ihre Instance in einem anderen Zustand ist (außer `shutting-down` und `terminated`), können Sie die AWS CLI verwenden, um Ihre Instance zu stoppen.
4. (Optional) Um das ordnungsgemäße Herunterfahren des Betriebssystems während des erzwungenen Anhaltens zu umgehen, aktivieren Sie das Kontrollkästchen Herunterfahren des Betriebssystems überspringen.
5. Wählen Sie Anhalten erzwingen.

AWS CLI

So erzwingen Sie das Anhalten einer Instance

Verwenden den Befehl stop-instances mit der Option `--force`.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --force
```

Fügen Sie die Option `--skip-os-shutdown` hinzu, um das ordnungsgemäße Herunterfahren des Betriebssystems während des erzwungenen Anhaltens zu umgehen.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --force \
    --skip-os-shutdown
```

PowerShell

So erzwingen Sie das Anhalten einer Instance

Verwenden Sie das cmdlet Stop-EC2Instance und setzen Sie `-Enforce` auf `true`.

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Enforce $true
```

Fügen Sie `-SkipOsShutdown $true` hinzu, um das ordnungsgemäße Herunterfahren des Betriebssystems während des erzwungenen Anhaltens zu umgehen.

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Enforce $true `
    -SkipOsShutdown $true
```

(Optional) Eine Ersatz-Instance erstellen

Während Sie auf Hilfe vom AWS re:Post oder vom Support-Center warten, können Sie eine Ersatz-Instance erstellen. Erstellen Sie eine AMI der hängengebliebenen Instance und starten Sie mit dem neuen AMI eine neue Instance.

> **Important**
>
> Sie können eine Ersatz-Instance erstellen, wenn die festgefahrene Instance nur Systemstatusprüfungen erstellt, da Instance-Statusprüfungen dazu führen, dass das AMI eine exakte Kopie des defekten Betriebssystems kopiert. Nachdem Sie die Statusmeldung bestätigt haben, erstellen Sie das AMI und starten Sie eine neue Instance mit dem neuen AMI.

Console

So erstellen Sie eine Ersatz-Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie die hängen gebliebene Instance aus.
3. Wählen Sie Actions (Aktionen), Image and templates (Image und Vorlagen), Create image (Image erstellen).
4. Gehen Sie auf der Seite Create image (Image erstellen) wie folgt vor:

   a. Geben Sie einen Namen und eine Beschreibung für das AMI ein.

   b. Löschen Sie die Reboot-Instance.

   c. Wählen Sie Create Image (Abbild erstellen) aus.

   Weitere Informationen finden Sie unter the section called “Ein AMI aus einer Instance erstellen”.
5. Starten Sie eine neue Instance über das AMI und überprüfen Sie, ob die neue Instance funktioniert.
6. Wählen Sie die hängen gebliebene Instance und anschließend Aktionen aus. Wählen Sie dann die Optionen Instance-Status und Instance beenden aus. Wenn die Instance beim Beenden auch hängen bleibt, erzwingt Amazon EC2 das Beenden automatisch innerhalb weniger Stunden.

Wenn Sie kein AMI auf der Instance wie in den vorherigen Schritten beschrieben erstellen können, richten Sie eine Ersatz-Instance wie folgt ein:

(Alternativ) Eine Ersatz-Instance mithilfe der Konsole erstellen

1. Wählen Sie die Instance und dann Description (Beschreibung), Block devices (Blockgeräte). Wählen Sie jedes Volume aus und notieren Sie sich seine Volume-ID. Machen Sie sich auch eine Notiz, welches Volume das Stamm-Volume ist.
2. Wählen Sie im Navigationsbereich Volumes aus. Wählen Sie jedes einzelne Volume für die Instance aus und klicken Sie dann auf Actions und Create Snapshot.
3. Wählen Sie im Navigationsbereich die Option Snapshots. Wählen Sie den Snapshot aus, den Sie gerade erstellt haben, und klicken Sie dann auf Actions und Create Volume.

4. Starten Sie eine Instance mit demselben Betriebssystem wie die hängen gebliebene Instance. Notieren Sie sich die Volume-ID und den Gerätenamen des Stamm-Volumes.
5. Wählen Sie im Navigationsbereich Instances aus, wählen Sie die Instance, die Sie soeben gestartet haben, aus und klicken Sie auf Instance State (Instance-Status), Stop instance (Instance anhalten).
6. Wählen Sie im Navigationsbereich Volumes und dann das Stamm-Volume der angehaltenen Instance aus. Klicken Sie auf Actions und Detach Volume.
7. Wählen Sie das Stamm-Volume aus, dass Sie von der hängen gebliebenen Instance erstellt haben. Klicken Sie auf Actions (Aktionen) und Attach Volume (Volume anhängen) und hängen Sie es der neuen Instance als Stamm-Volume an (mit dem Gerätenamen, den Sie sich notiert haben). Fügen Sie der Instance ggf. weitere nicht Stamm-Volumes an.
8. Klicken Sie im Navigationsbereich auf Instances und wählen Sie die Ersatz-Instance aus. Wählen Sie Instance state (Instance-Status), Start instance (Instance starten). Überprüfen Sie, ob die Instance ausgeführt wird.
9. Wählen Sie die hängen gebliebene Instance und anschließend Instance-Status und Instance beenden (löschen) aus. Wenn die Instance beim Beenden auch hängen bleibt, erzwingt Amazon EC2 das Beenden automatisch innerhalb weniger Stunden.

AWS CLI

So erstellen Sie eine Ersatz-Instance

1. Erstellen Sie ein AMI aus der hängengebliebenen Instance mit dem Befehl create-image und der Option `--no-reboot`.

```
aws ec2 create-image \
    --instance-id i-1234567890abcdef0 \
    --name "my-replacement-ami" \
    --description "AMI for replacement instance" \
    --no-reboot
```

2. Starten Sie aus dem gerade erstellten AMI eine neue Instance mit dem Befehl run-instances.
3. Überprüfen Sie, ob die neue Instance ausgeführt wird.
4. (Optional) Beenden Sie die hängengebliebene Instance mit dem Befehl terminate-instances.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

PowerShell

So erstellen Sie eine Ersatz-Instance

1. Erstellen Sie aus der hängengebliebenen Instance ein AMI mit dem cmdlet New-EC2Image und setzen Sie `-NoReboot` auf `true`.

```
New-EC2Image `
    -InstanceId i-1234567890abcdef0 `
    -Name "my-replacement-ami" `
    -Description "AMI for replacement instance" `
    -NoReboot $true
```

2. Starten Sie aus dem gerade erstellten AMI eine neue Instance mit dem cmdlet New-EC2Instance.
3. Überprüfen Sie, ob die neue Instance ausgeführt wird.
4. (Optional) Beenden Sie die hängengebliebene Instance mit dem cmdlet Remove-EC2Instance.

```
Remove-EC2Instance -InstanceId i-1234567890abcdef0
```

Probleme mit der Kündigung von EC2 Amazon-Instances beheben

Das Herunterfahren oder Löschen Ihrer Instance wird als Instance-Beendigung bezeichnet. Die folgenden Informationen können Ihnen helfen, Probleme bei der Beendigung Ihrer Instance zu beheben.

Während sich die Instance nicht im Status `running` befindet, wird Ihnen keine zusätzlichen Instance-Nutzung berechnet. Mit anderen Worten, wenn Sie eine Instance beenden, fallen für diese Instance keine Gebühren mehr an, sobald sich ihr Status in `shutting-down` ändert.

Die Instance wird sofort beendet

Mehrere Probleme können dazu führen, dass Ihre Instance beim Start sofort beendet wird. Weitere Informationen finden Sie unter Die Instance wird sofort beendet.

Verzögertes Beenden einer Instance

Wenn Ihre Instance länger als einige Minuten im Status `shutting-down` bleibt, kann dies folgende Ursachen haben:

- Auf der Instance werden Skripts zum Herunterfahren ausgeführt.
- Es besteht ein Problem mit dem zugrunde liegenden Host-Computer.

Nach mehreren Stunden im `shutting-down` Bundesstaat EC2 behandelt Amazon die Instance als festgefahren und beendet sie gewaltsam.

So beheben Sie eine hängengebliebene Instance selbst:

1. Beendigung der Instance erzwingen

   Verwenden Sie die EC2 Amazon-Konsole oder die AWS CLI , um das Beenden der Instance zu erzwingen. Die Schritte finden Sie in Beendigung einer Instance erzwingen.

   Die Instance versucht zunächst, das System ordnungsgemäß herunterzufahren. Dabei werden auch Dateisystem-Caches und Metadaten geleert (obwohl Sie optional das ordnungsgemäße Herunterfahren umgehen können).. Wenn das ordnungsgemäße Herunterfahren nicht innerhalb des Timeout-Zeitraums abgeschlossen werden kann, wird die Instance gewaltsam heruntergefahren, ohne die Dateisystem-Caches und Metadaten zu leeren.
2. Wenn die erzwungene Beendigung fehlschlägt

   Wenn die Instance nach mehreren Stunden nicht beendet wurde und beim Beenden hängen geblieben ist, gehen Sie wie folgt vor:

   a. Stellen Sie eine Hilfeanfrage an AWS re:Post. Um schneller eine Lösung zu erhalten, geben Sie die Instance-ID dabei an und beschreiben Sie die Schritte, die Sie unternommen haben.
   b. Wenn Sie einen Supportplan haben, können Sie auch einen technischen Support-Fall im Support Center erstellen.

Beendigung einer Instance erzwingen

Wenn Ihre Instance anscheinend beim Beenden hängen geblieben ist, können Sie die Beendigung der Instance erzwingen. Wenn die Instance nach mehreren Stunden nicht beendet wurde, posten Sie eine Hilfeanforderung auf AWS re:Post. Um schneller eine Lösung zu erhalten, geben Sie die

Instance-ID dabei an und beschreiben Sie die Schritte, die Sie unternommen haben. Wenn Sie einen Supportplan haben, können Sie auch einen technischen Support-Fall im Support Center erstellen.

Console

So erzwingen Sie die Beendigung einer Instance

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie die hängen gebliebene Instance aus.
3. Wählen Sie Instance-Status, Beendigung der Instance erzwingen.

   Beachten Sie, dass Beendigung der Instance erzwingen nur dann in der Konsole verfügbar ist, wenn sich Ihre Instance im Status `stopping` befindet. Wenn sich Ihre Instance in einem anderen Status befindet (außer `shutting-down` und`terminated`), können Sie den verwenden, AWS CLI um das Beenden Ihrer Instance zu erzwingen.
4. (Optional) Um das ordnungsgemäße Herunterfahren des Betriebssystems während der erzwungenen Beendigung zu umgehen, aktivieren Sie das Kontrollkästchen Herunterfahren des Betriebssystems überspringen.
5. Wählen Sie Beendigung erzwingen.

AWS CLI

So erzwingen Sie die Beendigung einer Instance

Verwenden Sie den Befehl erminate-instances mit der Option `--force`.

```
aws ec2 terminate-instances \
    --instance-ids i-1234567890abcdef0 \
    --force
```

Fügen Sie die Option `--skip-os-shutdown` hinzu, um das ordnungsgemäße Herunterfahren des Betriebssystems während der erzwungenen Beendigung zu umgehen.

```
aws ec2 terminate-instances \
    --instance-ids i-1234567890abcdef0 \
    --force \
    --skip-os-shutdown
```

PowerShell

So erzwingen Sie die Beendigung einer Instance

Verwenden Sie das Remove-EC2InstanceCmdlet und legen Sie den Wert auf fest-Enforce. true

```
Remove-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Enforce $true
```

Fügen Sie -SkipOsShutdown $true hinzu, um das ordnungsgemäße Herunterfahren des Betriebssystems während der erzwungenen Beendigung zu umgehen.

```
Remove-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Enforce $true `
    -SkipOsShutdown $true
```

Fortdauernde Anzeige einer beendeten Instance

Nachdem Sie eine Instance beendet haben, bleibt sie kurze Zeit sichtbar, bevor sie gelöscht wird. Der Status wird als angezeig `terminated`. Wenn der Eintrag nach einigen Stunden nicht gelöscht wird, wenden Sie sich an den Support.

Fehler: Die Instance ist möglicherweise nicht beendet worden. Ändern Sie das Instanzattribut 'disableApiTermination'

Wenn Sie versuchen, eine Instance zu beenden, und die Fehlermeldung The `instance i-1234567890abcdef0 may not be terminated. Modify its 'disableApiTermination' instance attribute` angezeigt wird, bedeutet dies, dass für die Instance der Beendigungsschutz aktiviert wurde. Der Beendigungsschutz verhindert, dass die Instance versehentlich beenden wird.

Bevor Sie die Instance beenden können, müssen Sie den Beendigungsschutz deaktivieren.

Weitere Informationen finden Sie unter Beendigungsschutz für Instances ändern.

Instances automatisch gestartet oder beendet

Im Allgemeinen bedeuten die folgenden Verhaltensweisen, dass Sie Amazon EC2 Auto Scaling, EC2 Fleet oder Spot Fleet verwendet haben, um Ihre Computerressourcen automatisch auf der Grundlage der von Ihnen definierten Kriterien zu skalieren:

- Sie beenden eine Instance, und eine neue Instance wird automatisch gestartet.
- Sie starten eine Instance, und eine Ihrer Instances wird automatisch beendet.
- Sie halten eine Instance an, und sie wird beendet, worauf eine neue Instance automatisch gestartet wird.

Um die Auto Scaling zu beenden, suchen Sie die Amazon EC2 Auto Scaling-Gruppe oder die Flotte, die die Instances startet, und setzen Sie entweder ihre Kapazität auf 0 oder löschen Sie sie.

Problembehandlung bei unerreichbaren Amazon-EC2-Instances

Die folgenden Informationen können Ihnen bei der Behebung von unerreichbaren Amazon-EC2-Instances helfen. Sie können Screenshots erstellen oder auf die Konsolenausgabe zugreifen, um Probleme zu diagnostizieren und festzustellen, ob Sie Ihre Instance neu starten sollten. Bei nicht erreichbaren Windows-Instances überprüfen Sie die vom Service zurückgesendeten Screenshots zur Fehlerbehebung.

Inhalt

- Instance-Neustart
- Instance-Konsolenausgabe
- Aufnehmen eines Screenshots einer nicht erreichbaren Instance
- Häufig verwendete Screenshots zur Fehlerbehebung bei nicht erreichbaren Windows-Instances
- Wiederherstellung einer Instance beim Ausfall eines Host-Computers
- Die Instance wurde offline angezeigt und unerwartet neu gestartet

Instance-Neustart

Die Möglichkeit, Instances, die sonst unerreichbar sind, neu zu starten, ist sowohl für die Problembehebung als auch für die allgemeine Instance-Verwaltung nützlich.

So wie Sie einen Computer über die Reset-Taste zurücksetzen können, so können Sie EC2 Instances mit der Amazon EC2-Konsole, der CLI oder der API zurücksetzen. Weitere Informationen finden Sie unter Eine Amazon-EC2-Instance neu starten.

Instance-Konsolenausgabe

Die Konsolenausgabe ist ein nützliches Tool für die Problemdiagnose. Es ist besonders hilfreich zur Behebung von Problemen mit dem Kernel und der Servicekonfiguration, die dazu führen können, dass eine Instance beendet wird oder nicht mehr erreichbar ist, bevor ihr SSH-Daemon gestartet werden kann.

- Linux-Instances – Die Ausgabe der Instance-Konsole zeigt genau die Konsolenausgabe an, die normalerweise auf einem physischen Monitor angezeigt wird, der an einen Computer angeschlossen ist. Die Konsolenausgabe gibt gepufferte Informationen zurück, die kurz nach einem Instance-Übergangsstatus (Start, Stopp, Neustart und Abbruch) gepostet wurden. Die bereitgestellte Ausgabe wird nicht kontinuierlich aktualisiert, sondern nur wenn es besonders sinnvoll ist.
- Windows-Instances – Die Ausgabe der Instance-Konsole enthält die letzten drei Fehler im Systemereignisprotokoll.

Auf die Konsolenausgabe kann nur der Instance-Eigentümer zugreifen.

Sie können die neueste Ausgabe der seriellen Konsole während des Instance-Lebenszyklus abrufen. Diese Option wird nur auf Nitro-basierten Instances unterstützt.

Console

Abrufen der Konsoleausgabe

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. Wählen Sie die Instance aus.
4. Wählen Sie Actions (Aktionen), Monitor and Troubleshoot (Überwachung und Fehlerbehebung), Get system log (Systemprotokoll abrufen).

AWS CLI

Abrufen der Konsoleausgabe

Verwenden Sie den Befehl get-console-output.

```
aws ec2 get-console-output --instance-id i-1234567890abcdef0
```

PowerShell

Abrufen der Konsoleausgabe

Verwenden Sie das cmdlet Get-EC2ConsoleOutput.

```
Get-EC2ConsoleOutput -InstanceId i-1234567890abcdef0
```

Aufnehmen eines Screenshots einer nicht erreichbaren Instance

Wenn Sie Ihre Instance nicht erreichen können, können Sie einen Screenshot Ihrer Instance aufnehmen und ihn als Bild anzeigen. Das Image kann den Status der Instance sichtbar machen, und die Problembehebung kann schneller durchgeführt werden.

Sie können während der Ausführung oder nach dem Absturz einer Instance Screenshots erstellen. Das Image wird im JPG-Format erstellt und umfasst maximal 100 KB. Für den Screenshot fallen keine Datenübertragungskosten an.

Einschränkungen

Dieses Feature wird in folgenden Fällen nicht unterstützt:

- Bare-Metal-Instances (Instances des Typs `*.metal`)
- Die Instance verwendet einen NVIDIA-GRID-Treiber
- Instances, die von ARM-basierten Graviton-Prozessoren angetrieben werden
- Windows-Instances in AWS Outposts
- Windows-Instances in AWS Local Zones

Regionsunterstützung

Dieses Feature ist in den folgenden Regionen nicht verfügbar:

- Asien-Pazifik (Thailand)
- Mexiko (Zentral)

- GovCloud-Regionen

Console

So rufen Sie einen Screenshot einer Instance ab

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. Wählen Sie die Instance aus, für die Sie einen Screenshot aufnehmen möchten.
4. Wählen Sie Actions (Aktionen), Monitor and Troubleshoot (Überwachung und Fehlerbehebung), Get instance screenshot (Instance-Screenshot abrufen).
5. Wählen Sie Download (Herunterladen) oder klicken Sie mit der rechten Maustaste auf das Image, um es herunterzuladen und zu speichern.

AWS CLI

So erstellen Sie einen Screenshot einer Instance

Verwenden Sie den Befehl get-console-screenshot. Die Ausgabe ist base64-kodiert.

```
aws ec2 get-console-screenshot --instance-id i-1234567890abcdef0
```

PowerShell

So erstellen Sie einen Screenshot einer Instance

Verwenden Sie das cmdlet Get-EC2ConsoleScreenshot. Die Ausgabe ist base64-kodiert.

```
Get-EC2ConsoleScreenshot -InstanceId i-1234567890abcdef0
```

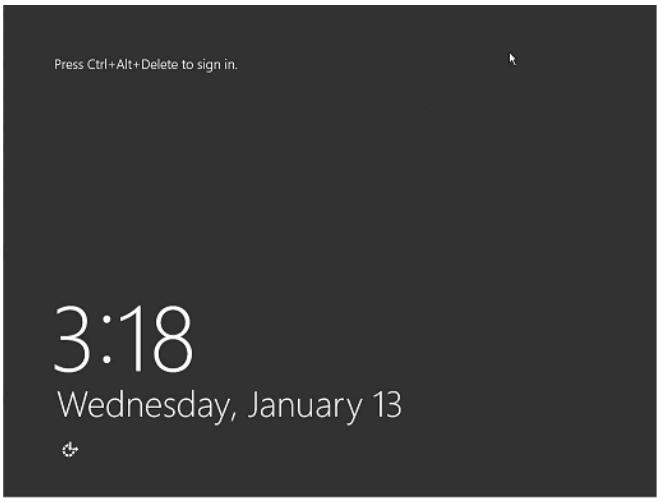
Häufig verwendete Screenshots zur Fehlerbehebung bei nicht erreichbaren Windows-Instances

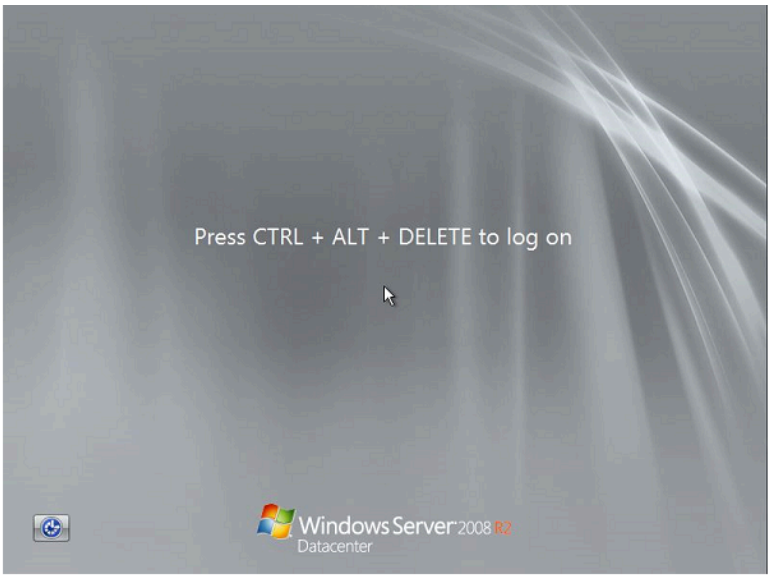
Die folgenden Informationen können Ihnen dabei helfen, Probleme in Zusammenhang mit unerreichbaren Windows-Instances zu beheben, indem Sie die Screenshots analysieren, die von dem Service zurückgegeben werden.

- Anmeldebildschirm (Strg+Alt+Entf)
- Wiederherstellungskonsolen-Bildschirm
- Windows-Start-Manager-Bildschirm
- Sysprep-Bildschirm
- Vorbereitungsbildschirm
- Windows Update-Bildschirm
- Chkdsk

Anmeldebildschirm (Strg+Alt+Entf)

Der Console Screenshot Service hat Folgendes zurückgegeben.





Wenn eine Instance bei der Anmeldung nicht mehr erreichbar ist, ist möglicherweise Ihre Netzwerkanbindung falsch konfiguriert oder es liegt ein Problem mit dem Windows-Remotedesktopdienst vor. Außerdem kann es vorkommen, dass eine Instance nicht mehr reagiert, wenn ein Prozess die CPU extrem stark auslastet.

Netzwerkkonfiguration

Verwenden Sie die folgenden Informationen, um Ihre AWS für Microsoft Windows und für das lokale (On-Premises) bzw. über die private Cloud eingerichtete Netzwerk den Zugriff auf die Instance nicht blockieren.

AWS-Netzwerkkonfiguration

Konfiguration	Überprüfen
Sicherheitsgruppenkonfiguration	Überprüfen Sie, ob Port 3389 für Ihre Sicherheitsgruppe offen ist. Stellen Sie sicher, dass die Verbindung zu der richtigen öffentlichen IP-Adresse hergestellt wird. Wenn die Instance mit keiner Elastic IP-Adresse verknüpft war, ändert sich die öffentliche IP-Adresse nach einem erneuten Start der Instance. Weitere Informationen finden Sie unter Der Remotedesktopdienst kann keine Verbindung zu dem Remotecomputer herstellen.
VPC-Konfiguration (Netzwerk-ACLs)	Stellen Sie sicher, dass die Access Control List (ACL) für Ihre Amazon VPC den Zugriff nicht blockiert. Weitere Informationen finden Sie unter Netzwerk-ACLs im Amazon VPC Benutzerhandbuch.
VPN-Konfiguration	Wenn Sie die Verbindung zu Ihrer VPC unter Verwendung einer Virtual Private Network (VPN) herstellen, überprüfen Sie die Anbindung des VPN-Tunnels. Weitere Informationen finden Sie unter Fehlerbehebung für AWS Client VPN: Tunnel-Konnektivitätsprobleme mit einer VPC.

Windows-Netzwerkkonfiguration

Konfiguration	Überprüfen
Windows-Firewall	Überprüfen Sie, ob die Windows-Firewall die Verbindung zu Ihrer Instance blockiert. Deaktivieren Sie die Windows-Firewall wie in Punkt 7 im Abschnitt zur Problembehandlung für Remotedesktopverbindungen

Konfiguration	Überprüfen
	unter beschrieb, Der Remotedesktopdienst kann keine Verbindung zu dem Remotecomputer herstellen.
Erweiterte TCP/IP-Konfiguration (statische IP-Adresse)	Möglicherweise reagiert die Instance nicht, weil Sie eine statische IP-Adresse konfiguriert haben. Wenn Sie eine VPC haben, erstellen Sie eine Netzwerkschnittstelle und fügen diese der Instance an.

On-Premises- bzw. über die private Cloud eingerichtete Netzwerkkonfiguration

Überprüfen Sie, ob nicht die lokale Netzwerkkonfiguration den Zugriff blockiert. Versuchen Sie, eine Verbindung zu einer anderen Instance herzustellen, die sich in derselben VPC befindet wie die nicht erreichbare Instance. Wenn Sie auch nicht auf diese andere Instance zugreifen können, überprüfen Sie zusammen mit Ihrem Netzwerkadministrator, ob der Zugriff durch lokale Richtlinien beschränkt wird.

Probleme mit Remotedesktopdiensten

Wenn die Instance bei der Anmeldung nicht erreichbar ist, liegt möglicherweise dem Remotedesktopdienst (Remote Desktop Service, RDS) auf der Instance vor.

> **Tip**
>
> Sie können das `AWSSupport-TroubleshootRDP` Runbook verwenden, um verschiedene Einstellungen zu überprüfen und zu ändern, die sich auf RDP-Verbindungen (Remote Desktop Protocol) auswirken können. Weitere Informationen finden Sie unter `AWSSupport-TroubleshootRDP` in der Referenz zum AWS Systems Manager-Automation-Runbook.

Remotedesktopdienst-Konfiguration

Konfiguration	Überprüfen
RDS wird ausgeführt.	Überprüfen Sie, ob RDS auf der Instance ausgeführt wird. Stellen Sie unter Verwendung der Microsoft Management

Konfiguration	Überprüfen
	Console (MMC) mit dem Dienste-Snap-In () eine Verbindung zu der Instance (`services.msc`). Überprüfen Sie in der Liste der Dienste, dass der Dienst Remotedesktopdienste den Status Wird ausgeführt trägt. wenn dies nicht der Fall ist, starten Sie den Dienst und legen Sie als Startup-Typ Automatisch fest. Wenn Sie auch über das Dienste-Snap-In keine Verbindung zu der Instance herstellen können, lösen Sie das Stamm-Volume von der Instance, nehmen Sie einen Snapshot des Volumes oder erstellen Sie anhand des Volumes ein AMI, weisen Sie dann das gelöste Stamm-Volume einer anderen Instance in derselben Availability Zone als sekundäres Volume zu und modifizieren Sie den Start-Registrierungsschlüssel. Wenn Sie fertig sind, binden Sie das Stamm-Volume wieder an die ursprüngliche Instance an.
RDS ist aktiviert.	Selbst wenn der Dienst gestartet wird, kann er deaktiviert sein. Trennen Sie das Stammvolume von der Instance, erstellen Sie einen Snapshot des Volumes oder erstellen Sie ein AMI daraus, fügen Sie das ursprüngliche Volume an eine andere Instance in derselben Availability Zone wie ein sekundäres Volume an und aktivieren Sie den Service, indem Sie den Terminalserver-Registrierungsschlüssel ändern, wie in Aktivieren von Remotedesktop für eine EC2-Instance mit Remote-Registrierung beschrieben. Wenn Sie fertig sind, binden Sie das Stamm-Volume wieder an die ursprüngliche Instance an.

Hohe CPU-Auslastung

Überprüfen Sie die Metrik CPUUtilization (Maximum) in Ihrer Instance unter Verwendung von Amazon CloudWatch. Wenn CPUUtilization (Maximum) sehr hoch ist, warten Sie, bis die CPU weniger stark ausgelastet ist, und wiederholen Sie dann den Verbindungsversuch. Eine hohe CPU-Auslastung kann die folgenden Ursachen haben:

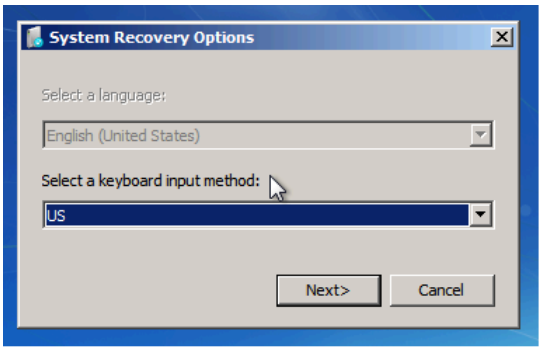
- Windows Update

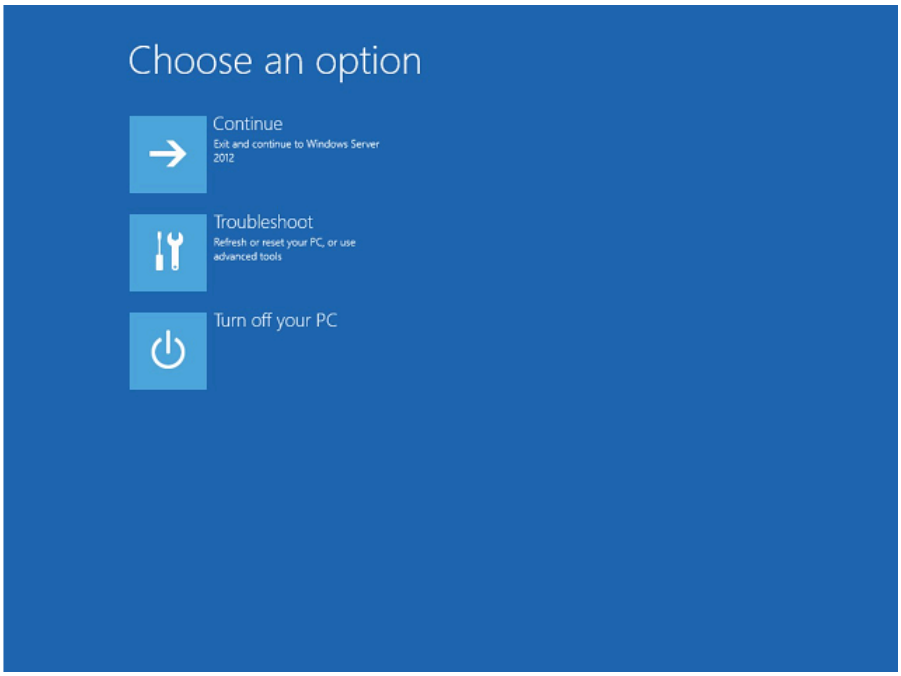
- Scan-Aktivität von Sicherheitssoftware
- Benutzerdefiniertes Startup-Script
- Aufgaben-Scheduler

Weitere Informationen finden Sie unter Abrufen von Statistiken für eine bestimmte Ressource im Amazon CloudWatch-Benutzerhandbuch. Weitere Tipps zur Fehlerbehebung finden Sie unter Hohe CPU-Auslastung kurz nach dem Windows-Start (Nur Windows-Instances).

Wiederherstellungskonsolen-Bildschirm

Der Console Screenshot Service hat Folgendes zurückgegeben.





Wenn für `bootstatuspolicy` ein anderer Wert als `ignoreallfailures` festgelegt ist, besteht die Möglichkeit, dass das Betriebssystem beim Starten die Wiederherstellungskonsole startet und in diesem Zustand verbleibt. Führen Sie folgende Schritte durch, um die Konfiguration für `bootstatuspolicy` in `ignoreallfailures` zu ändern.

Die Richtlinienkonfiguration für von AWS bereitgestellte öffentliche Windows-AMIs ist standardmäßig auf `ignoreallfailures` eingestellt.

1. Halten Sie die unerreichbare Instance an.
2. Erstellen Sie einen Snapshot des Stamm-Volumes. Das Stamm-Volume ist als an die Instance angefüg `/dev/sda1`.

Lösen Sie das Stamm-Volume von der nicht erreichbaren Instance, nehmen Sie einen Snapshot des Volumes oder erstellen Sie anhand des Volumes ein AMI und verbinden Sie es dann mit einer anderen Instance in derselben Availability Zone als sekundäres Volume.

> **Warning**
>
> Wenn Ihre temporäre Instance und die ursprüngliche Instance mit demselben AMI gestartet wurden, müssen Sie zusätzliche Schritte durchführen, da Sie sonst die ursprüngliche Instance nach der Wiederherstellung ihres Root-Volumes aufgrund einer Kollision der Festplattensignaturen nicht mehr booten können. Wenn Sie eine temporäre Instance mit demselben AMI erstellen müssen, um eine Kollision der Festplattensignaturen zu vermeiden, führen Sie die Schritte in Kollision der Festplattensignatur aus.
> Alternativ können Sie ein anderes AMI für die temporäre Instance verwenden. Wenn beispielsweise die Original-Instance ein AMI für Windows Server 2016 verwendet, starten Sie die temporäre Instance, indem Sie ein Windows-AMI für Windows Server 2019 verwenden.

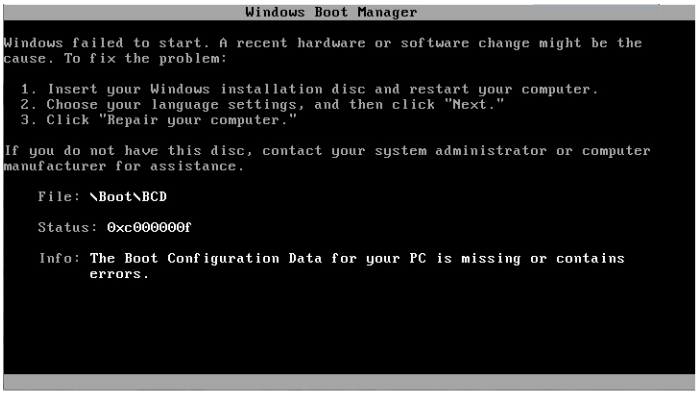
3. Melden Sie sich an der Instance an und führen Sie an der Eingabeaufforderung den folgenden Befehl aus, um die `bootstatuspolicy`-Konfiguration in `ignoreallfailures` zu ändern:

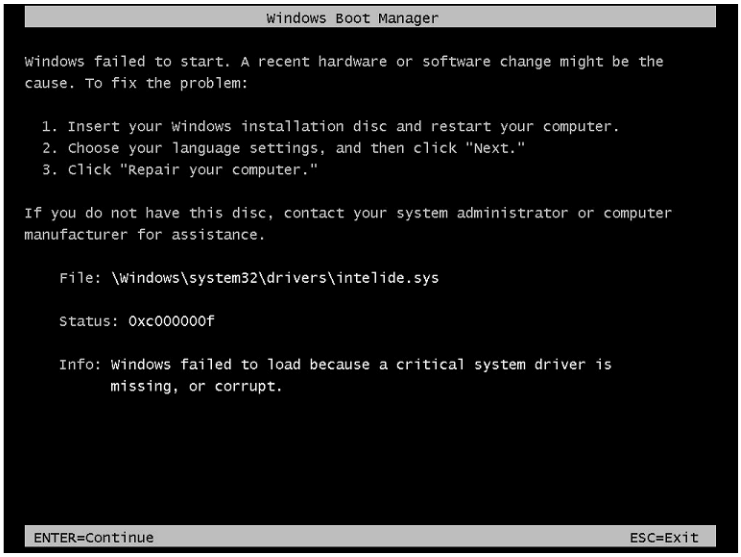
```
bcdedit /store Drive Letter:\boot\bcd /set {default} bootstatuspolicy
 ignoreallfailures
```

4. Hängen Sie das Volume wieder an die unerreichbare Instance an und starten Sie die Instance wieder.

Windows-Start-Manager-Bildschirm

Der Console Screenshot Service hat Folgendes zurückgegeben.

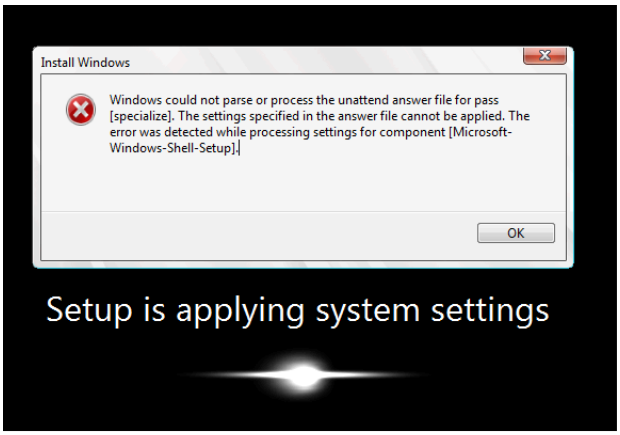


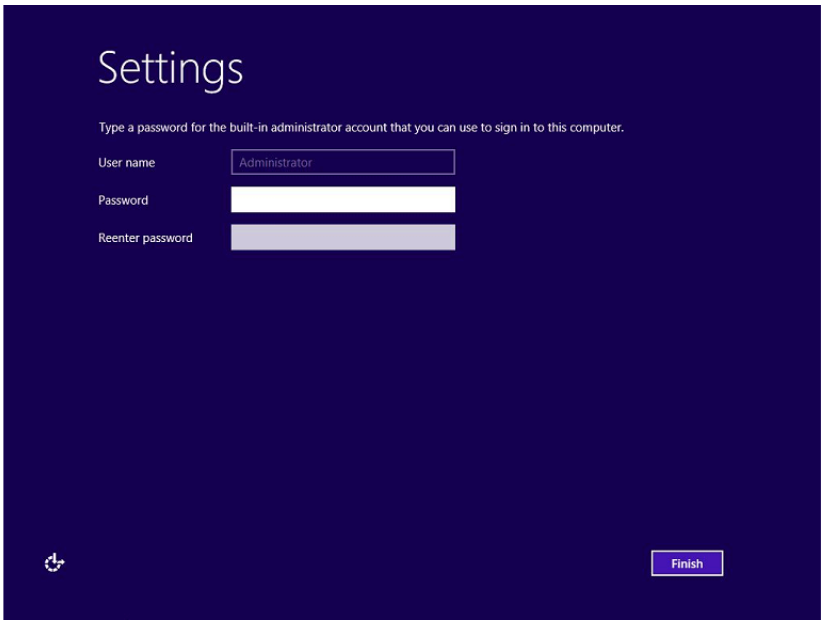


Das Betriebssystem wurde aufgrund eines fatalen Fehlers im Dateisystem oder in der Registrierung angehalten. Wenn eine Instance auf diese Weise „einfriert“, sollten Sie sie aus einem möglichst neuen Sicherungs-AMI wiederherstellen oder eine Austausch-Instance starten. Wenn Sie noch auf Daten auf der Instance zugreifen müssen, lösen Sie alle Stamm-Volumes von der nicht erreichbaren Instance, nehmen Sie einen Snapshot dieser Volumes oder erstellen Sie anhand der Volumes AMIs und verbinden Sie sie dann mit einer anderen Instance in derselben Availability Zone als sekundäres Volume.

Sysprep-Bildschirm

Der Console Screenshot Service hat Folgendes zurückgegeben.

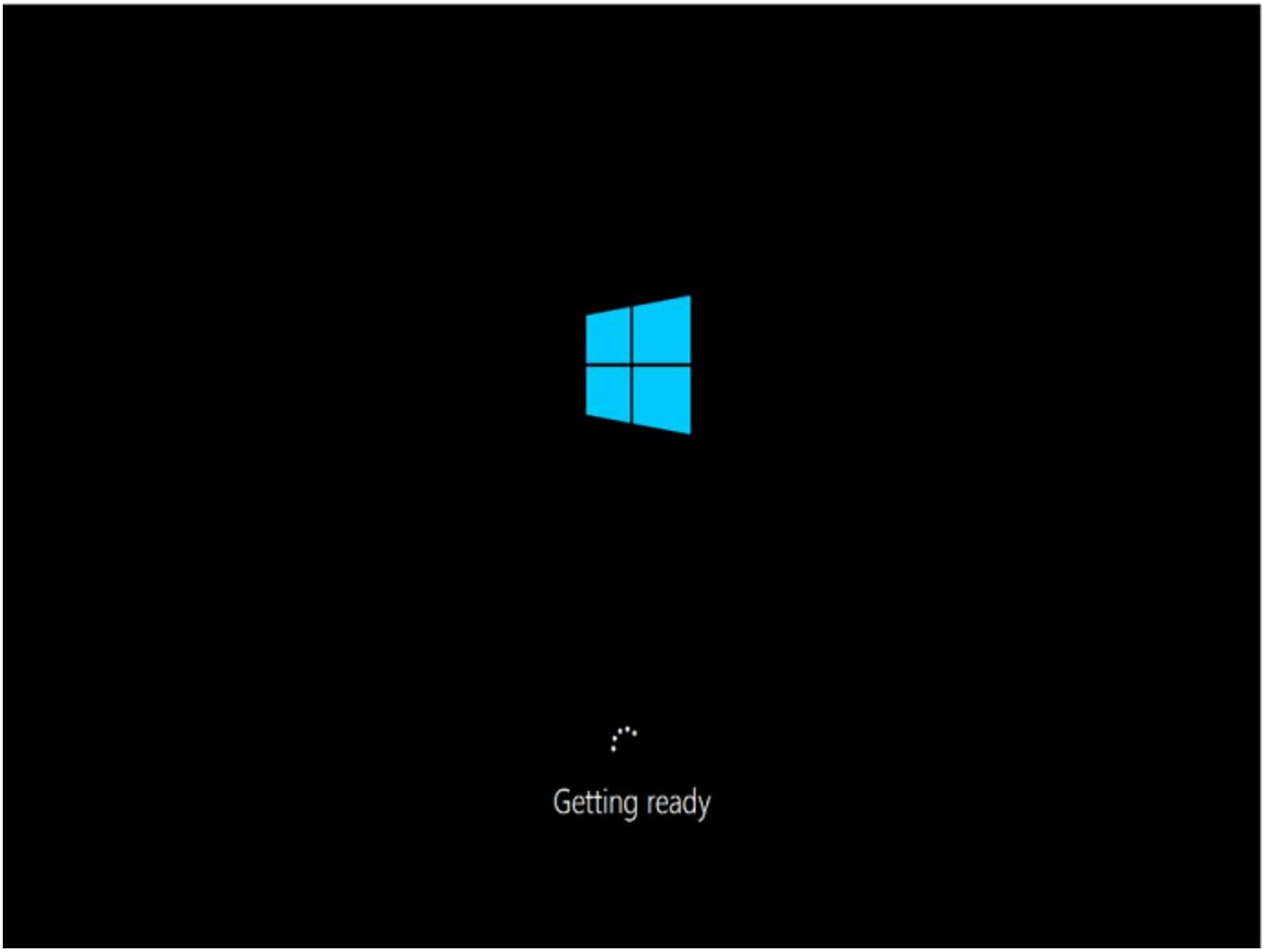




Dieser Bildschirm wird möglicherweise angezeigt, wenn Sie den EC2Config-Service nicht zum Aufrufen von Sysprep verwendet haben oder wenn das Betriebssystem während der Ausführung von Sysprep fehlgeschlagen ist. Sie können das Passwort mit EC2Rescue zurücksetzen. Andernfalls lesen Sie unter weiter Ein Amazon-EC2-AMI mit Windows Sysprep erstellen.

Vorbereitungsbildschirm

Der Console Screenshot Service hat Folgendes zurückgegeben.



Aktualisieren Sie den Instance Console Screenshot Service einige Male, um sicherzustellen, dass sich das Ringsymbol für die Fortschrittsanzeige dreht. Wenn sich das Ringsymbol dreht, warten Sie, bis das Betriebssystem gestartet ist. Sie können auch die Metrik CPUUtilization (Maximum) auf Ihrer Instance mit Amazon CloudWatch überprüfen, um festzustellen, ob das Betriebssystem aktiv ist. Wenn sich das Ringsymbol nicht dreht, ist die Instance möglicherweise während des Startvorgangs eingefroren. Starten Sie die Instance neu. Wenn sich das Problem nicht durch einen Neustart beheben lässt, sollten Sie die Instance aus einem möglichst neuen Sicherungs-AMI wiederherstellen

oder eine Austausch-Instance starten. Wenn Sie noch auf Daten in der Instance zugreifen müssen, lösen Sie das Stamm-Volume aus der nicht erreichbaren Instance und erstellen Sie einen Snapshot des Volumes oder erstellen Sie ein AMI aus dem Volume. Hängen Sie das Volume an eine andere Instance in derselben Availability Zone als sekundäres Volume an.

Windows Update-Bildschirm

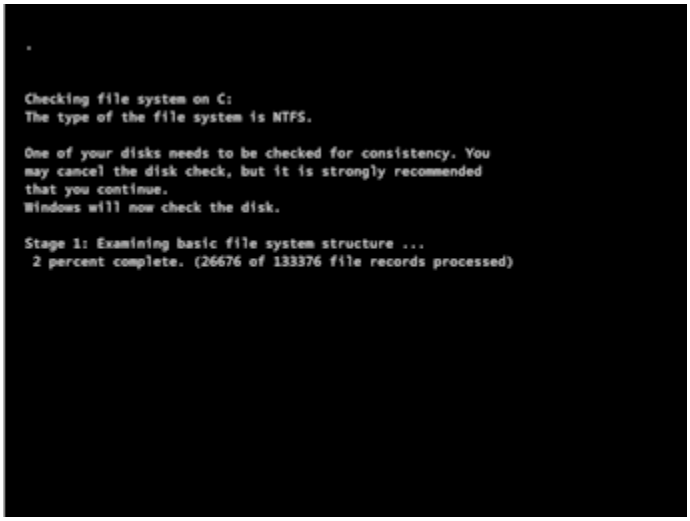
Der Console Screenshot Service hat Folgendes zurückgegeben.

Der Windows Update-Prozess aktualisiert die Registrierung. Warten Sie bis die Aktualisierung abgeschlossen ist. Halten Sie die Instance nicht an und starten Sie sie nicht neu, da dies während einer Aktualisierung zu einer Datenbeschädigung führen kann.

> **Note**
>
> Der Windows Update-Prozess kann während der Aktualisierung Serverressourcen beanspruchen. Falls dieses Problem bei Ihnen häufiger auftritt, sollten Sie möglicherweise schnellere Instance-Typen bzw. schnellere EBS-Volumes verwenden.

Chkdsk

Der Console Screenshot Service hat Folgendes zurückgegeben.



Windows führt das System-Tool chkdsk über dem Laufwerk aus, um die Integrität des Dateisystems zu überprüfen und logische Fehler in dem Dateisystem zu beheben. Warten Sie, bis der Vorgang abgeschlossen ist.

Wiederherstellung einer Instance beim Ausfall eines Host-Computers

Wenn ein nicht wiederherstellbarer Fehler mit der Hardware eines zugrunde liegenden Host-Computers vorliegt, kann AWS ein "Stop"-Ereignis für die Instance planen. Sie werden im Vorfeld per E-Mail über ein solches Ereignis informiert.

So stellen Sie eine Amazon EBS-gestützte Instance, die auf einem ausgefallen Host-Computer ausgeführt wird, wieder her

1. Sichern Sie alle wichtigen Daten auf Ihren Instance-Speicher-Volumes in Amazon EBS oder Amazon S3.
2. Halten Sie die Instance an.
3. Starten Sie die Instance.
4. Stellen Sie alle wichtigen Daten wieder her.

Weitere Informationen finden Sie unter Stoppen und starten Sie EC2 Amazon-Instances.

So stellen Sie eine Instance mit einem Instance-Speicher-Root-Volume, die auf einem ausgefallen Host-Computer ausgeführt wird, wieder her

1. Erstellen Sie aus der Instance ein AMI.
2. Laden Sie das Image in Amazon S3 hoch.

3. Sichern Sie wichtige Daten in Amazon EBS oder Amazon S3.
4. Beenden Sie die Instance.
5. Starten Sie eine neue Instance aus dem AMI.
6. Stellen Sie alle wichtigen Daten auf der neuen Instance wieder her.

Die Instance wurde offline angezeigt und unerwartet neu gestartet

Wenn die Instance anscheinend offline war und dann unerwartet neu gestartet wurde, wurde sie möglicherweise automatisch wiederhergestellt. Dies passiert, wenn AWS erkennt, dass die Instance aufgrund eines zugrunde liegenden Hardware- oder Softwareproblems nicht verfügbar ist und entweder die vereinfachte automatische Wiederherstellung oder die aktionsbasierte CloudWatch-Wiederherstellung für die Instance aktiviert ist.

Während des Wiederherstellungsprozesses versucht AWS, die Verfügbarkeit der Instance wiederherzustellen, indem sie auf eine andere Hardware migriert wird. Informationen dazu, ob für Ihre Instance eine automatische Instance-Wiederherstellung stattgefunden hat, finden Sie unter Überprüfen, ob eine automatische Instance-Wiederherstellung stattgefunden hat.

> **Note**
>
> Wenn Ihre Workload oder Ihre Anwendung nicht reagiert, überprüfen Sie, ob sie auf der Instance ausgeführt wird. Wenn nicht, starten Sie sie manuell. Um dieses Problem in Zukunft zu vermeiden, implementieren Sie einen Wiederherstellungsplan, um sicherzustellen, dass Ihre Workload oder Anwendung nach der Wiederherstellung der Instance ordnungsgemäß funktioniert.

Fehlersuche bei Verbindungsproblemen mit Ihrer Amazon-EC2-Linux-Instance

Die folgenden Informationen und häufigen Fehler können Ihnen bei der Fehlersuche für die Verbindung zu Ihrer Linux-Instance helfen.

Verbindungsprobleme

- Häufige Ursachen für Verbindungsprobleme

- Fehler beim Herstellen der Verbindung mit Ihrer Instance: „Connection timed out“
- Fehler: Schlüssel kann nicht geladen werden ... Erwartend: JEDER PRIVATE SCHLÜSSEL
- Fehler: Benutzerschlüssel wird vom Server nicht erkannt
- Fehler: Berechtigung verweigert oder Verbindung durch [instance] Port 22 geschlossen
- Fehler: Ungeschützte private Schlüsseldatei
- Fehler: Der private Schlüssel muss mit „-----BEGIN RSA PRIVATE KEY-----“ und mit „-----END RSA PRIVATE KEY-----“ enden
- Fehler: Hostschlüssel-Validierung fehlgeschlagen
- Fehler: Der Server lehnte unseren Schlüssel ab oder es sind keine unterstützten Authentifizierungsmethoden verfügbar.
- Die Instance ist nicht per Ping erreichbar.
- Fehler: Der Server hat die Netzwerkverbindung unerwartet geschlossen
- Fehler: Hostschlüssel-Validierung fehlgeschlagen für EC2 Instance Connect
- Mit EC2 Instance Connect kann keine Verbindung zur Ubuntu-Instance hergestellt werden
- Ich habe meinen privaten Schlüssel verloren. Wie kann ich eine Verbindung zu meiner Instance herstellen?

Häufige Ursachen für Verbindungsprobleme

Wir empfehlen, dass Sie mit der Behebung von Instance-Verbindungsproblemen beginnen, indem Sie sicherstellen, dass Sie die folgenden Aufgaben korrekt ausgeführt haben.

Überprüfen des Benutzernamens für Ihre Instance

Sie können mit dem Benutzernamen für Ihr Benutzerkonto oder dem Standardbenutzernamen für das AMI, das Sie zum Starten Ihrer Instance verwendet haben, eine Verbindung zu Ihrer Instance herstellen.

- Abrufen des Benutzernamens für Ihr Benutzerkonto ab.

  Weitere Informationen zum Erstellen eines Benutzerkontos finden Sie unter Verwalten von Benutzern auf einer Amazon-EC2-Linux-Instance.
- Abrufen des Standardbenutzernamens für das AMI, das Sie zum Starten der Instance verwendet haben.

Zum Starten der Instance verwendetes AMI	Standardbenutzername
Amazon Linux	`ec2-user`
CentOS	`centos` oder `ec2-user`
Debian	`admin`
Fedora	`fedora` oder `ec2-user`
FreeBSD	`ec2-user`
RHEL	`ec2-user` oder `root`
SUSE	`ec2-user` oder `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Sonstige	Wenden Sie sich an den AMI-Anbieter

Überprüfen Sie, ob Ihre Sicherheitsgruppenregeln Datenverkehr zulassen.

Stellen Sie sicher, dass die mit Ihrer Instance verknüpfte Sicherheitsgruppe eingehenden SSH-Datenverkehr von Ihrer IP-Adresse zulässt. Die standardmäßige Sicherheitsgruppe für die VPC lässt keinen eingehenden SSH-Datenverkehr zu. Die über den Launch Instance Wizard erstellte Sicherheitsgruppe lässt eingehenden SSH-Datenverkehr standardmäßig zu. Schritte zum Hinzufügen einer Regel für eingehenden SSH-Datenverkehr zu Ihrer Linux-Instance finden Sie unter Regeln für die Verbindung mit Instances von Ihrem Computer aus. Schritte zur Überprüfung finden Sie unter Fehler beim Herstellen der Verbindung mit Ihrer Instance: „Connection timed out“.

Stellen Sie sicher, dass Ihre Instance bereit ist.

Wenn Sie die Instance starten, kann es einige Minuten dauern, bis die Instance bereit ist, Verbindungen zu akzeptieren. Überprüfen Sie Ihre Instance, um sicherzustellen, dass sie ausgeführt wird und ihre Statusüberprüfungen bestanden hat.

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie anschließend Ihre Instance aus.
3. Überprüfen Sie Folgendes:
   a. Stellen Sie in der Spalte Instance state (Instance-Status) sicher, dass sich Ihre Instance im `running`-Status befindet.
   b. Überprüfen Sie in der Spalte Statusprüfung, ob Ihre Instance die beiden Statusprüfungen bestanden hat.

Sicherstellen, dass alle Voraussetzungen zum Herstellen einer Verbindung erfüllt sind

Stellen Sie sicher, dass Sie über alle Informationen verfügen, die Sie für die Verbindung benötigen. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance mit SSH.

Herstellen einer Verbindung von Linux oder macOS X

Wenn es sich bei Ihrem lokalen Computer-Betriebssystem um Linux oder macOS X handelt, lesen Sie das Folgende für die spezifischen Voraussetzungen, um eine Verbindung zu einer Linux-Instance herzustellen:

- SSH-Client
- EC2 Instance Connect
- AWS Systems Manager Session Manager

Herstellen einer Verbindung über Windows

Wenn es sich bei Ihrem lokalen Computer-Betriebssystem um Windows handelt, lesen Sie das Folgende für die spezifischen Voraussetzungen, um eine Verbindung zu einer Linux-Instance herzustellen:

- OpenSSH
- PuTTY
- AWS Systems Manager Session Manager
- Windows-Subsystem für Linux

Prüfen Sie, ob es sich bei der Instance um eine verwaltete Instance handelt

Benutzerinitiierte Verbindungen zu verwalteten Instances sind nicht erlaubt. Um festzustellen, ob die Instance verwaltet wird, suchen Sie das Feld Verwaltet für die Instance. Wenn der Wert wahr ist, handelt es sich um eine verwaltete Instance. Weitere Informationen finden Sie unter Verwaltete Amazon-EC2-Instances.

Fehler beim Herstellen der Verbindung mit Ihrer Instance: „Connection timed out“

Wenn Sie versuchen, eine Verbindung zu Ihrer Instance herzustellen, und die Fehlermeldung `Network error: Connection timed out` oder `Error connecting to [instance], reason: -> Connection timed out: connect` erhalten, versuchen Sie Folgendes:

Prüfen Sie Ihre Sicherheitsgruppenregeln.

Sie benötigen eine Sicherheitsgruppenregel, die den eingehenden Datenverkehr von Ihrer öffentlichen IPv4-Adresse Ihres lokalen Computers auf dem entsprechenden Port zulässt.

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie anschließend Ihre Instance aus.
3. Überprüfen Sie auf der Registerkarte Security (Sicherheit) am unteren Rand der Konsolenseite unter Inbound rules (Eingangsregeln), die Liste der Regeln, die für die ausgewählte Instance gültig sind. Überprüfen Sie, ob eine Regel vorhanden ist, die den Datenverkehr von Ihrem Computer auf Port 22 (SSH) zulässt.

   Wenn Ihre Sicherheitsgruppe keine Regel enthält, die eingehenden Datenverkehr von Ihrem lokalen Computer zulässt, fügen Sie eine Regel zu Ihrer Sicherheitsgruppe hinzu. Weitere Informationen finden Sie unter Regeln für die Verbindung mit Instances von Ihrem Computer aus.
4. Die Regel, die eingehenden Datenverkehr zulässt, finden Sie im Feld Quelle. Wenn der Wert eine einzelne IP-Adresse ist und die IP-Adresse nicht statisch ist, wird bei jedem Neustart des Computers eine neue IP-Adresse zugewiesen. Dies führt dazu, dass die Regel den IP-Adressverkehr Ihres Computers nicht berücksichtigt. Die IP-Adresse darf nicht statisch sein, wenn sich Ihr Computer in einem Unternehmensnetzwerk befindet oder Sie eine Verbindung über einen Internetdienstanbieter (ISP) herstellen oder Ihre Computer-IP-Adresse dynamisch ist und sich bei jedem Neustart des Computers ändert. Um sicherzustellen, dass Ihre Sicherheitsgruppenregel eingehenden Datenverkehr von Ihrem lokalen Computer zulässt, geben

Sie den IP-Adressbereich an, der von Client-Computern verwendet wird, anstatt eine einzelne IP-Adresse für Quelle anzugeben.

Weitere Informationen zu den Regeln der Sicherheitsgruppe finden Sie unter Sicherheitsgruppenregeln im Amazon VPC-Benutzerhandbuch.

Überprüfen Sie die Routing-Tabelle für das Subnetz.

Sie benötigen eine Route, die den gesamten Datenverkehr außerhalb der VPC an das Internet-Gateway für die VPC sendet.

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie anschließend Ihre Instance aus.
3. Notieren Sie sich auf der Registerkarte Networking (Netzwerk) die Werte für VPC ID (VPC-ID) und Subnet ID (Subnetz-ID).
4. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
5. Wählen Sie im Navigationsbereich Internet Gateways aus. Überprüfen Sie, ob Ihrer VPC ein Internet-Gateway angefügt ist. Andernfalls wählen Sie Create internet gateway (Internet-Gateway erstellen), geben Sie einen Namen für das Internet-Gateway ein und wählen Sie Create internet gateway (Internet-Gateway erstellen). Wählen Sie dann für das von Ihnen erstellte Internet-Gateway Actions (Aktionen), Attach to VPC (An VPC anhängen), wählen Sie Ihre VPC aus und wählen Sie dann Attach internet gateway (Internet-Gateway anhängen), um es an Ihre VPC anzuhängen.
6. Wählen Sie im Navigationsbereich die Option Subnets und dann Ihr Subnetz aus.
7. Überprüfen Sie, ob auf der Registerkarte Route Table (Routing-Tabelle) eine Route mit `0.0.0.0/0` unter "Destination" und das Internet-Gateway für Ihre VPC unter "Target" vorhanden ist. Wenn Sie eine Verbindung mit Ihrer Instance mithilfe der IPv6-Adresse herstellen, überprüfen Sie, dass eine Route für den gesamten IPv6-Datenverkehr (`::/0`) vorhanden ist, die zum Internet-Gateway führt. Andernfalls gehen Sie wie folgt vor:

   a. Wählen Sie die ID der Routing-Tabelle (rtb-xxxxxxxx) aus, um zur Routing-Tabelle zu gelangen.

   b. Klicken Sie auf der Registerkarte Routes (Routen) auf Edit routes (Routen bearbeiten). Wählen Sie Add route (Route hinzufügen) aus, verwenden Sie `0.0.0.0/0` als Ziel und das Internet-Gateway als Ziel. Wählen Sie für IPv6 Add route (Route hinzufügen) aus, verwenden Sie `::/0` als Ziel und das Internet-Gateway als Ziel.

c. Wählen Sie Save Rules (Routen speichern) aus.

Überprüfen Sie die Access Control List (ACL) für das Subnetz.

Die Netzwerk-ACLs müssen ein- und ausgehenden Datenverkehr von Ihrer lokalen IP-Adresse auf Port 22 zulassen. Sie müssen auch ausgehenden Datenverkehr zu den kurzlebigen Ports (1024-65535) zulassen.

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets aus.
3. Subnetz auswählen
4. Stellen Sie auf der Registerkarte Netzwerk-ACL für Eingehende Regeln sicher, dass die Regeln eingehenden Datenverkehr von Ihrem Computer auf dem erforderlichen Port zulassen. Andernfalls löschen oder ändern Sie die Regel, die den Datenverkehr blockiert.
5. Überprüfen Sie für ausgehende Regeln, ob die Regeln ausgehenden Datenverkehr zu Ihrem Computer über die kurzlebigen Ports zulassen. Andernfalls löschen oder ändern Sie die Regel, die den Datenverkehr blockiert.

Wenn sich Ihr Computer in einem Unternehmensnetzwerk befindet

Fragen Sie Ihren Netzwerkadministrator, ob die interne Firewall ein- und ausgehenden Datenverkehr von Ihrem Computer auf Port 22 zulässt.

Wenn auf Ihrem Computer eine Firewall aktiviert ist, überprüfen Sie, dass diese den ein- und ausgehenden Datenverkehr von Ihrem Computer auf Port 22 zulässt.

Prüfen Sie, ob Ihre Instance über eine öffentliche IPv4-Adresse verfügt.

Falls nicht, verknüpfen Sie eine Elastic IP-Adresse mit der Instance. Weitere Informationen finden Sie unter Elastic-IP-Adressen.

Überprüfen Sie die CPU-Auslastung auf Ihrer Instance. Möglicherweise ist der Server überlastet.

AWS stellt automatisch Daten wie Amazon-CloudWatch-Metriken und Instance-Status bereit. Anhand dieser Daten können Sie feststellen, wie hoch die CPU-Auslastung auf Ihrer Instance ist, und die Verarbeitung Ihrer Lasten nach Bedarf ändern. Weitere Informationen finden Sie unter Überwachen Sie Ihre Instances mit CloudWatch.

- Wenn Ihre Last variabel ist, können Sie Ihre Instances automatisch mit Auto Scaling und Elastic Load Balancing nach oben und unten skalieren.
- Wenn Ihre Last kontinuierlich zunimmt, können Sie auf einen größeren Instance-Typ umsteigen. Weitere Informationen finden Sie unter Änderungen des EC2 Amazon-Instanztyps.

Um eine Verbindung mit Ihrer Instance mit einer IPv6-Adresse herzustellen, prüfen Sie Folgendes:

- Ihr Subnetz muss einer Routing-Tabelle zugeordnet sein, die über eine Route für IPv6-Datenverkehr (`::/0`) zu einem Internet-Gateway verfügt.
- Ihre Sicherheitsgruppenregeln müssen eingehenden Datenverkehr von Ihrer lokalen IPv6-Adresse auf Port 22 zulassen.
- Ihre Netzwerk-ACL-Regeln müssen ein- und ausgehenden IPv6-Datenverkehr zulassen.
- Wenn Sie Ihre Instance aus einem älteren AMI gestartet haben, ist sie möglicherweise nicht für DHCPv6 konfiguriert (IPv6-Adressen werden nicht automatisch von der Netzwerkschnittstelle erkannt). Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf Ihren Instances im Benutzerhandbuch von Amazon VPC.
- Ihr lokaler Computer muss über eine IPv6-Adresse verfügen und zur Verwendung von IPv6 konfiguriert sein.

Fehler: Schlüssel kann nicht geladen werden ... Erwartend: JEDER PRIVATE SCHLÜSSEL

Wenn Sie versuchen, eine Verbindung mit Ihrer Instance herzustellen und die Fehlermeldung `unable to load key ... Expecting: ANY PRIVATE KEY` erhalten, ist die Datei, in der der private Schlüssel gespeichert ist, nicht korrekt konfiguriert. Auch wenn die Datei mit dem privaten Schlüssel auf `.pem` endet, ist sie möglicherweise dennoch falsch konfiguriert. Eine mögliche Ursache für eine falsch konfigurierte Datei für den privaten Schlüssel ist ein fehlendes Zertifikat.

Wenn die Datei für den privaten Schlüssel falsch konfiguriert ist, führen Sie die folgenden Schritte aus, um den Fehler zu beheben.

1. Erstellen Sie ein neues Schlüsselpaar. Weitere Informationen finden Sie unter Erstellen Sie ein key pair mit Amazon EC2.

> **Note**
>
> Alternativ können Sie auch mit einem Drittanbietertool ein neues Schlüsselpaar erstellen. Weitere Informationen finden Sie unter Erstellen Sie ein key pair mit einem Drittanbieter-Tool und importieren Sie den öffentlichen Schlüssel zu Amazon EC2.

2. Fügen Sie das neue Schlüsselpaar Ihrer Instance hinzu. Weitere Informationen finden Sie unter Ich habe meinen privaten Schlüssel verloren. Wie kann ich eine Verbindung zu meiner Instance herstellen?.
3. Stellen Sie mittels des neuen Schlüsselpaars eine Verbindung mit Ihrer Instance her.

Fehler: Benutzerschlüssel wird vom Server nicht erkannt

Bei Verwendung von SSH zum Verbinden mit Ihrer Instance

- Verwenden Sie `ssh -vvv`, um beim Herstellen der Verbindung ausführliche Debugging-Informationen zu erhalten:

```
ssh -vvv -i path/key-pair-name.pem instance-user-
name@ec2-203-0-113-25.compute-1.amazonaws.com
```

Die folgende Beispielausgabe veranschaulicht, was Sie sehen, wenn Sie versuchen, eine Verbindung mit Ihrer Instance mithilfe eines Schlüssels herzustellen, der vom Server nicht erkannt wird:

```
open/ANT/myusername/.ssh/known_hosts).
debug2: bits set: 504/1024
debug1: ssh_rsa_verify: signature correct
debug2: kex_derive_keys
debug2: set_newkeys: mode 1
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug2: set_newkeys: mode 0
debug1: SSH2_MSG_NEWKEYS received
debug1: Roaming not allowed by server
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug2: service_accept: ssh-userauth
debug1: SSH2_MSG_SERVICE_ACCEPT received
```

```
debug2: key: boguspem.pem ((nil))
debug1: Authentications that can continue: publickey
debug3: start over, passed a different list publickey
debug3: preferred gssapi-keyex,gssapi-with-mic,publickey,keyboard-
interactive,password
debug3: authmethod_lookup publickey
debug3: remaining preferred: keyboard-interactive,password
debug3: authmethod_is_enabled publickey
debug1: Next authentication method: publickey
debug1: Trying private key: boguspem.pem
debug1: read PEM private key done: type RSA
debug3: sign_and_send_pubkey: RSA 9c:4c:bc:0c:d0:5c:c7:92:6c:8e:9b:16:e4:43:d8:b2
debug2: we sent a publickey packet, wait for reply
debug1: Authentications that can continue: publickey
debug2: we did not send a packet, disable method
debug1: No more authentication methods to try.
Permission denied (publickey).
```

Bei Verwendung von PuTTY zum Verbinden mit Ihrer Instance

- Überprüfen Sie, dass Ihre private Schlüsseldatei (PEM) in das Format konvertiert wurde, das von PuTTY (PPK) erkannt wird. Weitere Informationen zum Konvertieren Ihres privaten Schlüssels finden Sie unter Verbindung mit Ihrer Linux-Instance mithilfe von PuTTY.

  > **Note**
  >
  > Laden Sie Ihren privaten Schlüssel in PuTTYgen und wählen Sie Save Private Key (Privaten Schlüssel speichern) statt Generate (Generieren) aus.

- Überprüfen Sie, dass Sie eine Verbindung mit dem richtigen Benutzernamen für Ihr AMI herstellen. Geben Sie den Benutzernamen im Feld Host-Name des Fensters PuTTY-Konfiguration ein.

Zum Starten der Instance verwendetes AMI	Standardbenutzername
Amazon Linux	`ec2-user`
CentOS	`centos` oder `ec2-user`
Debian	`admin`

Zum Starten der Instance verwendetes AMI	Standardbenutzername
Fedora	`fedora` oder `ec2-user`
FreeBSD	`ec2-user`
RHEL	`ec2-user` oder `root`
SUSE	`ec2-user` oder `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Sonstige	Wenden Sie sich an den AMI-Anbieter

- Überprüfen Sie, dass eine eingehende Sicherheitsgruppenregel vorhanden ist, um den eingehenden Datenverkehr am entsprechenden Port zuzulassen. Weitere Informationen finden Sie unter Regeln für die Verbindung mit Instances von Ihrem Computer aus.

Fehler: Berechtigung verweigert oder Verbindung durch [instance] Port 22 geschlossen

Wenn Sie beim Herstellen einer Verbindung mit Ihrer Instance über SSH den Fehler `Host key not found in [directory]`, `Permission denied (publickey)`, `Authentication failed, permission denied` oder `Connection closed by [instance] port 22` erhalten, stellen Sie sicher, dass Sie die Verbindung mit dem entsprechenden Benutzernamen für Ihr AMI herstellen und dass Sie den richtigen privaten Schlüssel (`.pem`)-Datei) für Ihre Instance angegeben haben.

Die entsprechenden Benutzernamen lauten wie folgt:

Zum Starten der Instance verwendetes AMI	Standardbenutzername
Amazon Linux	`ec2-user`

Zum Starten der Instance verwendetes AMI	Standardbenutzername
CentOS	`centos` oder `ec2-user`
Debian	`admin`
Fedora	`fedora` oder `ec2-user`
FreeBSD	`ec2-user`
RHEL	`ec2-user` oder `root`
SUSE	`ec2-user` oder `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Sonstige	Wenden Sie sich an den AMI-Anbieter

Um beispielsweise einen SSH-Client für die Verbindung mit einer Amazon Linux-Instance zu verwenden, verwenden Sie den folgenden Befehl:

```
ssh -i /path/key-pair-name.pem instance-user-
name@ec2-203-0-113-25.compute-1.amazonaws.com
```

Vergewissern Sie sich, dass Sie den privaten Schlüssel verwenden, der dem Schlüsselpaar entspricht, das Sie beim Starten der Instance angegeben haben.

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie anschließend Ihre Instance aus.
3. Überprüfen Sie auf der Registerkarte Details unter Instance details (Instance-Details) den Wert des Key pair name (Schlüsselpaarnamens).
4. Wenn Sie beim Starten der Instance kein Schlüsselpaar angegeben haben, können Sie die Instance beenden und eine neue unter Angabe eines Schlüsselpaars starten. Wenn Sie diese

Instance zwar verwendet haben, aber die `.pem`-Datei für Ihr Schlüsselpaar nicht mehr vorliegt, können Sie das Schlüsselpaar durch ein neues ersetzen. Weitere Informationen finden Sie unter Ich habe meinen privaten Schlüssel verloren. Wie kann ich eine Verbindung zu meiner Instance herstellen?.

Wenn Sie ein eigenes Schlüsselpaar generiert haben, stellen Sie sicher, dass Ihr Schlüsselgenerator für das Erstellen von RSA-Schlüssel eingerichtet ist. DSA-Schlüssel werden nicht akzeptiert.

Wenn Sie einen `Permission denied (publickey)`-Fehler erhalten und keiner der oben angegebenen Fälle zutrifft (z. B. wenn Sie zuvor eine Verbindung herstellen konnten), wurden die Berechtigungen für das Stammverzeichnis Ihrer Instance möglicherweise geändert. Berechtigungen für /home/*instance-user-name*/.ssh/authorized_keys müssen auf den Eigentümer beschränkt sein.

So überprüfen Sie die Berechtigungen für Ihre Instance

1. Beenden Sie Ihre Instance und trennen Sie das Stamm-Volume von der Instance. Weitere Informationen finden Sie unter Stoppen und starten Sie EC2 Amazon-Instances.
2. Starten Sie eine temporäre Instance in derselben Availability Zone wie Ihre aktuelle Instance (verwenden Sie ein ähnliches oder dasselbe AMI wie für die aktuelle Instance) und fügen Sie der temporären Instance das Stamm-Volume an.
3. Stellen Sie eine Verbindung mit der temporären Instance her, erstellen Sie einen Mountingpunkt und mounten Sie das angefügte Volume.
4. Überprüfen Sie über die temporäre Instance die Berechtigungen des Verzeichnisses /home/*instance-user-name*/ des angefügten Volumes. Passen Sie die Berechtigungen bei Bedarf wie folgt an:

```
[ec2-user ~]$ chmod 600 mount_point/home/instance-user-name/.ssh/authorized_keys
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name/.ssh
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name
```

5. Heben Sie die Bereitstellung des Volumes auf, trennen Sie es von der temporären Instance und fügen Sie es der ursprünglichen Instance wieder an. Stellen Sie sicher, dass Sie den richtigen Gerätenamen für das Stamm-Volume verwenden; z. B, `/dev/xvda`.

6. Starten Sie Ihre Instance. Sie können die temporäre Instance beenden, wenn Sie sie nicht mehr benötigen.

Fehler: Ungeschützte private Schlüsseldatei

Ihre private Schlüsseldatei muss vor Lese- und Schreibvorgängen anderer Benutzer geschützt sein. Wenn Ihr privater Schlüssel nur von anderen, aber nicht von Ihnen gelesen oder geschrieben werden kann, ignoriert SSH Ihren Schlüssel und Sie erhalten die folgende Warnmeldung.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0777 for '.ssh/my_private_key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: .ssh/my_private_key.pem
Permission denied (publickey).
```

Wenn Sie beim Anmelden bei Ihrer Instance eine ähnliche Meldung erhalten, sehen Sie sich die erste Zeile der Fehlermeldung an, um zu überprüfen, ob Sie den richtigen öffentlichen Schlüssel für Ihre Instance verwenden. Das obige Beispiel verwendet den privaten Schlüssel `.ssh/my_private_key.pem` mit Dateiberechtigungen `0777`, die zulassen, das jeder Benutzer diese Datei lesen oder beschreiben kann. Da diese Berechtigungsebene sehr unsicher ist, wird dieser Schlüssel von SSH ignoriert.

Wenn Sie eine Verbindung über macOS oder Linux herstellen, führen Sie den folgenden Befehl aus, um diesen Fehler zu beheben, und ersetzen Sie dabei den Pfad durch Ihre private Schlüsseldatei.

```
[ec2-user ~]$ chmod 0400 .ssh/my_private_key.pem
```

Wenn Sie die Verbindung zu einer Linux-Instance von Windows aus herstellen möchten, führen Sie die folgenden Schritte auf dem lokalen Computer aus.

1. Navigieren Sie zu Ihrer PEM-Datei.
2. Klicken Sie mit der rechten Maustaste auf die PEM-Datei und wählen Sie Eigenschaften aus.
3. Wählen Sie die Registerkarte Sicherheit aus.
4. Klicken Sie auf Erweitert.

5. Stellen Sie sicher, dass Sie der Besitzer der Datei sind. Wenn nicht, ändern Sie den Besitzer in Ihren Benutzernamen.
6. Wählen Sie Vererbung deaktivieren und Alle vererbten Berechtigungen aus diesem Objekt entfernen aus.
7. Wählen Sie Hinzufügen und Prinzipal auswählen aus, geben Sie Ihren Benutzernamen ein und klicken Sie auf OK.
8. Erteilen Sie im Fenster Berechtigungseintrag die Berechtigungen zum Lesen und klicken Sie auf OK.
9. Klicken auf Apply (Anwenden), damit alle Einstellungen gespeichert werden.
10. Klicken Sie auf OK, um das Fenster Erweiterte Sicherheitseinstellungen zu schließen.
11. Klicken Sie auf OK, um das Fenster Eigenschaften zu schließen.
12. Sie sollten in der Lage sein, per SSH eine Verbindung von Windows zu Ihrer Linux-Instance herzustellen.

Führen Sie in einer Windows-Eingabeaufforderung die folgenden Befehle aus:

1. Navigieren Sie von der Eingabeaufforderung zum Dateipfad Ihrer PEM-Datei.
2. Führen Sie den folgenden Befehl aus, um explizite Berechtigungen zurückzusetzen und zu entfernen:

```
icacls.exe $path /reset
```

3. Führen Sie den folgenden Befehl aus, um dem aktuellen Benutzer Leseberechtigungen zu erteilen:

```
icacls.exe $path /GRANT:R "$($env:USERNAME):(R)"
```

4. Führen Sie den folgenden Befehl aus, um die Vererbung zu deaktivieren und geerbte Berechtigungen zu entfernen.

```
icacls.exe $path /inheritance:r
```

5. Sie sollten in der Lage sein, per SSH eine Verbindung von Windows zu Ihrer Linux-Instance herzustellen.

Fehler: Der private Schlüssel muss mit „-----BEGIN RSA PRIVATE KEY-----“ und mit „-----END RSA PRIVATE KEY-----“ enden

Wenn Sie ein Tools von Drittanbietern, wie ssh-keygen, zum Erstellen eines RSA-Schlüsselpaars verwenden, generiert es den privaten Schlüssel im Format für OpenSSH-Schlüssel. Wenn Sie eine Verbindung zu Ihrer Instance herstellen und den privaten Schlüssel im OpenSSH-Format verwenden, um das Passwort zu entschlüsseln, erhalten Sie folgenden Fehler: `Private key must begin with "-----BEGIN RSA PRIVATE KEY-----" and end with "-----END RSA PRIVATE KEY-----"`.

Der private Schlüssel muss im PEM-Format vorliegen, damit dieser Fehler nicht auftritt. Verwenden Sie folgenden Befehl, um den privaten Schlüssel im PEM-Format zu erstellen:

```
ssh-keygen -m PEM
```

Fehler: Hostschlüssel-Validierung fehlgeschlagen

Dieser Fehler tritt auf, wenn der Hostschlüssel, der auf der Instance in der `known_hosts`-Datei gespeichert ist, nicht mit dem auf dem Client gespeicherten Hostschlüssel übereinstimmt. Eine Nichtübereinstimmung kann beispielsweise auftreten, wenn Sie über eine öffentliche IP-Adresse eine Verbindung zu einer Instance herstellen und dann erneut versuchen, eine Verbindung mit einer anderen öffentlichen IP-Adresse herzustellen. Dies kann passieren, nachdem Sie eine Elastic IP-Adresse hinzugefügt oder entfernt haben, da sich dadurch die öffentliche IP-Adresse einer Instance ändert.

Um diesen Fehler zu beheben, überprüfen Sie zunächst, ob eine erwartete Änderung des Hostschlüssels oder der Netzwerkkonfiguration der Instance eingetreten ist. Bevor Sie eine Verbindung mit der Instance herstellen, sollten Sie möglicherweise auch den Host-Fingerabdruck überprüfen. Nachdem Sie eine Verbindung mit der Instance hergestellt haben, können Sie den alten Hostschlüssel aus der `known_hosts`-Datei entfernen. Anweisungen finden Sie in der Dokumentation der Linux-Distribution, die auf Ihrer Instance verwendet wird.

Fehler: Der Server lehnte unseren Schlüssel ab oder es sind keine unterstützten Authentifizierungsmethoden verfügbar.

Wenn Sie PuTTY verwenden, um sich mit Ihrer Instance zu verbinden, und eine der folgenden Fehlermeldungen erhalten, Fehler: Server hat unseren Schlüssel abgelehnt oder Fehler: Keine

unterstützten Authentifizierungsmethoden verfügbar, überprüfen Sie, ob Sie sich mit dem richtigen Benutzernamen für Ihr AMI verbinden. Geben Sie den Benutzernamen im Feld Benutzername des Fensters PuTTY-Konfiguration ein.

Die entsprechenden Benutzernamen lauten wie folgt:

Zum Starten der Instance verwendetes AMI	Standardbenutzername
Amazon Linux	`ec2-user`
CentOS	`centos` oder `ec2-user`
Debian	`admin`
Fedora	`fedora` oder `ec2-user`
FreeBSD	`ec2-user`
RHEL	`ec2-user` oder `root`
SUSE	`ec2-user` oder `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Sonstige	Wenden Sie sich an den AMI-Anbieter

Sie sollten auch Folgendes überprüfen:

- Verwenden Sie die neueste Version von PuTTY? Weitere Informationen finden Sie auf der PuTTY-Webseite.
- Ihre private Schlüsseldatei (PEM) wurde korrekt in das Format konvertiert, das von PuTTY (.ppk) erkannt wird. Weitere Informationen zum Konvertieren Ihres privaten Schlüssels finden Sie unter Verbindung mit Ihrer Linux-Instance mithilfe von PuTTY.

Die Instance ist nicht per Ping erreichbar.

Der `ping`-Befehl ist eine Art ICMP—Datenverkehr. Wenn Sie Ihre Instance per Ping nicht erreichen können, stellen Sie sicher, dass Ihre eingehenden Sicherheitsgruppenregeln ICMP-Datenverkehr für die `Echo Request`-Meldung von allen Quellen oder vom Computer bzw. von der Instance zulassen, auf dem bzw. der Sie den Befehl ausgeben.

Wenn Sie keinen `ping`-Befehl auf Ihrer Instance ausgeben können, stellen Sie sicher, dass Ihre ausgehenden Sicherheitsgruppenregeln ICMP-Datenverkehr für die `Echo Request`-Meldung an alle Ziele oder an den Host, den Sie per Ping zu erreichen versuchen, zulassen.

`Ping`-Befehle können aufgrund von Netzwerklatenz oder Hardwareproblemen auch von einer Firewall blockiert werden oder es kann zu einer Zeitüberschreitung kommen. Wenden Sie sich an Ihren lokalen Netzwerk- oder Systemadministrator, um Hilfe bei der weiteren Fehlerbehebung zu erhalten.

Fehler: Der Server hat die Netzwerkverbindung unerwartet geschlossen

Wenn Sie mit Ihrer Instance mit PuTTY verbunden sind und den Fehler "Server unexpectedly closed network connection (Der Server hat die Netzwerkverbindung unerwartet geschlossen)" erhalten, vergewissern Sie sich, dass Sie Keepalives auf der Verbindungsseite der PuTTY-Konfiguration aktiviert haben, um eine Trennung der Verbindung zu vermeiden. Einige Server trennen die Verbindung von Clients, wenn sie innerhalb des angegebenen Zeitraums keine Daten empfangen. Legen Sie als Anzahl der Sekunden zwischen Keepalives 59 Sekunden fest.

Wenn nach dem Aktivieren von Keepalives weiterhin Probleme auftreten, versuchen Sie, den Nagle-Algorithmus auf der Verbindungsseite der PuTTY-Konfiguration zu deaktivieren.

Fehler: Hostschlüssel-Validierung fehlgeschlagen für EC2 Instance Connect

Wenn Sie Ihre Instance-Hostschlüssel rotieren, werden die neuen Hostschlüssel nicht automatisch in die Datenbank mit vertrauenswürdigen Hostschlüsseln von AWS hochgeladen. Dies führt dazu, dass die Hostschlüssel-Validierung fehlschlägt, wenn Sie versuchen, eine Verbindung zu Ihrer Instance über den browserbasierten Client EC2 Instance Connect herzustellen, und Sie keine Verbindung mit Ihrer Instance herstellen können.

Um den Fehler zu beheben, müssen Sie das `eic_harvest_hostkeys`-Skript auf Ihrer Instance ausführen, das Ihren neuen Hostschlüssel in EC2 Instance Connect hochlädt. Das Skript befindet sich bei `/opt/aws/bin/` auf Amazon Linux 2-Instances und bei `/usr/share/ec2-instance-connect/` auf Ubuntu-Instances.

Amazon Linux 2

Beheben des Fehlers der Hostschlüssel-Validierung auf einer Amazon Linux 2-Instance

1. Stellen Sie per SSH eine Verbindung mit Ihrer Instance her.

   Sie können eine Verbindung herstellen, indem Sie die EC2-Instance-Connect-CLI verwenden oder das SSH-Schlüsselpaar verwenden, das beim Start Ihrer Instance dieser zugewiesen wurde, und den Standardbenutzernamen des AMI, mit dem Sie Ihre Instance gestartet haben. Bei Amazon Linux 2 ist der Standardbenutzername `ec2-user`.

   Beispiel: Wenn Ihre Instance mit Amazon Linux 2 gestartet wurde und der öffentliche DNS-Name Ihrer Instance ist `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` und das Schlüsselpaar `my_ec2_private_key.pem`, nutzen Sie den folgenden Befehl, um eine SSH-Sitzung auf Ihrer Instance zu starten:

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Verbinden mit der Linux-Instance über einen SSH-Client.
2. Navigieren Sie zum folgenden Ordner.

   ```
   [ec2-user ~]$ cd /opt/aws/bin/
   ```
3. Führen Sie den folgenden Befehl auf Ihrer Instance aus.

   ```
   [ec2-user ~]$ ./eic_harvest_hostkeys
   ```

   Beachten Sie, dass ein erfolgreicher Anruf zu keiner Ausgabe führt.

   Sie können jetzt den browserbasierten Clienten EC2 Instance Connect benutzen, um mit Ihrer Instance eine Verbindung herzustellen

Ubuntu

Beheben des Fehlers der Hostschlüssel-Validierung auf einer Ubuntu-Instance

1. Stellen Sie per SSH eine Verbindung mit Ihrer Instance her.

Sie können eine Verbindung herstellen, indem Sie die EC2-Instance-Connect-CLI verwenden oder das SSH-Schlüsselpaar verwenden, das beim Start Ihrer Instance dieser zugewiesen wurde, und den Standardbenutzernamen des AMI, mit dem Sie Ihre Instance gestartet haben. Für Ubuntu lautet der Standardbenutzername `ubuntu`.

Beispiel: Wenn Ihre Instance mit Ubuntu gestartet wurde und der öffentliche DNS-Name Ihrer Instance ist `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` und das Schlüsselpaar `my_ec2_private_key.pem`, nutzen Sie den folgenden Befehl, um eine SSH-Sitzung auf Ihrer Instance zu starten:

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Verbinden mit der Linux-Instance über einen SSH-Client.

2. Navigieren Sie zum folgenden Ordner.

```
[ec2-user ~]$ cd /usr/share/ec2-instance-connect/
```

3. Führen Sie den folgenden Befehl auf Ihrer Instance aus.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Beachten Sie, dass ein erfolgreicher Anruf zu keiner Ausgabe führt.

Sie können jetzt den browserbasierten Clienten EC2 Instance Connect benutzen, um mit Ihrer Instance eine Verbindung herzustellen

Mit EC2 Instance Connect kann keine Verbindung zur Ubuntu-Instance hergestellt werden

Wenn Sie EC2 Instance Connect verwenden, um eine Verbindung zu Ihrer Ubuntu-Instance herzustellen und beim Verbindungsversuch eine Fehlermeldung angezeigt wird, können Sie die folgenden Informationen verwenden, um das Problem zu beheben.

Mögliche Ursache

Das `ec2-instance-connect`-Paket auf der Instance ist nicht die neueste Version.

Lösung

Aktualisieren Sie das `ec2-instance-connect`-Paket auf der Instance wie folgt auf die neueste Version:

1. Stellen Sie eine Verbindung mit einer anderen Methode als EC2 Instance Connect mit Ihrer Instance her.
2. Führen Sie den folgenden Befehl auf Ihrer Instance aus, um das `ec2-instance-connect`-Paket auf die neueste Version zu aktualisieren.

```
apt update && apt upgrade
```

Ich habe meinen privaten Schlüssel verloren. Wie kann ich eine Verbindung zu meiner Instance herstellen?

Falls Sie den privaten Schlüssel für eine per EBS abgesicherte Instance verlieren, können Sie den Zugriff auf Ihre Instance zurückerlangen. Sie müssen die Instance anhalten, das Stamm-Volume trennen, es einer anderen Instance als Daten-Volume anfügen, die Datei `authorized_keys` mit einem neuen öffentlichen Schlüssel modifizieren, das Volume zurück zur ursprünglichen Instance verschieben und die Instance neu starten. Weitere Informationen zum Starten, Herstellen von Verbindungen und Anhalten von Instances finden Sie im Abschnitt Amazon-EC2-Instance-Statusänderungen.

Dieses Verfahren wird nur für Instance mit EBS-Stamm-Volumes unterstützt. Wenn die Instance ein Instance-Speicher-Root-Volume hat, können Sie dieses Verfahren nicht verwenden, um den Zugriff auf Ihre Instance wiederherzustellen. Sie benötigen den privaten Schlüssel, um eine Verbindung mit der Instance herzustellen. Um den Root-Volume-Typ Ihrer Instance zu ermitteln, öffnen Sie die Amazon-EC2-Konsole, wählen Sie Instances, wählen Sie die Instance aus, wählen Sie die Registerkarte Speicher und überprüfen Sie im Abschnitt Root-Gerätedetails den Wert des Root-Gerätetyps.

Der Wert ist entweder `EBS` oder `INSTANCE-STORE`.

Wenn Sie Ihren privaten Schlüssel verlieren, gibt es weitere Möglichkeiten, eine Verbindung mit Ihrer Linux-Instance herzustellen. Weitere Informationen finden Sie unter Wie kann ich eine Verbindung zu

meiner Amazon EC2 Instance herstellen, wenn ich mein SSH-Schlüsselpaar nach dem ersten Start verloren habe?

Schritte für die Herstellung einer Verbindung zu einer EBS-gestützten Instance mittels eines anderen Schlüsselpaars

- Schritt 1: Erstellen eines neuen Schlüsselpaars
- Schritt 2: Abrufen von Informationen über die ursprüngliche Instance und ihr Stamm-Volume
- Schritt 3: Anhalten der ursprünglichen Instance
- Schritt 4: Starten einer temporären Instance
- Schritt 5: Trennen des Stamm-Volumes von der ursprünglichen Instance und Anfügen an die temporäre Instance
- Schritt 6: Hinzufügen des neuen öffentlichen Schlüssels zu authorized_keys auf dem ursprünglichen Volume, das auf der temporären Instance gemountet wird
- Schritt 7: Aufheben der Bereitstellung und Trennen des ursprünglichen Volumes von der temporären Instance und erneutes Anfügen an die ursprüngliche Instance
- Schritt 8: Verbinden Sie sich mit der ursprünglichen Instance mit dem neuen Schlüsselpaar
- Schritt 9: Bereinigen

Schritt 1: Erstellen eines neuen Schlüsselpaars

Erstellen Sie ein neues Schlüsselpaar mit der Amazon EC2-Konsole oder einem Tool eines Drittanbieters. Falls der Name des neuen Schlüsselpaares dem des verlorenen privaten Schlüssels genau entsprechen soll, müssen Sie das vorhandene Schlüsselpaar erst löschen. Weitere Informationen zum Erstellen eines neuen Schlüsselpaars finden Sie unter Erstellen Sie ein key pair mit Amazon EC2 oder Erstellen Sie ein key pair mit einem Drittanbieter-Tool und importieren Sie den öffentlichen Schlüssel zu Amazon EC2.

Schritt 2: Abrufen von Informationen über die ursprüngliche Instance und ihr Stamm-Volume

Notieren Sie sich die folgenden Informationen, da Sie sie benötigen werden, um dieses Verfahren abzuschließen.

So erhalten Sie Informationen zu Ihrer ursprünglichen Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Instances und dann die Instance aus, zu der Sie eine Verbindung herstellen möchten. (Wir bezeichnen diese als ursprüngliche Instance.)
3. Notieren Sie sich auf der Registerkarte Details die Instance-ID und die AMI-ID.
4. Notieren Sie sich auf der Registerkarte Network (Netzwerk) die Availability Zone.
5. Notieren Sie sich auf der Registerkarte Storage (Speicher) den Gerätenamen für das Root-Volume unter Root device name (Root-Gerätename) (z. B. `/dev/xvda`). Suchen Sie diesen Gerätenamen unter Block devices (Geräte blockieren) und notieren Sie sich die Volume-ID (z. B. vol-0a1234b5678c910de).

Schritt 3: Anhalten der ursprünglichen Instance

Wählen Sie Instance state (Instance-Status), Stop instance (Instance anhalten). Wenn diese Option deaktiviert ist, wurde die Instance entweder bereits angehalten oder das Root-Volume ist ein Instance-Speicher-Volume.

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

Schritt 4: Starten einer temporären Instance

So starten Sie eine temporäre Instance

1. Wählen Sie im Navigationsbereich Instances und Launch instances (Instances starten) aus.
2. Im Abschnitt Name and tags (Name und Tags) geben Sie beiName Temporary (Temporär) ein.
3. Im Abschnitt Application and OS Images (Anwendungs- und Betriebssystem-Images) wählen Sie dasselbe AMI aus, das Sie beim Start der ursprünglichen Instance verwendet haben. Falls diese AMI nicht verfügbar ist, können Sie eine AMI erstellen, die Sie von der angehaltenen Instance verwenden können. Weitere Informationen finden Sie unter Ein Amazon-EBS-gestütztes AMI erstellen.
4. Behalten Sie im Abschnitt Instance type (Instance-Typ) den standardmäßigen Instance-Typ bei.
5. Im Abschnitt Key pair (Schlüsselpaar) unter Key pair name (Schlüsselpaarname) wählen Sie das vorhandene Schlüsselpaar aus, das Sie verwenden oder erstellen Sie ein neues.

6. Im Abschnitt Network settings (Netzwerkeinstellungen) wählen Sie Edit (Bearbeiten), aus. Wählen Sie dann unter Subnet (Subnetz) ein Subnetz in derselben Availability Zone wie die ursprüngliche Instance aus.
7. Wählen Sie im Bereich Summary (Übersicht) Launch (Starten) aus.

Schritt 5: Trennen des Stamm-Volumes von der ursprünglichen Instance und Anfügen an die temporäre Instance

1. Wählen Sie im Navigationsbereich Volumes und wählen Sie das Root-Volume für die ursprüngliche Instance aus (Sie haben die Volume-ID in einem früheren Schritt notiert). Wählen Sie Actions (Aktionen) und danach Detach volume (Volume trennen) aus, gefolgt von Detach (Trennen). Warten Sie, bis der Status des Volumes wir `available`. (Sie müssen möglicherweise das Symbol Refresh (Aktualisieren) wählen.)
2. Wählen Sie bei ausgewähltem Volume Actions (Aktionen) und wählen Sie dann Attach Volume (Volume anfügen) aus. Wählen Sie die Instance-ID der vorübergehenden Instance aus, notieren Sie den Gerätenamen unter Device name (Gerätenamen) (zum Beispiel `/dev/sdf`) und wählen Sie dann Attach volume (Volume anhängen) aus.

> **Note**
>
> Falls Sie Ihre ursprüngliche Instance über eine AWS Marketplace-AMI gestartet haben und Ihr Volume AWS Marketplace-Codes enthält, müssen Sie zuerst die temporäre Instance anhalten, bevor Sie das Volume anfügen können.

Schritt 6: Hinzufügen des neuen öffentlichen Schlüssels zu **`authorized_keys`** auf dem ursprünglichen Volume, das auf der temporären Instance gemountet wird

1. Stellen Sie eine Verbindung mit der temporären Instance her.
2. Mounten Sie in der temporären Instance das Volume, das Sie an die Instance angefügt haben, damit Sie auf ihr Dateisystem zugreifen können. Beispiel: Falls der Gerätename `/dev/sdf` lautet, verwenden Sie die folgenden Befehle zum Mounten des Volume als `/mnt/tempvol`.

> **Note**
>
> Der Gerätename wird auf Ihrer Instance möglicherweise anders angezeigt. Beispiel: Geräte, die als `/dev/sdf` gemountet wurden, werden auf der Instance möglicherweise als `/dev/xvdf` angezeigt. Einige Versionen von Red Hat (oder Varianten wie CentOS) können den letzten Buchstaben möglicherweise noch um 4 Zeichen erhöhen, wobei `/dev/sdf` zu `/dev/xvdk` wird.

a. Verwenden Sie den Befehl lsblk, um zu ermitteln, ob das Volume partitioniert ist.

```
[ec2-user ~]$ lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda    202:0    0    8G  0 disk
##xvda1 202:1    0    8G  0 part /
xvdf    202:80   0  101G  0 disk
##xvdf1 202:81   0  101G  0 part
xvdg    202:96   0   30G  0 disk
```

Im Beispiel oben sind `/dev/xvda` und `/dev/xvdf` partitionierte Volumes und `/dev/xvdg` nicht. Falls Ihr Volume partitioniert ist, mounten Sie die Partition (`/dev/xvdf1`) anstelle des Rohdatenträgers (`/dev/xvdf`) in den nächsten Schritten.

b. Erstellen Sie ein temporäres Verzeichnis zum Mounten des Volumes.

```
[ec2-user ~]$ sudo mkdir /mnt/tempvol
```

c. Mounten Sie das Volume (oder die Partitionierung) am temporären Mount-Punkt mithilfe des Volume-Namens oder des Gerätenamens, den Sie vorher in Erfahrung gebracht haben. Der erforderliche Befehl hängt vom Dateisystem Ihres Betriebssystems ab. Beachten Sie, dass der Gerätename auf Ihrer Instance möglicherweise anders angezeigt wird. Weitere Informationen finden Sie in note in Schritt 6.

- Amazon Linux, Ubuntu und Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2, CentOS, SUSE Linux 12 und RHEL 7.x

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

> **Note**
>
> Wenn Sie einen Fehler erhalten, der besagt, dass das Dateisystem beschädigt ist, führen Sie den folgenden Befehl aus, um mit dem Dienstprogramm fsck das Dateisystem zu prüfen und mögliche Probleme zu beheben:
>
> ```
> [ec2-user ~]$ sudo fsck /dev/xvdf1
> ```

3. Verwenden Sie in der temporären Instance den folgenden Befehl, um `authorized_keys` mit dem neuen öffentlichen Schlüssel über `authorized_keys` für die temporäre Instance am gemounteten Volume zu aktualisieren.

> **Important**
>
> Die folgenden Beispiele verwenden den Amazon-Linux-Benutzernamen `ec2-user`. Sie können ihn durch einen anderen Benutzernamen ersetzen, wie etwa `ubuntu` für Ubuntu-Instances.

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Falls diese Kopie erfolgreich verlief, können Sie mit dem nächsten Schritt fortfahren.

(Optional) Falls Sie keine Berechtigung zum Bearbeiten von Dateien in `/mnt/tempvol` besitzen, müssen Sie die Datei mithilfe von sudo aktualisieren und dann die Berechtigungen für die Datei überprüfen, um zu gewährleisten, dass Sie sich an der ursprünglichen Instance anmelden können. Führen Sie den folgenden Befehl aus, um die Berechtigungen für die Datei zu prüfen.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
total 4
-rw------- 1 222 500 398 Sep 13 22:54 authorized_keys
```

In dieser Beispielausgabe lautet die Benutzer-ID *222* und die Gruppen-ID *500*. Verwenden Sie als Nächstes sudo, um den fehlgeschlagenen Kopierbefehl erneut auszuführen.

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Führen Sie den folgenden Befehl noch einmal aus, um zu ermitteln, ob sich die Berechtigungen geändert haben.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

Falls sich die Benutzer-ID und die Gruppen-ID geändert haben, verwenden Sie den folgenden Befehl, um sie wiederherzustellen.

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

Schritt 7: Aufheben der Bereitstellung und Trennen des ursprünglichen Volumes von der temporären Instance und erneutes Anfügen an die ursprüngliche Instance

1. Entfernen Sie in der temporären Instance das Volume, das Sie angefügt haben, damit Sie es wieder an der ursprünglichen Instance anhängen können. Verwenden Sie beispielsweise den folgenden Befehl, um die Bereitstellung des Volumes unter aufzuhebe `/mnt/tempvol`.

   ```
   [ec2-user ~]$ sudo umount /mnt/tempvol
   ```

2. Trennen Sie das Volume von der temporären Instance (Sie haben das Mounting der Bereitstellung im vorherigen Schritt aufgehoben): Wählen Sie in der Amazon-EC2-Konsole im Navigationsbereich Volumes, wählen sie das Root-Volume für die ursprüngliche Instance (Sie haben die Volume-ID in einem vorherigen Schritt notiert) wählen Sie Aktionen, Volume trennen und dann Trennen aus. Warten Sie, bis der Status des Volumes wir `available`. (Sie müssen möglicherweise das Symbol Refresh (Aktualisieren) wählen.)
3. Erneutes Anfügen des Volume an die ursprüngliche Instance: Wählen Sie bei weiter ausgewähltem Volume Actions (Aktionen) die Option Attach Volume (Volume anfügen) aus. Wählen Sie die Instance-ID der ursprünglichen Instance aus, geben Sie den Gerätenamen an, den Sie zuvor in Schritt 2 für den ursprünglichen Root-Volume-Anhang (`/dev/sda1` oder `/dev/xvda`) notiert haben, und wählen Sie dann Volume anhängen aus.

> **Important**
>
> Falls Sie nicht denselben Gerätenamen als ursprünglichen Anhang angeben, können Sie die ursprüngliche Instance nicht starten. Amazon EC2 erwartet das Root-Volume unter `sda1` oder `/dev/xvda`.

Schritt 8: Verbinden Sie sich mit der ursprünglichen Instance mit dem neuen Schlüsselpaar

Wählen Sie die ursprüngliche Instance und dann Instance state (Instance-Status), Start instance (Instance starten). Wenn die Instance den Status `running` erhält, können Sie mit der Datei mit dem privaten Schlüssel für Ihr neues Schlüsselpaar eine Verbindung zu ihr herstellen.

> **Note**
>
> Falls sich der Name Ihres neuen Schlüsselpaars und der entsprechenden Datei mit dem privaten Schlüssel vom Namen des ursprünglichen Schlüsselpaars unterscheidet, müssen Sie den Namen der Datei mit dem neuen privaten Schlüssel angeben, wenn Sie eine Verbindung mit Ihrer Instance herstellen.

Schritt 9: Bereinigen

(Optional) Sie können die temporäre Instance beenden, falls Sie keine weitere Verwendung mehr dafür haben. Wählen Sie die temporäre Instance und dann Instance-Status, Instance beenden (löschen) aus.

Problembehandlung bei Amazon EC2 Linux-Instances mit fehlgeschlagenen Statusprüfungen

Die folgenden Informationen können Ihnen helfen, Probleme zu beheben, wenn Ihre Linux-Instance eine Statusprüfung nicht besteht. Stellen Sie zunächst fest, ob in Ihren Anwendungen Probleme bestehen. Wenn Sie feststellen, dass die Instance Ihre Anwendung nicht erwartungsgemäß ausführt, gehen Sie die Informationen der Statusprüfung und die Systemprotokolle durch.

Beispiele für Probleme, die dazu führen können, dass Statusprüfungen fehlschlagen, finden Sie unter Statuschecks für EC2 Amazon-Instances.

Inhalt

- Informationen der Statusprüfung durchgehen
- Systemprotokolle abrufen
- Fehlerbehebung bei Systemprotokollfehlern für Linux-Instances
- Out of memory: kill process
- ERROR: mmu_update failed (Fehler beim Aktualisieren der Speicherverwaltung)
- I/O-Fehler (Blockgerätfehler)
- I/O ERROR: neither local nor remote disk (defektes verteiltes Blockgerät)
- request_module: runaway loop modprobe (Endlosschleife des modprobe-Programms auf Legacy-Kerneln älterer Linux-Versionen)
- "FATAL: kernel too old" und "fsck: No such file or directory while trying to open /dev" (fehlende Übereinstimmung zwischen Kernel und AMI)
- „SCHWERWIEGEND: /lib/modules" oder "BusyBox" (Fehlende Kernelmodule) konnten nicht geladen werden
- FEHLER Ungültiger Kernel (inkompatibler Kernel) EC2
- fsck: No such file or directory while trying to open... (Dateisystem nicht gefunden)
- Allgemeiner Fehler beim Mounten von Dateisystemen (Mountfehler)
- VFS: Unable to mount root fs on unknown-block (fehlende Übereinstimmung des Stammdateisystems)
- Fehler: Die major/minor Anzahl der Root-Geräte konnte nicht ermittelt werden... (Root-Datei system/device stimmt nicht überein)
- XENBUS: Device with no driver...
- ... days without being checked, check forced (Dateisystemprüfung erforderlich)
- fsck died with exit status... (fehlendes Gerät)
- GRUB prompt (grubdom>)
- Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring. (hartcodierte MAC-Adresse)
- Die Richtlinie konnte nicht geladen werden SELinux . Machine is in enforcing mode. Wird jetzt angehalten. (SELinux Fehlkonfiguration)

- XENBUS: Timeout connecting to devices (Xenbus-Timeout)

Informationen der Statusprüfung durchgehen

Um beeinträchtigte Instances mithilfe der EC2 Amazon-Konsole zu untersuchen

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie anschließend Ihre Instance aus.
3. Wählen Sie die Registerkarte Status und Alarme, um die einzelnen Ergebnisse aller Systemstatusprüfungen, Instance-Statusprüfungen und der Statusprüfungen für angefügte EBS anzuzeigen.

Wenn eine Statusprüfung fehlgeschlagen ist, können Sie eine der folgenden Optionen verwenden:

- Erstellen Sie einen Alarm, um die Instance als Reaktion auf die fehlgeschlagene Statusprüfung wiederherzustellen. Weitere Informationen finden Sie unter Erstellen von Alarmen, mit denen eine Instance angehalten, beendet, neu gestartet oder wiederhergestellt wird.
- (Instance-Statusprüfungen) Wenn Sie den Instance-Typ in eine Nitro-basierte Instance geändert haben, schlagen die Statusprüfungen fehl, wenn Sie von einer Instance migriert haben, die nicht über die erforderliche ENA und NVMe Treiber verfügt. Weitere Informationen finden Sie unter Kompatibilität zum Ändern des Instance-Typs.
- Bei einer Instance mit einem EBS-Root-Volume halten Sie die Instance an und starten Sie sie erneut. Weitere Informationen finden Sie unter Stoppen und starten Sie EC2 Amazon-Instances.
- Bei einer Instance mit Instance-Speicher-Root-Volume beenden Sie die Instance und starten Sie eine Ersatz-Instance. Weitere Informationen finden Sie unter EC2 Amazon-Instances beenden.
- Warten Sie EC2 , bis Amazon das Problem gelöst hat.
- Wenden Sie sich an AWS re:POST Support oder posten Sie Ihr Problem.
- Wenn sich Ihre Instance in einer Amazon EC2 Auto Scaling Scaling-Gruppe befindet:
  - (Systemstatusprüfungen und Instance-Statusprüfungen) Standardmäßig startet Amazon EC2 Auto Scaling automatisch eine Ersatz-Instance. Weitere Informationen finden Sie unter Zustandsprüfungen für Instances in einer Amazon EC2 Auto Scaling Scaling-Gruppe im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.
  - (Beigefügte EBS-Statusprüfungen) Sie müssen Amazon EC2 Auto Scaling so konfigurieren, dass automatisch eine Ersatz-Instance gestartet wird. Weitere Informationen finden Sie unter

Überwachen und Ersetzen von Amazon EC2 Auto Scaling Scaling-Instances mit beeinträchtigten Amazon EBS-Volumes im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

- Rufen Sie das Systemprotokoll ab und prüfen Sie es auf Fehler. Weitere Informationen finden Sie unter Systemprotokolle abrufen.

Systemprotokolle abrufen

Wenn eine Instance-Statusprüfung fehlschlägt, können Sie die Instance neu starten und die Systemprotokolle abrufen. Die Protokolle geben Aufschluss, ob ein Fehler vorliegt, was Ihnen bei der Problembehebung helfen kann. Durch den Neustart werden nicht benötigte Informationen in den Protokollen gelöscht.

So starten Sie eine Instance neu und rufen das Systemprotokoll ab

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie Ihre Instance aus.
3. Wählen Sie Instance state (Instance-Status), Reboot instance (Instance neu starten). Es kann einige Minuten dauern, bis Ihre Instance neu gestartet wird.
4. Überprüfen Sie, ob das Problem nach wie vor besteht. In einigen Fällen lässt sich das Problem durch den Neustart lösen.
5. Wenn die Instance im `running`-Status ist, wählen Sie Actions (Aktionen), Monitor and Troubleshoot (Überwachung und Fehlerbehebung), Get system log (Systemprotokoll abrufen).
6. Sehen Sie sich das Protokoll an, das auf dem Bildschirm angezeigt wird, und greifen Sie zur Problembehebung auf die Liste der bekannten Systemprotokoll-Fehlermeldungen zurück.
7. Wenn Ihr Problem nicht behoben ist, posten Sie es auf AWS re:Post.

Fehlerbehebung bei Systemprotokollfehlern für Linux-Instances

Überprüfen Sie bei Linux-Instances, die eine Instance-Statusprüfung wie die Instance-Erreichbarkeitsprüfung nicht bestanden haben, dass Sie die oben angegebenen Schritte zum Aufrufen des Systemprotokolls ausgeführt haben. Die folgende Liste enthält einige allgemeine Systemprotokollfehler und Vorschläge für Aktionen, die Sie ausführen können, um den jeweiligen Fehler zu beheben.

Memory Errors

- Out of memory: kill process
- ERROR: mmu_update failed (Fehler beim Aktualisieren der Speicherverwaltung)

Device Errors

- I/O-Fehler (Blockgerätfehler)
- I/O ERROR: neither local nor remote disk (defektes verteiltes Blockgerät)

Kernel Errors

- request_module: runaway loop modprobe (Endlosschleife des modprobe-Programms auf Legacy-Kerneln älterer Linux-Versionen)
- "FATAL: kernel too old" und "fsck: No such file or directory while trying to open /dev" (fehlende Übereinstimmung zwischen Kernel und AMI)
- „SCHWERWIEGEND: /lib/modules" oder "BusyBox" (Fehlende Kernelmodule) konnten nicht geladen werden
- FEHLER Ungültiger Kernel (inkompatibler Kernel) EC2

File System Errors

- fsck: No such file or directory while trying to open... (Dateisystem nicht gefunden)
- Allgemeiner Fehler beim Mounten von Dateisystemen (Mountfehler)
- VFS: Unable to mount root fs on unknown-block (fehlende Übereinstimmung des Stammdateisystems)
- Fehler: Die major/minor Anzahl der Root-Geräte konnte nicht ermittelt werden... (Root-Datei system/device stimmt nicht überein)
- XENBUS: Device with no driver...
- ... days without being checked, check forced (Dateisystemprüfung erforderlich)
- fsck died with exit status... (fehlendes Gerät)

Operating System Errors

- GRUB prompt (grubdom>)

- Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring. (hartcodierte MAC-Adresse)
- Die Richtlinie konnte nicht geladen werden SELinux . Machine is in enforcing mode. Wird jetzt angehalten. (SELinux Fehlkonfiguration)
- XENBUS: Timeout connecting to devices (Xenbus-Timeout)

Out of memory: kill process

Ein out-of-memory Fehler wird durch einen Systemprotokolleintrag angezeigt, der dem unten abgebildeten ähnelt.

```
[115879.769795] Out of memory: kill process 20273 (httpd) score 1285879
or a child
[115879.769795] Killed process 1917 (php-cgi) vsz:467184kB, anon-
rss:101196kB, file-rss:204kB
```

Mögliche Ursache

Unzureichender Speicher

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie eine der folgenden Aufgaben aus: • Halten Sie die Instance an und ändern Sie sie in einen anderen Instance-Typ. Starten Sie die Instance dann erneut. Verwenden Sie z. B. einen größeren oder speicheroptimierte n Instance-Typ. • Starten Sie die Instance neu, um sie in einen nicht eingeschränkten Status zu versetzen. Das Problem tritt wahrscheinlich erneut auf, wenn Sie den Instance-Typ nicht ändern.
Instance Store-Backup	Führen Sie eine der folgenden Aufgaben aus:

Für diesen Instance-Typ	Vorgehensweise
	• Beenden Sie die Instance und starten Sie eine neue Instance unter Angabe eines anderen Instance-Typs. Verwenden Sie z. B. einen größeren oder speicheroptimierten Instance-Typ. • Starten Sie die Instance neu, um sie in einen nicht eingeschränkten Status zu versetzen. Das Problem tritt wahrscheinlich erneut auf, wenn Sie den Instance-Typ nicht ändern.

ERROR: mmu_update failed (Fehler beim Aktualisieren der Speicherverwaltung)

Update-Fehler bei der Speicherverwaltung werden von einem Systemprotokolleintrag ähnlich wie unten dargestellt angegeben:

```
...
Press `ESC' to enter the menu... 0   [H[J  Booting 'Amazon Linux 2011.09
 (2.6.35.14-95.38.amzn1.i686)'


root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /boot/vmlinuz-2.6.35.14-95.38.amzn1.i686 root=LABEL=/ console=hvc0 LANG=

en_US.UTF-8 KEYTABLE=us

initrd /boot/initramfs-2.6.35.14-95.38.amzn1.i686.img

ERROR: mmu_update failed with rc=-22
```

Mögliche Ursache

Problem mit Amazon Linux

Vorgeschlagene Aktion

Posten Sie Ihr Problem auf AWS re:Post oder kontaktieren Sie Support.

I/O-Fehler (Blockgerätfehler)

Ein input/output Fehler wird durch einen Systemprotokolleintrag angezeigt, der dem folgenden Beispiel ähnelt:

```
[9943662.053217] end_request: I/O error, dev sde, sector 52428288
[9943664.191262] end_request: I/O error, dev sde, sector 52428168
[9943664.191285] Buffer I/O error on device md0, logical block 209713024
[9943664.191297] Buffer I/O error on device md0, logical block 209713025
[9943664.191304] Buffer I/O error on device md0, logical block 209713026
[9943664.191310] Buffer I/O error on device md0, logical block 209713027
[9943664.191317] Buffer I/O error on device md0, logical block 209713028
[9943664.191324] Buffer I/O error on device md0, logical block 209713029
[9943664.191332] Buffer I/O error on device md0, logical block 209713030
[9943664.191339] Buffer I/O error on device md0, logical block 209713031
[9943664.191581] end_request: I/O error, dev sde, sector 52428280
[9943664.191590] Buffer I/O error on device md0, logical block 209713136
[9943664.191597] Buffer I/O error on device md0, logical block 209713137
[9943664.191767] end_request: I/O error, dev sde, sector 52428288
[9943664.191970] end_request: I/O error, dev sde, sector 52428288
[9943664.192143] end_request: I/O error, dev sde, sector 52428288
[9943664.192949] end_request: I/O error, dev sde, sector 52428288
[9943664.193112] end_request: I/O error, dev sde, sector 52428288
[9943664.193266] end_request: I/O error, dev sde, sector 52428288
...
```

Mögliche Ursachen

Instance-Typ	Mögliche Ursache
Amazon EBS-gestützt	Ein ausgefallenes Amazon EBS-Volume
Instance Store-Backup	Ein ausgefallenes physisches Laufwerk

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Halten Sie die Instance an. 2. Trennen Sie das Volume ab. 3. Versuchen Sie, das Volume wiederher zustellen. **Note** Es hat sich bewährt, häufig Snapshots von Amazon EBS-Volum es zu erstellen. Dadurch wird das Risiko von Datenverlusten aufgrund eines Ausfalls erheblich gesenkt. 4. Fügen Sie das Volume der Instance wieder an. 5. Starten Sie die Instance.
Instance Store-Backup	Beenden Sie die Instance und starten Sie eine neue Instance. **Note** Die Daten können nicht wiederher gestellt werden. Führen Sie eine Wiederherstellung anhand von Datensicherungen durch.

Für diesen Instance-Typ	Vorgehensweise
	Note Es hat sich bewährt, entweder Amazon S3 oder Amazon EBS für Datensich erungen zu verwenden. Ausfälle von einzelnen Hosts und Datenträg ern wirken sich direkt auf Instance-Speicher-Volumes aus.

I/O ERROR: neither local nor remote disk (defektes verteiltes Blockgerät)

Ein input/output Fehler auf dem Gerät wird durch einen Systemprotokolleintrag angezeigt, der dem folgenden Beispiel ähnelt:

```
...
block drbd1: Local IO failed in request_timer_fn. Detaching...

Aborting journal on device drbd1-8.

block drbd1: IO ERROR: neither local nor remote disk

Buffer I/O error on device drbd1, logical block 557056

lost page write due to I/O error on drbd1

JBD2: I/O error detected when updating journal superblock for drbd1-8.
```

Mögliche Ursachen

Instance-Typ	Mögliche Ursache
Amazon EBS-gestützt	Ein ausgefallenes Amazon EBS-Volume
Instance Store-Backup	Ein ausgefallenes physisches Laufwerk

Vorgeschlagene Aktion

Beenden Sie die Instance und starten Sie eine neue Instance.

Bei einer Amazon EBS-gestützten Instance können Sie Daten anhand eines aktuellen Snapshots wiederherstellen, indem Sie ein Image davon erstellen. Alle Daten, die nach dem Snapshot hinzugefügt wurden, können nicht wiederhergestellt werden.

request_module: runaway loop modprobe (Endlosschleife des modprobe-Programms auf Legacy-Kerneln älterer Linux-Versionen)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben. Die Verwendung eines instabilen oder alten Linux-Kernels (z. B. 2.6.16-xenU) kann beim Startup eine Endlosschleife verursachen.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007

BIOS-provided physical RAM map:

 Xen: 0000000000000000 - 0000000026700000 (usable)

0MB HIGHMEM available.
...

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c
```

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Verwenden Sie einen neueren Kernel, entweder GRUB-basiert oder statisch, indem Sie eine der folgenden Optionen auswählen: Option 1: Beenden Sie die Instance und starten Sie eine neue Instance unter Angabe der Parameter `-kernel` und `-ramdisk`. Option 2: 1. Halten Sie die Instance an. 2. Ändern Sie die Attribute "kernel" und "ramdisk" und legen Sie sie auf einen neueren Kernel fest. 3. Starten Sie die Instance.
Instance Store-Backup	Beenden Sie die Instance und starten Sie eine neue Instance unter Angabe der Parameter `-kernel` und `-ramdisk`.

"FATAL: kernel too old" und "fsck: No such file or directory while trying to open /dev" (fehlende Übereinstimmung zwischen Kernel und AMI)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
Linux version 2.6.16.33-xenU (root@dom0-0-50-45-1-a4-ee.z-2.aes0.internal)
(gcc version 4.1.1 20070105 (Red Hat 4.1.1-52)) #2 SMP Wed Aug 15 17:27:36 SAST 2007
...
FATAL: kernel too old
Kernel panic - not syncing: Attempted to kill init!
```

Mögliche Ursachen

Kernel und Land des Benutzers sind nicht kompatibel.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Halten Sie die Instance an. 2. Ändern Sie die Konfiguration zur Verwendung eines neueren Kernels. 3. Starten Sie die Instance.
Instance Store-Backup	Führen Sie die folgenden Schritte aus: 1. Erstellen Sie ein AMI, das einen neueren Kernel verwendet. 2. Beenden Sie die Instance. 3. Starten Sie eine neue Instance mit dem AMI, das Sie erstellt haben.

„SCHWERWIEGEND: /lib/modules" oder "BusyBox" (Fehlende Kernelmodule) konnten nicht geladen werden

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
[    0.370415] Freeing unused kernel memory: 1716k freed
Loading, please wait...
WARNING: Couldn't open directory /lib/modules/2.6.34-4-virtual: No such file or
 directory
FATAL: Could not open /lib/modules/2.6.34-4-virtual/modules.dep.temp for writing: No
 such file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
Couldn't get a file descriptor referring to the console
Begin: Loading essential drivers... ...
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
```

```
Done.
Begin: Running /scripts/init-premount ...
Done.
Begin: Mounting root file system... ...
Begin: Running /scripts/local-top ...
Done.
Begin: Waiting for root file system... ...
Done.
Gave up waiting for root device.  Common problems:
 - Boot args (cat /proc/cmdline)
   - Check rootdelay= (did the system wait long enough?)
   - Check root= (did the system wait for the right device?)
 - Missing modules (cat /proc/modules; ls /dev)
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
ALERT! /dev/sda1 does not exist. Dropping to a shell!


BusyBox v1.13.3 (Ubuntu 1:1.13.3-1ubuntu5) built-in shell (ash)
Enter 'help' for a list of built-in commands.

(initramfs)
```

Mögliche Ursachen

Dieses Problem kann durch einen oder mehrere der folgenden Zustände verursacht werden:

- Fehlende Ramdisk
- Fehlende korrekte Module von der Ramdisk
- Amazon EBS-Stamm-Volume nicht korrekt als angefüg `/dev/sda1`

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Wählen Sie die korrigierte Ramdisk für das Amazon EBS-Volume aus.

Für diesen Instance-Typ	Vorgehensweise
	2. Halten Sie die Instance an. 3. Trennen Sie das Volume und reparieren Sie es. 4. Fügen Sie das Volume der Instance an. 5. Starten Sie die Instance. 6. Ändern Sie das AMI so, dass die korrigierte Ramdisk verwendet wird.
Instance Store-Backup	Führen Sie die folgenden Schritte aus: 1. Beenden Sie die Instance und starten Sie eine neue Instance mit der korrekten Ramdisk. 2. Erstellen Sie ein neues AMI mit der korrekten Ramdisk.

FEHLER Ungültiger Kernel (inkompatibler Kernel) EC2

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
...
root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz root=/dev/sda1 ro

initrd /initrd.img

ERROR Invalid kernel: elf_xen_note_check: ERROR: Will only load images
built for the generic loader or Linux images
xc_dom_parse_image returned -1

Error 9: Unknown boot failure

  Booting 'Fallback'
```

```
root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz.old root=/dev/sda1 ro

Error 15: File not found
```

Mögliche Ursachen

Dieses Problem kann durch einen oder beide der folgenden Zustände verursacht werden:

- Der bereitgestellte Kernel wird von GRUB nicht unterstützt.
- Der Fallback-Kernel ist nicht vorhanden.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Halten Sie die Instance an. 2. Tauschen Sie sie durch einen funktioni erenden Kernel aus. 3. Installieren Sie einen Fallback-Kernel. 4. Ändern Sie das AMI, indem Sie den Kernel korrigieren.
Instance Store-Backup	Führen Sie die folgenden Schritte aus: 1. Beenden Sie die Instance und starten Sie eine neue Instance mit dem korrekten Kernel. 2. Erstellen Sie ein AMI mit dem korrekten Kernel.

Für diesen Instance-Typ	Vorgehensweise
	3. (Optional) Wenden Sie sich an den , um technische Unterstützung zur Datenwied erherstellung zu erhalten Support.

fsck: No such file or directory while trying to open... (Dateisystem nicht gefunden)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
  Welcome to Fedora
  Press 'I' to enter interactive startup.
Setting clock : Wed Oct 26 05:52:05 EDT 2011 [  OK  ]

Starting udev: [  OK  ]

Setting hostname localhost:  [  OK  ]

No devices found
Setting up Logical Volume Management: File descriptor 7 left open
  No volume groups found
[  OK  ]

Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1: clean, 82081/1310720 files, 2141116/2621440 blocks
[/sbin/fsck.ext3 (1) -- /mnt/dbbackups] fsck.ext3 -a /dev/sdh
fsck.ext3: No such file or directory while trying to open /dev/sdh

/dev/sdh:
The superblock could not be read or does not describe a correct ext2
filesystem.  If the device is valid and it really contains an ext2
filesystem (and not swap or ufs or something else), then the superblock
is corrupt, and you might try running e2fsck with an alternate superblock:
    e2fsck -b 8193 <device>

[FAILED]
```

```
*** An error occurred during the file system check.
*** Dropping you to a shell; the system will reboot
*** when you leave the shell.
Give root password for maintenance
(or type Control-D to continue):
```

Mögliche Ursachen

- In den Ramdisk-Dateisystemdefinitionen "/etc/fstab" liegt ein Fehler vor.
- Die Dateisystemdefinitionen in "/etc/fstab" sind falsch konfiguriert.
- Das Laufwerk fehlt/ist fehlerhaft.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Stoppen Sie die Instance, trennen Sie das Root-Volume, repair/modify /etc/fstab das Volume, hängen Sie das Volume an die Instance an und starten Sie die Instance. 2. Korrigieren Sie die Ramdisk, sodass die geänderte Datei "/etc/fstab" enthalten ist (falls zutreffend). 3. Ändern Sie das AMI zur Verwendung einer neueren Ramdisk. Das sechste Feld in der fstab-Datei definiert die Verfügbarkeitsanforderungen für das Mounting. Ein Wert ungleich null impliziert, dass ein fsck-Befehl für dieses Volume ausgeführt wird und erfolgreich beendet werden muss. Die Verwendung dieses Felds kann in Amazon problematisch sein EC2 , da ein Fehler in der Regel zu einer interaktiven Konsolenaufforderu

Für diesen Instance-Typ	Vorgehensweise
	ng führt, die derzeit bei Amazon nicht verfügbar ist EC2. Verwenden Sie dieses Feature mit Bedacht und lesen Sie den Abschnitt über die fstab-Datei im Linux-Handbuch.
Instance Store-Backup	Führen Sie die folgenden Schritte aus: 1. Beenden Sie die Instance und starten Sie eine neue Instance. 2. Trennen Sie fehlerhafte Amazon EBS-Volum es und die Neustart-Instance. 3. (Optional) Wenden Sie sich an den , um technische Unterstützung zur Datenwied erherstellung zu erhalten Support.

Allgemeiner Fehler beim Mounten von Dateisystemen (Mountfehler)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
Loading xenblk.ko module
xen-vbd: registered block device major 8

Loading ehci-hcd.ko module
Loading ohci-hcd.ko module
Loading uhci-hcd.ko module
USB Universal Host Controller Interface driver v3.0

Loading mbcache.ko module
Loading jbd.ko module
Loading ext3.ko module
Creating root device.
Mounting root filesystem.
kjournald starting.  Commit interval 5 seconds

EXT3-fs: mounted filesystem with ordered data mode.

Setting up other filesystems.
Setting up new root fs
```

```
no fstab.sys, mounting internal defaults
Switching to new root and running init.
unmounting old /dev
unmounting old /proc
unmounting old /sys
mountall:/proc: unable to mount: Device or resource busy
mountall:/proc/self/mountinfo: No such file or directory
mountall: root filesystem isn't mounted
init: mountall main process (221) terminated with status 1

General error mounting filesystems.
A maintenance shell will now be started.
CONTROL-D will terminate this shell and re-try.
Press enter for maintenance
(or type Control-D to continue):
```

Mögliche Ursachen

Instance-Typ	Mögliche Ursache
Amazon EBS-gestützt	• Das Amazon EBS-Volume wurde getrennt oder ist ausgefallen. • Das Dateisystem ist beschädigt. • Die Ramdisk- und AMI-Kombination stimmt nicht überein (z. B. Debian-Ramdisk mit einem SUSE-AMI).
Instance Store-Backup	• Das Laufwerk ist ausgefallen. • Ein Dateisystem ist beschädigt. • Die Ramdisk- und AMI-Kombination stimmt nicht überein (z. B. Debian-Ramdisk mit einem SUSE-AMI).

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Halten Sie die Instance an. 2. Trennen Sie das Stamm-Volume. 3. Fügen Sie das Stamm-Volume einer funktionierenden Instance an. 4. Führen Sie eine Dateisystemprüfung aus (fsck -a /dev/...). 5. Beheben Sie vorhandene Fehler. 6. Trennen Sie das Volume von der funktioni erenden Instance. 7. Fügen Sie das Volume der angehaltenen Instance an. 8. Starten Sie die Instance. 9. Prüfen Sie den Status der Instance erneut.
Instance Store-Backup	Führen Sie einen der folgenden Schritte aus: • Starten Sie eine neue Instance. • (Optional) Wenden Sie sich an den , um technische Unterstützung zur Datenwied erherstellung zu erhalten Support.

VFS: Unable to mount root fs on unknown-block (fehlende Übereinstimmung des Stammdateisystems)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
 20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
Kernel command line:  root=/dev/sda1 ro 4
```

```
...
Registering block device major 8
...
Kernel panic - not syncing: VFS: Unable to mount root fs on unknown-block(8,1)
```

Mögliche Ursachen

Instance-Typ	Mögliche Ursache
Amazon EBS-gestützt	• Das Gerät ist nicht ordnungsgemäß angefügt. • Das Stammgerät wurde nicht am korrekten Gerätepunkt angefügt. • Das Dateisystem hat nicht das erwartete Format. • Es wurde ein Legacy-Kernel (z. B. 2.6.16-XenU) verwendet. • Ein aktuelles Kernel-Update Ihrer Instance wurde fehlerhaft ausgeführt oder enthält einen Fehler.
Instance Store-Backup	Das Hardware-Gerät ist ausgefallen.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie eine der folgenden Aufgaben aus: • Halten Sie die Instance an und starten Sie sie neu. • Ändern Sie das Root-Volume so, dass es am richtigen Gerätepunkt angehängt wird, möglich/dev/sda1 instead of /dev/sda. • Halten Sie das Gerät an und ändern Sie es auf einen aktuellen Kernel.

Für diesen Instance-Typ	Vorgehensweise
	• Bekannte Fehler beim Update finden Sie in der Dokumentation Ihrer Linux-Verteilung. Ändern Sie den Kernel oder installieren Sie ihn neu.
Instance Store-Backup	Beenden Sie die Instance und starten Sie eine neue Instance mit einem aktuellen Kernel.

Fehler: Die major/minor Anzahl der Root-Geräte konnte nicht ermittelt werden... (Root-Datei system/device stimmt nicht überein)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
...
XENBUS: Device with no driver: device/vif/0
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

Mögliche Ursachen

- Der virtuelle Blockgerättreiber fehlt oder ist falsch konfiguriert.
- Es liegt eine Gerätenummerierungskollision vor (sda statt xvda oder sda statt sda1).
- Der falsche Instance-Kernel wurde ausgewählt.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Halten Sie die Instance an. 2. Trennen Sie das Volume ab. 3. Beheben Sie das Gerätezuweisungspr oblem. 4. Starten Sie die Instance. 5. Ändern Sie das AMI, um die Gerätezuw eisungsprobleme zu beheben.
Instance Store-Backup	Führen Sie die folgenden Schritte aus: 1. Erstellen Sie ein neues AMI mit der entsprechenden Fehlerbehebung (weisen Sie das Blockgerät korrekt zu). 2. Beenden Sie die Instance und starten Sie eine neue Instance mit dem AMI, das Sie erstellt haben.

XENBUS: Device with no driver...

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
```

```
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

Mögliche Ursachen

- Der virtuelle Blockgerättreiber fehlt oder ist falsch konfiguriert.
- Es liegt eine Gerätenummerierungskollision vor (sda statt xvda).
- Der falsche Instance-Kernel wurde ausgewählt.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Halten Sie die Instance an. 2. Trennen Sie das Volume ab. 3. Beheben Sie das Gerätezuweisungsproblem. 4. Starten Sie die Instance. 5. Ändern Sie das AMI, um die Gerätezuweisungsprobleme zu beheben.
Instance Store-Backup	Führen Sie die folgenden Schritte aus: 1. Erstellen Sie ein AMI mit der entsprechenden Fehlerbehebung (weisen Sie das Blockgerät korrekt zu). 2. Beenden Sie die Instance und starten Sie eine neue Instance mit dem AMI, das Sie erstellt haben.

... days without being checked, check forced (Dateisystemprüfung erforderlich)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
...
Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1 has gone 361 days without being checked, check forced
```

Mögliche Ursachen

Der Zeitpunkt der Dateisystemprüfung ist überschritten; eine Dateisystemprüfung wird erzwungen.

Vorgeschlagene Aktionen

- Warten Sie, bis die Dateisystemprüfung abgeschlossen ist. Eine solche Prüfung kann je nach Größe des Stammdateisystems einige Zeit in Anspruch nehmen.
- Ändern Sie Ihre Dateisysteme, um die Erzwingung der Dateisystemprüfung (fsck) mit tune2fs oder mit für Ihr Dateisystem geeigneten Tools zu entfernen.

fsck died with exit status... (fehlendes Gerät)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
Cleaning up ifupdown....
Loading kernel modules...done.
...
Activating lvm and md swap...done.
Checking file systems...fsck from util-linux-ng 2.16.2
/sbin/fsck.xfs: /dev/sdh does not exist
fsck died with exit status 8
[31mfailed (code 8).[39;49m
```

Mögliche Ursachen

- Die Ramdisk sucht nach einem fehlenden Laufwerk.

- Die Konsistenzprüfung des Dateisystems wurde erzwungen.
- Das Laufwerk ist ausgefallen oder wurde getrennt.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie einen oder mehrere der folgenden Schritte aus, um das Problem zu lösen: • Halten Sie die Instance an und fügen Sie das Volume einer vorhandenen, aktuell ausgeführten Instance an. • Führen Sie Konsistenzprüfungen manuell aus. • Korrigieren Sie die Ramdisk, sodass sie relevante Dienstprogramme umfasst. • Ändern Sie Parameter zur Optimierung des Dateisystems, um Konsistenzanforderungen zu entfernen (nicht empfohlen).
Instance Store-Backup	Führen Sie einen oder mehrere der folgenden Schritte aus, um das Problem zu lösen: • Bündeln Sie die Ramdisk mit den richtigen Tools neu. • Ändern Sie Parameter zur Optimierung des Dateisystems, um Konsistenzanforderungen zu entfernen (nicht empfohlen). • Beenden Sie die Instance und starten Sie eine neue Instance. • (Optional) Wenden Sie sich an den , um technische Unterstützung zur Datenwiederherstellung zu erhalten Support.

GRUB prompt (grubdom>)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
    GNU GRUB  version 0.97  (629760K lower / 0K upper memory)

       [ Minimal BASH-like line editing is supported.   For

         the   first   word,  TAB  lists  possible  command

         completions.  Anywhere else TAB lists the possible

         completions of a device/filename. ]

grubdom>
```

Mögliche Ursachen

Instance-Typ	Mögliche Ursachen
Amazon EBS-gestützt	• Die GRUB-Konfigurationsdatei fehlt. • Es wird ein falsches GRUB-Image verwendet , sodass die GRUB-Konfigurationsdatei an einem anderen Speicherort erwartet wird. • Es wird ein nicht unterstütztes Dateisystem zum Speichern Ihrer GRUB-Konfiguration sdatei verwendet (Ihr Stammdateisystem wird z. B. in einen Typ konvertiert, der von einer früheren GRUB-Version nicht unterstüt zt wird).
Instance Store-Backup	• Die GRUB-Konfigurationsdatei fehlt. • Es wird ein falsches GRUB-Image verwendet , sodass die GRUB-Konfigurationsdatei an einem anderen Speicherort erwartet wird. • Es wird ein nicht unterstütztes Dateisystem zum Speichern Ihrer GRUB-Konfiguration sdatei verwendet (Ihr Stammdateisystem

Instance-Typ	Mögliche Ursachen
	wird z. B. in einen Typ konvertiert, der von einer früheren GRUB-Version nicht unterstützt wird).

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Option 1: Ändern Sie das AMI und starten Sie die Instance neu: 1. Ändern Sie das Quell-AMI, um eine GRUB-Konfigurationsdatei am Standardspeicherort (/boot/grub/menu.lst) zu erstellen. 2. Überprüfen Sie, dass Ihre GRUB-Version den zugrunde liegenden Dateisystemtyp unterstützt, und upgraden Sie GRUB, falls erforderlich. 3. Wählen Sie das geeignete GRUB-Image aus ("hd0-1st drive" oder "hd00 – 1st drive, 1st partition"). 4. Beenden Sie die Instance, und starten Sie eine neue Instance mit dem AMI, das Sie erstellt haben. Option 2: Reparieren Sie die vorhandene Instance: 1. Halten Sie die Instance an. 2. Trennen Sie das Stammdateisystem. 3. Fügen Sie das Stammdateisystem einer funktionierenden Instance an. 4. Mounten Sie das Dateisystem.

Für diesen Instance-Typ	Vorgehensweise
	5. Erstellen Sie eine GRUB-Konfiguration sdatei. 6. Überprüfen Sie, dass Ihre GRUB-Version den zugrunde liegenden Dateisystemtyp unterstützt, und upgraden Sie GRUB, falls erforderlich. 7. Trennen Sie das Dateisystem. 8. Fügen Sie es der ursprünglichen Instance an. 9. Ändern Sie das Kernel-Attribut zur Verwendung des entsprechenden GRUB-Images ("hd0-1st drive" oder "hd00 – 1st drive, 1st partition"). 10. Starten Sie die Instance.

Für diesen Instance-Typ	Vorgehensweise
Instance Store-Backup	Option 1: Ändern Sie das AMI und starten Sie die Instance neu: 1. Erstellen Sie das neue AMI mit einer GRUB-Konfigurationsdatei am Standardspeicherort (/boot/grub/menu.lst). 2. Wählen Sie das geeignete GRUB-Image aus ("hd0-1st drive" oder "hd00 – 1st drive, 1st partition"). 3. Überprüfen Sie, dass Ihre GRUB-Version den zugrunde liegenden Dateisystemtyp unterstützt, und upgraden Sie GRUB, falls erforderlich. 4. Beenden Sie die Instance und starten Sie eine neue Instance mit dem AMI, das Sie erstellt haben. Option 2: Beenden Sie die Instance und starten Sie eine neue Instance unter Angabe des korrekten Kernels. **Note** Wenden Sie sich an den Support, um Daten von der vorhandenen Instance wiederherzustellen.

Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring. (hartcodierte MAC-Adresse)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
. . .
```

```
Bringing up loopback interface:  [  OK  ]

Bringing up interface eth0:  Device eth0 has different MAC address than expected,
 ignoring.
[FAILED]

Starting auditd: [  OK  ]
```

Mögliche Ursachen

In der AMI-Konfiguration ist eine hartcodierte MAC-Schnittstelle enthalten.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie eine der folgenden Aufgaben aus: • Ändern Sie das AMI, um die Hartcodierung zu entfernen, und starten Sie die Instance neu. • Ändern Sie die Instance, um die hartcodierte MAC-Adresse zu entfernen. ODER Führen Sie die folgenden Schritte aus: 1. Halten Sie die Instance an. 2. Trennen Sie das Stamm-Volume. 3. Fügen Sie das Volume einer anderen Instance an und ändern Sie das Volume, um die hartcodierte MAC-Adresse zu entfernen. 4. Fügen Sie das Volume der ursprünglichen Instance an. 5. Starten Sie die Instance.
Instance Store-Backup	Führen Sie eine der folgenden Aufgaben aus:

Für diesen Instance-Typ	Vorgehensweise
	• Ändern Sie die Instance, um die hartcodierte MAC-Adresse zu entfernen. • Beenden Sie die Instance und starten Sie eine neue Instance.

Die Richtlinie konnte nicht geladen werden SELinux . Machine is in enforcing mode. Wird jetzt angehalten. (SELinux Fehlkonfiguration)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
audit(1313445102.626:2): enforcing=1 old_enforcing=0 auid=4294967295
Unable to load SELinux Policy. Machine is in enforcing mode. Halting now.
Kernel panic - not syncing: Attempted to kill init!
```

Mögliche Ursachen

SELinux wurde irrtümlich aktiviert:

- Der bereitgestellte Kernel wird von GRUB nicht unterstützt.
- Der Fallback-Kernel ist nicht vorhanden.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Halten Sie die ausgefallene Instance an. 2. Trennen Sie die ausgefallene Instance vom Stamme-Volume. 3. Fügen Sie das Stamm-Volume einer anderen, aktuell ausgeführten Linux-Instance an (diese wird nachfolgend als Wiederher stellungs-Instance bezeichnet).

Für diesen Instance-Typ	Vorgehensweise
	4. Stellen Sie eine Verbindung mit der Wiederherstellungs-Instance her und mounten Sie das Stamm-Volume der ausgefallenen Instance. 5. SELinux Auf dem bereitgestellten Root-Volume deaktivieren. Dieser Prozess ist je nach Linux-Verteilung unterschiedlich. Weitere Informationen finden Sie in der betriebssystemspezifischen Dokumentation. **Note** Auf einigen Systemen deaktivieren Sie, SELinux indem Sie `SELINUX=disabled` in der `/mount_point/etc/sysconfig/selinux` Datei angeben, wo sich der Speicherort *`mount_point`* befindet, an dem Sie das Volume auf Ihrer Wiederherstellungsinstanz bereitgestellt haben. 6. Heben Sie die Bereitstellung des Stamm-Volumes auf, trennen Sie es von der Wiederherstellungs-Instance und fügen Sie es der ursprünglichen Instance wieder an. 7. Starten Sie die Instance.
Instance Store-Backup	Führen Sie die folgenden Schritte aus: 1. Beenden Sie die Instance und starten Sie eine neue Instance. 2. (Optional) Wenden Sie sich an den , um technische Unterstützung zur Datenwiederherstellung zu erhalten Support.

XENBUS: Timeout connecting to devices (Xenbus-Timeout)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
XENBUS: Timeout connecting to devices!
...
Kernel panic - not syncing: No init found.  Try passing init= option to kernel.
```

Mögliche Ursachen

- Das Blockgerät ist nicht mit der Instance verbunden.
- Die Instance verwendet einen alten Instance-Kernel.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie eine der folgenden Aufgaben aus: • Ändern Sie das AMI und die Instance, um einen aktuellen Kernel zu verwenden, und starten Sie die Instance neu. • Starten Sie die Instance neu.
Instance Store-Backup	Führen Sie eine der folgenden Aufgaben aus: • Beenden Sie die Instance. • Ändern Sie das AMI, um einen aktuellen Kernel zu verwenden, und starten Sie eine neue Instance mit dem geänderten AMI.

Fehlerbehebung bei einer Amazon EC2 Linux-Instance, die von einem falschen Volume gestartet wurde

In einigen Situationen stellen Sie möglicherweise fest, dass ein anderes Volume als das der Datei `/dev/xvda` oder `/dev/sda` angefügte als Root-Volume Ihrer Instance verwendet wird. Dies kann der Fall sein, wenn Sie das Stamm-Volume einer anderen Instance – oder ein aus dem Snapshot eines Stamm-Volumes erstelltes Volume – einer Instance mit einem vorhandenen Stamm-Volume angefügt haben.

Die Ursache ist in der Funktionsweise der anfänglichen Ramdisk in Linux zu suchen. Sie wählt das Volume, das als `/` in `/etc/fstab` definiert ist, aus und in einigen Verteilungen wird dies durch die Bezeichnung bestimmt, die der Volume-Partition angefügt ist. Ihre `/etc/fstab`-Datei sieht ähnlich aus wie im folgenden Beispiel dargestellt:

```
LABEL=/ / ext4 defaults,noatime 1 1
tmpfs /dev/shm tmpfs defaults 0 0
devpts /dev/pts devpts gid=5,mode=620 0 0
sysfs /sys sysfs defaults 0 0
proc /proc proc defaults 0 0
```

Wenn Sie die Bezeichnung beider Volumes überprüfen, stellen Sie fest, dass beide die `/`-Bezeichnung enthalten:

```
[ec2-user ~]$ sudo e2label /dev/xvda1
/
[ec2-user ~]$ sudo e2label /dev/xvdf1
/
```

In diesem Beispiel wird `/dev/xvdf1` möglicherweise zum Root-Volume, von dem aus Ihre Instance startet, nachdem die anfängliche Ramdisk ausgeführt wird, statt dass der Start wie beabsichtigt über das `/dev/xvda1`-Volume erfolgt. Um dies zu beheben, verwenden Sie denselben e2label-Befehl, um die Bezeichnung des angefügten Volumes zu ändern, von dem aus der Start nicht erfolgen soll.

In manchen Fällen kann dies durch die Angabe einer UUID in `/etc/fstab` gelöst werden. Wenn jedoch beide Volumes aus demselben Snapshot kommen oder das sekundäre Volume aus einem Snapshot des primären Volumes erstellt wird, haben sie eine gemeinsame UUID.

```
[ec2-user ~]$ sudo blkid
```

```
/dev/xvda1: LABEL="/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
/dev/xvdf1: LABEL="old/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
```

So ändern Sie die Bezeichnung eines angefügten ext4- Volumes

1. Ändern Sie mit dem e2label-Befehl die Bezeichnung des Volumes, sodass sie nicht / lautet.

   ```
   [ec2-user ~]$ sudo e2label /dev/xvdf1 old/
   ```

2. Überprüfen Sie, dass das Volume über die neue Bezeichnung verfügt.

   ```
   [ec2-user ~]$ sudo e2label /dev/xvdf1
   old/
   ```

So ändern Sie die Bezeichnung eines angefügten xfs-Volumes

- Ändern Sie mit dem xfs_admin-Befehl die Bezeichnung des Volumes, sodass sie nicht / lautet.

  ```
  [ec2-user ~]$ sudo xfs_admin -L old/ /dev/xvdf1
  writing all SBs
  new label = "old/"
  ```

Nachdem Sie die Bezeichnung des Volumes wie gezeigt geändert haben, sollten Sie die Instance neu starten können und das richtige Volume sollte von der anfänglichen Ramdisk beim Start der Instance ausgewählt werden.

> **Important**
>
> Wenn Sie das Volume mit dem neuen Etikett trennen und an eine andere Instance zur Verwendung als Root-Volume zurückgeben möchten, müssen Sie das obige Verfahren erneut durchführen und das Volumeetikett wieder auf seinen ursprünglichen Wert setzen. Andernfalls wird die andere Instance nicht gestartet, da die Ramdisk das Volume mit dem Etikett nicht finden kan /.

Verbindungsprobleme mit Ihrer Amazon-EC2-Windows-Instance beheben

Die folgenden Informationen und häufigen Fehler können Ihnen bei der Fehlersuche für die Verbindung zu Ihrer Windows-Instance helfen.

Verbindungsprobleme

- Der Remotedesktopdienst kann keine Verbindung zu dem Remotecomputer herstellen
- Fehler beim Verwenden des macOS RDP-Clients
- RDP zeigt anstelle des Desktops einen schwarzen Bildschirm an
- Die Remote-Anmeldung bei einer Instance mit einem Benutzer, der kein Administrator ist, ist nicht möglich
- Fehlerbehebung bei Remotedesktop-Problemen mit AWS Systems Manager
- Aktivieren von Remotedesktop für eine EC2-Instance mit Remote-Registrierung
- Ich habe meinen privaten Schlüssel verloren. Wie kann ich mich mit meiner Windows-Instance verbinden?

Der Remotedesktopdienst kann keine Verbindung zu dem Remotecomputer herstellen

Versuchen Sie, Verbindungsprobleme mit Ihre Instance mit den folgenden Maßnahmen zu beheben:

- Vergewissern Sie sich, dass Sie den richtigen öffentlichen DNS-Hostnamen verwenden. (Wählen Sie in der Amazon EC2-Konsole die Instance aus und überprüfen Sie im Detailbereich den Wert für Public DNS (IPv4).) Wenn sich Ihre Instance in einer VPC befindet, aber kein öffentlicher DNS-Name angezeigt wird, müssen Sie die DNS-Hostnamen aktivieren. Weitere Infomationen finden Sie unter DNS-Attribute für Ihre VPC im Amazon VPC-Benutzerhandbuch.
- Überprüfen Sie, ob Ihre Instance über eine öffentliche IPv4-Adresse verfügt. Falls nicht, verknüpfen Sie eine Elastic IP-Adresse mit der Instance. Weitere Informationen finden Sie unter Elastic-IP-Adressen.
- Um eine Verbindung zu Ihrer Instance mit einer IPv6-Adresse herzustellen, überprüfen Sie, dass Ihr lokaler Computer muss über eine IPv6-Adresse verfügt und zur Verwendung von IPv6 konfiguriert ist. Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf Ihren Instances im Benutzerhandbuch von Amazon VPC.

- Überprüfen Sie, ob für Ihre Sicherheitsgruppe eine Regel eingerichtet ist, die den RDP-Zugriff über Port 3389 zulässt.
- Wenn Sie das Passwort kopiert und eingefügt haben, und die Fehlermeldung `Your credentials did not work` angezeigt wird, geben Sie das Passwort manuell ein. Möglicherweise ist beim Kopieren des Passworts ein Buchstabe zu wenig oder ein Leerzeichen zu viel markiert gewesen.
- Überprüfen Sie, ob Ihre Instance ihre Statusprüfungen bestanden hat. Weitere Informationen finden Sie unter Statuschecks für EC2 Amazon-Instances und the section called “Nicht bestandene Statusprüfungen einer Linux-Instance”.
- Überprüfen Sie, dass die Routing-Tabelle für das Subnetz eine Route hat, die den gesamten Datenverkehr mit Zielen außerhalb der VPC an das Internet-Gateway für die VPC sendet. Weitere Informationen finden Sie unter Erstellen einer benutzerdefinierten Routing-Tabelle (Internet-Gateways) im Amazon VPC Benutzerhandbuch.
- Überprüfen Sie, ob die Windows-Firewall – oder eine andere Firewall-Software – den RDP-Datenverkehr zu Ihrer Instance blockiert. Wir empfehlen, die Windows-Firewall zu deaktivieren und den Zugriff auf Ihre Instance mithilfe von Sicherheitsgruppenregeln zu steuern. Versuchen Sie es mit einer der folgenden Optionen:
  - Verwenden Sie AWSSupport-TroubleshootRDP für disable the Windows Firewall profiles using SSM Agent. Diese Option erfordert, dass die Instance für AWS Systems Manager konfiguriert ist.
  - Verwenden Sie AWSSupport-ExecuteEC2Rescue.
  - Halten Sie die Instance an, trennen Sie das Root-Volume und fügen Sie das Volume als Daten-Volume an eine temporäre Instance an. Stellen Sie eine Verbindung zur temporären Instance her und bringen Sie das Volume online. Laden Sie die Registry Hive aus dem Daten-Volume. Legen Sie unter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicyStandardProfile` die Option `EnableFirewall` auf 0. Entladen Sie die Registry Hive und stellen Sie das Volume offline. Trennen Sie das Volume von der temporären Instance und fügen Sie es an die ursprüngliche Instance als Root-Volume an. Starten Sie die ursprüngliche Instance.
- Stellen Sie sicher, dass die Authentifizierung auf Netzwerkebene für Instances, die nicht Teil einer Active-Directory-Domain sind, deaktiviert ist (verwenden Sie AWSSupport-TroubleshootRDP um disable NLA auszuführen).
- Stellen Sie sicher, dass der Startup-Typ des Remotedesktopservices (TermService) auf „Automatisch“ festgelegt ist und der Service gestartet wurde (verwenden Sie AWSSupport-TroubleshootRDP um enable and start the RDP service auszuführen).

- Stellen Sie sicher, dass Sie die Verbindung mit dem richtigen Port des Remotedesktop-Protokolls herstellen, der standardmäßig 3389 lautet (verwenden Sie AWSSupport-TroubleshootRDP um read the current RDP port und change it back to 3389 auszuführen).
- Stellen Sie sicher, dass Remote-Desktop-Verbindungen auf Ihrer Instance hergestellt werden können (verwenden Sie AWSSupport-TroubleshootRDP um enable Remote Desktop connections auszuführen).
- Überprüfen Sie, dass das Passwort nicht abgelaufen ist. Wenn das Passwort abgelaufen ist, können Sie es zurücksetzen. Weitere Informationen finden Sie unter Zurücksetzen des Windows-Administratorpassworts für eine Amazon-EC2-Windows-Instance.
- Wenn Sie versuchen, eine Verbindung mit einem Benutzer herzustellen, den Sie auf der Instance erstellt haben, und den Fehler `The user cannot connect to the server due to insufficient access privileges` erhalten, überprüfen Sie, ob Sie dem Benutzer das Recht zur lokalen Anmeldung gewährt haben. Weitere Informationen finden Sie unter Einem Mitglied das Recht zur lokalen Anmeldung gewähren.
- Wenn Sie versuchen, eine Sitzung zu starten, und es ist bereits die Höchstgrenze gleichzeitiger RDP-Sitzungen erreicht, wird Ihre Sitzung mit der folgenden Meldung beendet: `Your Remote Desktop Services session has ended. Another user connected to the remote computer, so your connection was lost.` Standardmäßig sind pro Instance zwei gleichzeitige RDP-Sitzungen pro Instance erlaubt.

Fehler beim Verwenden des macOS RDP-Clients

Wenn Sie eine Verbindung mit einer Windows-Server-Instance über den Remote Desktop Connection-Client auf der Microsoft-Website herstellen, erhalten Sie möglicherweise folgenden Fehler:

```
Remote Desktop Connection cannot verify the identity of the computer that you want to
 connect to.
```

Laden Sie die Microsoft Remote Desktop App vom Mac App Store herunter und stellen Sie die Verbindung mit Ihrer Instance über die App her.

RDP zeigt anstelle des Desktops einen schwarzen Bildschirm an

Versuchen Sie, das Problem wie folgt zu beheben:

- Überprüfen Sie die Ausgabe der Konsole, ob weitere Informationen gegeben werden. Um die Ausgabe der Konsole für Ihre Instance mit der Amazon EC2-Konsole abzurufen, wählen Sie die Instance aus, wählen Sie dann Actions (Aktionen), Monitor and troubleshoot (Überwachung und Fehlerbehebung), Get System Log (Systemprotokoll abrufen).
- Überprüfen Sie, ob Sie die neueste Version Ihres RDP-Clients verwenden.
- Verwenden Sie versuchsweise die Standardeinstellungen für den RDP-Client.
- Wenn Sie eine Remotedesktopverbindung verwenden, versuchen Sie, diese wie folgt mit der Option `/admin` zu starten.

```
mstsc /v:instance /admin
```

- Wenn der Server eine Anwendung im Vollbildschirmmodus ausführt, besteht die Möglichkeit, dass diese Anwendung nicht mehr reagiert. Starten Sie mit Strg+Umschalt+Esc den Windows-Task-Manager und beenden Sie die betreffende Anwendung.
- Wenn der Server überlastet ist, besteht die Möglichkeit, dass der Server nicht mehr reagiert. Um die Instance mit der Amazon EC2-Konsole zu überwachen, wählen Sie die Instance aus und wählen Sie dann die Registerkarte Monitoring. Wenn Sie den Typ der Instance in einen größeren Typ ändern müssen, siehe Änderungen des EC2 Amazon-Instanztyps.

Die Remote-Anmeldung bei einer Instance mit einem Benutzer, der kein Administrator ist, ist nicht möglich

Wenn Sie sich mit einem Benutzer, bei dem es sich nicht um ein Administratorkonto handelt, nicht remote an einer Windows-Instance anmelden können, stellen Sie sicher, dass Sie dem Benutzer das Recht zur lokalen Anmeldung gewährt haben. Siehe Einem Benutzer oder einer Gruppe das Recht zur lokalen Anmeldung bei den Domain-Controllern in der Domain gewähren.

Fehlerbehebung bei Remotedesktop-Problemen mit AWS Systems Manager

Sie können AWS Systems Manager verwenden, um Probleme bei der Herstellung der Verbindung zur Ihrer Windows-Instance mit RDP zu beheben.

AWSSupport-TroubleshootRDP

Mit dem Automatisierungsdokument AWSSupport-TroubleshootRDP kann der Benutzer häufige Einstellungen auf der Ziel-Instance, die Remote Desktop Protocol (RDP)-Verbindungen

beeinträchtigen können, wie z. B. die RDP-Port-, Network Layer Authentication (NLA)- und Windows-Firewall-Profile, überprüfen und ändern. Standardmäßig liest das Dokument die Werte dieser Einstellungen und gibt sie aus.

Das AWSSupport-TroubleshootRDP-Automatisierungsdokument kann mit EC2-Instances, On-Premises-Instances und virtuellen Maschinen (VMs) verwendet werden, die für die Verwendung mit AWS Systems Manager (verwaltete Instances) aktiviert sind. Darüber hinaus kann es auch mit EC2-Instances für Windows Server verwendet werden, die nicht für die Verwendung mit Systems Manager aktiviert sind. Informationen über die Aktivierung von Instances zur Verwendung mit AWS Systems Manager finden Sie unter Verwaltete Knoten im Benutzerhandbuch von AWS Systems Manager.

Fehlerbehebung mit dem Dokument AWSSupport-TroubleshootRDP

1. Melden Sie sich bei der Systems Manager-Konsole an.
2. Vergewissern Sie sich, dass Sie sich in der gleichen Region wie die beeinträchtigte -Instance befinden.
3. Wählen Sie im linken Navigationsbereich Documents (Dokumente) aus.
4. Auf der Registerkarte Owned by Amazon (Im Besitz von Amazon) geben Sie `AWSSupport-TroubleshootRDP` im Suchfeld ein. Wenn das Dokument `AWSSupport-TroubleshootRDP` angezeigt wird, wählen Sie es aus.
5. Wählen Sie Automatisierung ausführen.
6. Wählen Sie für Execution mode (Ausführungsmodus) die Option Simple execution (Einfache Ausführung) aus.
7. Aktivieren Sie für Input parameters (Eingabeparameter), InstanceID die Option Show interactive instance picker (Interaktiven Instance-Picker anzeigen).
8. Wählen Sie Ihre Amazon EC2-Instance aus.
9. Überprüfen Sie die Beispiele und wählen Sie dann Execute (Ausführen) aus.
10. Um den Fortschritt der Ausführung zu überwachen, warten Sie bei Execution status (Ausführungsstatus), bis sich der Status von Pending (Ausstehend) in Success (Erfolg) ändert. Erweitern Sie Outputs, um die Ergebnisse anzuzeigen. Zum Anzeigen der Ausgabe der einzelnen Schritte wählen Sie unter Executed Steps (Ausgeführte Schritte) ein Element aus Step ID (Schritt-ID) aus.

AWSSupport-TroubleshootRDP-Beispiele

Die nachstehenden Beispiele veranschaulichen, wie gängige Aufgaben zur Fehlerbehebung mit AWSSupport-TroubleshootRDP ausgeführt werden. Sie können entweder den Beispielbefehl AWS CLI start-automation-execution oder den bereitgestellten Link zur AWS-Managementkonsole verwenden.

Example Beispiel: Überprüfen des aktuellen RDP-Status

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom" --region region_code
```

AWS Systems Manager-Konsole

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region#documentVersion=$LATEST
```

Example Beispiel: Deaktivieren der Windows-Firewall

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=i-1234567890abcdef0, Action=Custom, Firewall=Disable" --
region region_code
```

AWS Systems Manager-Konsole

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&Firewall=Disable
```

Example Beispiel: Deaktivieren der Authentifizierung auf Netzwerkebene

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom, NLASettingAction=Disable" --
region region_code
```

AWS Systems Manager-Konsole

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion
```

Example Beispiel: Stellen Sie den Startup-Typ des RDP-Services auf „Automatic“ (Automatisch) ein und starten Sie den RDP-Service

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom, RDPServiceStartupType=Auto,
 RDPServiceAction=Start" --region region_code
```

AWS Systems Manager-Konsole

```
https://console.aws.amazon.com/systems-manager/automation/execute/
AWSSupport-TroubleshootRDP?region=region_code#documentVersion=
$LATEST&RDPServiceStartupType=Auto&RDPServiceAction=Start
```

Example Beispiel: Wiederherstellen des Standard-RDP-Ports (3389)

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom, RDPPortAction=Modify" --
region region_code
```

AWS Systems Manager-Konsole

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RDPPortAction=Modify
```

Example Beispiel: Zulassen von Remote-Verbindungen

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=i-1234567890abcdef0, Action=Custom, RemoteConnections=Enable" --
region region_code
```

AWS Systems Manager-Konsole

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RemoteConnections=Enable
```

AWSSupport-ExecuteEC2Rescue

Das Automatisierungsdokument „AWSSupport-ExecuteEC2Rescue“ verwendet EC2Rescue zur automatischen Fehlerbehebung und Wiederherstellung bei EC2-Instance-Konnektivitäts- und RDP-Problemen. Weitere Informationen finden Sie unter Ausführen des EC2Rescue-Tools auf nicht erreichbaren Instances.

Das Automatisierungsdokument AWSSupport-ExecuteEC2Rescue erfordert, dass die Instance angehalten und neu gestartet wird. Die Systems Manager-Automatisierung hält die Instance an und erstellt ein Amazon Machine Image (AMI). Alle in den Instance-Speichervolumes gespeicherten Daten gehen verloren. Die öffentliche IP-Adresse ändert sich, wenn Sie keine Elastic IP-Adresse verwenden. Weitere Informationen finden Sie unter Ausführen des EC2Rescue-Tools auf nicht erreichbaren Instances im Benutzerhandbuch von AWS Systems Manager.

Fehlerbehebung mit dem Dokument AWSSupport-ExecuteEC2Rescue

1. Öffnen Sie die Systems Manager-Konsole.
2. Vergewissern Sie sich, dass Sie sich in der gleichen Region wie die beeinträchtigte Amazon EC2-Instance befinden.
3. Wählen Sie im Navigationsbereich die Option Dokumente.
4. Suchen Sie nach dem Dokument `AWSSupport-ExecuteEC2Rescue`, wählen Sie es aus und wählen Sie dann Automatisierung ausführen.
5. Wählen Sie unter Execution mode (Ausführungsmodus) die Option Simple execution (Einfache Ausführung) aus.
6. Geben Sie im Abschnitt Input parameters (Eingabeparameter) für UnreachableInstanceId die Amazon EC2-Instance-ID der nicht erreichbaren Instance ein.
7. (Optional) Geben Sie für LogDestination den Amazon Simple Storage Service (Amazon S3)-Bucketnamen ein, wenn Sie Betriebssystemprotokolle für die Fehlerbehebung bei Ihrer Amazon EC2-Instance erfassen möchten. Protokolle werden automatisch in den angegebenen Bucket hochgeladen.
8. Wählen Sie Execute (Ausführen).

9. Um den Fortschritt der Ausführung zu überwachen, warten Sie unter Execution status (Ausführungsstatus), bis sich der Status von Pending (Ausstehend) in Success (Erfolg) ändert. Erweitern Sie Outputs, um die Ergebnisse anzuzeigen. Zum Anzeigen der Ausgabe der einzelnen Schritte klicken Sie unter Executed Steps (Ausgeführte Schritte) auf Step ID (Schritt-ID).

Aktivieren von Remotedesktop für eine EC2-Instance mit Remote-Registrierung

Wenn Ihre nicht erreichbare Instance nicht von AWS Systems Manager Session Manager verwaltet wird, können Sie Remote Desktop mithilfe der Remoteregistrierung aktivieren.

1. Beenden Sie die nicht erreichbare Instance über die EC2-Konsole.
2. Trennen Sie das Stamm-Volume der nicht erreichbaren Instance und fügen Sie es an eine erreichbare Instance in der gleichen Availability Zone an, in der sich auch ein Speicher-Volume befindet. Sollten Sie über keine erreichbare Instance in der gleichen Availability Zone verfügen, starten Sie eine. Notieren Sie sich den Gerätenamen des Stamm-Volumes in der nicht erreichbaren Instance.
3. Öffnen Sie in der erreichbaren Instance die Datenträgerverwaltung. Hierzu können Sie den folgenden Befehl in einem Eingabeaufforderungsfenster ausführen.

   ```
   diskmgmt.msc
   ```

4. Klicken Sie mit der rechten Maustaste auf das neu angefügte Volume, das von der nicht erreichbaren Instance stammt, und wählen Sie anschließend Online aus.
5. Öffnen Sie den Windows Registrierungs-Editor. Hierzu können Sie den folgenden Befehl in einem Eingabeaufforderungsfenster ausführen.

   ```
   regedit
   ```

6. Wählen Sie im Registrierungs-Editor die Option HKEY_LOCAL_MACHINE und anschließend Datei > Hive laden aus.
7. Wählen Sie das Laufwerk des angeschlossenen Volumes aus, navigieren Sie zu `\Windows\System32\config\`, wählen Sie `SYSTEM` aus und wählen Sie dann Open (Öffnen) aus.
8. Geben Sie unter Key Name (Schlüsselname) einen eindeutigen Namen für die Struktur ein, und wählen Sie OK.

9. Sichern Sie die Registrierungsstruktur, bevor Sie Änderungen an der Registrierung vornehmen.

    a. Wählen Sie in der Baumstruktur der Konsole des Registrierungs-Editors die von Ihnen geladene Struktur aus: HKEY_LOCAL_MACHINE*Name Ihres Schlüssels*.

    b. Wählen Sie Datei >Exportieren aus.

    c. Wählen Sie im Dialogfeld „Registrierungsdatei exportieren“ den Speicherort aus, an dem die Sicherungskopie gespeichert werden soll, und geben Sie dann im Feld Dateiname einen Namen für die Sicherungsdatei ein.

    d. Wählen Sie Speichern.

10. Navigieren Sie im Registrierungs-Editor zu `HKEY_LOCAL_MACHINE\`*`your key name`*`\ControlSet001\Control\Terminal Server` und doppelklicken Sie anschließend im Detailbereich auf fDenyTSConnections.

11. Geben Sie im Fenster Edit DWORD (DWORD bearbeiten) in das Feld Value data (Wertedaten) `0` ein.

12. Klicken Sie auf OK.

> **Note**
>
> Wenn der Wert im Wert-Datenfeld `1` lautet, verweigert die Instance Remotedesktopverbindungen. Der Wert `0` erlaubt Remotedesktopverbindungen.

13. Wählen Sie im Registrierungs-Editor die Option HKEY_LOCAL_MACHINE*Name Ihres Schlüssels* und anschließend Datei > Hive entladen aus.

14. Schließen Sie den Registrierungs-Editor und die Datenträgerverwaltung.

15. Trennen Sie über die EC2-Konsole das Volume von der erreichbaren Instance und fügen Sie es wieder an die nicht erreichbare Instance an. Geben Sie beim Anfügen des Volumes an die nicht erreichbare Instance den zuvor gespeicherten Gerätenamen in das Feld Gerät ein.

16. Starten Sie die unerreichbare Instance neu.

Ich habe meinen privaten Schlüssel verloren. Wie kann ich mich mit meiner Windows-Instance verbinden?

Wenn Sie eine Verbindung zu einer neu gestarteten Windows-Instance herstellen, entschlüsseln Sie das Passwort für das Administrator-Konto mithilfe des privaten Schlüssels des Schlüsselpaars, das Sie beim Starten der Instance festgelegt haben.

Wenn Sie das Administratorpasswort und den privaten Schlüssel nicht mehr haben, müssen Sie das Passwort zurücksetzen oder eine neue Instance erstellen. Weitere Informationen finden Sie unter Zurücksetzen des Windows-Administratorpassworts für eine Amazon-EC2-Windows-Instance. Schritte zum Zurücksetzen des Kennworts mithilfe eines Systems-Manager-Dokuments finden Sie unter Zurücksetzen von Kennwörtern und SSH-Schlüsseln auf EC2-Instances im AWS Systems Manager-Benutzerhandbuch.

Problembehebung bei Startproblemen von Amazon-EC2-Windows-Instance

Mithilfe der folgenden Tipps können Sie Passwort- und Aktivierungs-Probleme von Amazon-EC2-Windows-Instances beheben.

Problembereiche

- Passwort nicht verfügbar
- Passwort noch nicht verfügbar
- Windows-Passwort kann nicht abgerufen werden
- Warten auf Metadaten-Service
- Windows kann nicht aktiviert werden
- Keine Original-Windows-Version (0x80070005)
- Kein Terminal Server License-Server verfügbar, um eine Lizenz bereitzustellen
- „Einige Einstellungen werden von Ihrer Organisation verwaltet.“ (Windows 2019)

Passwort nicht verfügbar

Um eine Verbindung zu der Windows-Instance unter Verwendung der Remotedesktopdienste herzustellen, müssen Sie einen Benutzernamen und ein Passwort angeben. Die bereitgestellten Benutzerkonten und Passwörter richten sich nach dem AMI, mit dem die Instance gestartet wurde. Sie können entweder das automatisch erzeugte Passwort für das Administrator-Konto abrufen oder das Benutzerkonto und das Passwort verwenden, das in der ursprünglichen Instance bei der Erstellung des AMI verwendet wurden.

Sie können ein Passwort für das Administratorkonto für Instances generieren, die unter Verwendung eines benutzerdefinierten Windows-AMIs gestartet wurden. Um das Passwort zu generieren, müssen

Sie einige Einstellungen im Betriebssystem konfigurieren, bevor das AMI erstellt wird. Weitere Informationen finden Sie unter Ein Amazon-EBS-gestütztes AMI erstellen.

Wenn Ihre Windows-Instance nicht für die Generierung eines zufällig gewählten Passworts konfiguriert sind, wird bei dem Versuch, das automatisch generierte Passwort über die Konsole abzurufen, die folgende Meldung angezeigt:

```
Password is not available.
The instance was launched from a custom AMI, or the default password has changed. A
password cannot be retrieved for this instance. If you have forgotten your password,
 you can
reset it using the Amazon EC2 configuration service. For more information, see
 Passwords for a
Windows Server instance.
```

Überprüfen Sie die Ausgabe der Konsole für die Instance daraufhin, ob auf dem zum Starten der Instance verwendeten AMI die automatische Generierung des Passworts deaktiviert ist. Wenn die Generierung des Passworts deaktiviert ist, sieht die Ausgabe der Konsole wie folgt aus:

```
Ec2SetPassword: Disabled
```

Wenn die automatische Passwortgenerierung deaktiviert ist und Sie sich nicht an das Passwort der ursprünglichen Instance erinnern, können Sie das Passwort für diese Instance zurücksetzen. Weitere Informationen finden Sie unter Zurücksetzen des Windows-Administratorpassworts für eine Amazon-EC2-Windows-Instance.

Passwort noch nicht verfügbar

Um eine Verbindung zu der Windows-Instance unter Verwendung der Remotedesktopdienste herzustellen, müssen Sie einen Benutzernamen und ein Passwort angeben. Die bereitgestellten Benutzerkonten und Passwörter richten sich nach dem AMI, mit dem die Instance gestartet wurde. Sie können entweder das automatisch erzeugte Passwort für das Administrator-Konto abrufen oder das Benutzerkonto und das Passwort verwenden, das in der ursprünglichen Instance bei der Erstellung des AMI verwendet wurden.

Ihr Passwort sollte innerhalb von einigen Minuten verfügbar sein. Wenn das Passwort noch nicht verfügbar ist, wird bei dem Versuch, das automatisch generierte Passwort über die Konsole abzurufen, die folgende Meldung angezeigt:

```
Password not available yet.
```

```
Please wait at least 4 minutes after launching an instance before trying to retrieve
 the
auto-generated password.
```

Wenn Sie das Passwort auch nach etwa vier Minuten nicht abrufen können, ist möglicherweise der Launch-Agent für Ihre Instance nicht für die Generierung eines Passworts konfiguriert. Sie können dies daran erkennen, dass die Ausgabe der Konsole leer ist. Weitere Informationen finden Sie unter Abrufen der Konsoleausgabe nicht möglich.

Überprüfen Sie auch, dass das IAM-Konto (AWS Identity and Access Management), mit dem auf das Management Portal zugegriffen wird, die Aktion `ec2:GetPasswordData` ausführen darf. Weitere Informationen zum Verwalten von IAM-Berechtigungen finden Sie unter Was ist IAM?.

Windows-Passwort kann nicht abgerufen werden

Um das automatisch generierte Passwort für das Administrator-Konto abzurufen, müssen Sie das Schlüsselpaar verwenden, das Sie beim Starten der Instance festgelegt haben. Wenn Sie beim Starten Ihrer Instance kein Schlüsselpaar angegeben haben, wird die folgende Meldung angezeigt.

```
Cannot retrieve Windows password
```

Sie können diese Instance beenden und eine neue Instance mit demselben AMI starten. Stellen Sie dabei sicher, dass Sie ein Schlüsselpaar angeben.

Warten auf Metadaten-Service

Windows-Instances müssen Informationen aus den Instance-Metadaten abrufen, damit sie sich aktivieren können. Standardmäßig wird mit der Einstellung `WaitForMetaDataAvailable` sichergestellt, dass der EC2Config-Service darauf wartet, dass die Instance-Metadaten zugänglich sind, bevor der Startvorgang fortgesetzt wird. Weitere Informationen finden Sie unter Verwenden Sie Instanz-Metadaten, um Ihre EC2 Instanz zu verwalten.

Wenn die Instance die Erreichbarkeitsprüfung nicht besteht, gehen Sie wie folgt vor, um dieses Problem zu beheben.

- Überprüfen Sie bei EC2-VPC den CIDR-Block Ihrer VPC. Windows-Instances können nicht ordnungsgemäß gestartet werden, wenn sie in einer VPC in einem IP-Adressbereich von `224.0.0.0` bis `255.255.255.255` gestartet werden (IP-Adressbereiche Klasse D und Klasse E). Diese IP-Adressbereiche sind reserviert und sollten keinen Hostgeräten zugewiesen werden. Wir

empfehlen, eine VPC mit einem CIDR-Block aus dem privaten (nicht öffentlich routingfähigen) IP-Adressbereich zu erstellen, wie in RFC 1918 spezifiziert.

- Möglicherweise wurde das System mit einer statischen IP-Adresse konfiguriert. Probieren Sie, eine Netzwerkschnittstelle zu erstellen und sie der Instance anzufügen.
- So aktivieren Sie DHCP auf einer Windows-Instance, zu der Sie keine Verbindung herstellen können

  1. Beenden Sie die betroffene Instance und trennen Sie das Stamm-Volume von der Instance.
  2. Starten Sie eine temporäre Instance in derselben Availability Zone wie die betroffene Instance.

     > **Warning**
     >
     > (Optional) Wenn ihre temporäre Instance auf demselben AMI basiert wie die ursprüngliche Instance, müssen Sie zusätzliche Schritte ausführen. Anderenfalls werden Sie die ursprüngliche Instance nach der Wiederherstellung des Stamm-Volumes wegen einer Festplatten-Signaturkollision nicht booten können. Alternativ können Sie ein anderes AMI für die temporäre Instance verwenden. Wenn beispielsweise die Original-Instance das AWS-Windows-AMI für Windows Server 2016 verwendet, starten Sie die temporäre Instance mithilfe des AWS-Windows-AMI für Windows Server 2019.

  3. Hängen Sie das Stamm-Volume aus der betroffenen Instance an diese temporäre Instance an. Stellen Sie eine Verbindung mit der temporären Instance her, öffnen Sie das Datenträgerverwaltung-Dienstprogramm und bringen Sie das Laufwerk online.
  4. Öffnen Sie von der temporären Instance aus Regedit und wählen Sie HKEY_LOCAL_MACHINE. Wählen Sie im Menü File die Option Load Hive aus. Wählen Sie das Laufwerk aus, öffnen Sie die Datei `Windows\System32\config\SYSTEM` und geben Sie einen (frei wählbaren) Schlüsselnamen ein, wenn Sie dazu aufgefordert werden.
  5. Wählen Sie den gerade geladenen Schlüssel aus und navigieren Sie zu `ControlSet001\Services\Tcpip\Parameters\Interfaces`. Dort sind alle Netzwerkschnittstellen nach ihrer GUID sortiert aufgelistet. Wählen Sie die richtige Netzwerkschnittstelle aus. Wenn DHCP deaktiviert und eine statische IP-Adresse zugewiesen ist, ist `EnableDHCP` auf 0 gesetzt. Um DHCP zu aktivieren, setzen Sie `EnableDHCP` auf 1 und löschen Sie die folgenden Schlüssel (falls vorhanden): `NameServer`, `SubnetMask`, `IPAddress` und `DefaultGateway`. Wählen Sie den Schlüssel erneut aus und wählen Sie dann aus dem Menü File den Befehl Unload Hive.

> **Note**
>
> Wenn Sie mehrere Netzwerkschnittstellen konfiguriert haben, müssen Sie DHCP für die richtige Schnittstelle aktivieren. Um die richtige Netzwerkschnittstelle zu identifizieren, überprüfen Sie die folgenden Schlüsselwerte: `NameServer`, `SubnetMask`, `IPAddress` und `DefaultGateway`. Diese Werte enthalten die statische Konfiguration der vorangehenden Instance.

6. (Optional) Wenn DHCP bereits aktiviert ist, besteht die Möglichkeit, dass keine Route zu dem Metadaten-Service vorhanden ist. Sie können dieses Problem beheben, indem Sie EC2Config aktualisieren.

   a. Laden Sie die aktuelle Version des EC2Config-Service herunter und installieren Sie sie. Weitere Informationen zum Installieren dieses Service erhalten Sie unter the section called “Installieren von EC2Config”.

   b. Extrahieren Sie die Dateien aus der `.zip`-Datei in das `Temp`-Verzeichnis auf dem von Ihnen angefügten Laufwerk.

   c. Öffnen Sie Regedit und wählen Sie HKEY_LOCAL_MACHINE. Wählen Sie im Menü File die Option Load Hive aus. Wählen Sie das Laufwerk aus, öffnen Sie die Datei `Windows\System32\config\SOFTWARE` und geben Sie einen (frei wählbaren) Schlüsselnamen ein, wenn Sie dazu aufgefordert werden.

   d. Wählen Sie den gerade geladenen Schlüssel aus und navigieren Sie zu `Microsoft\Windows\CurrentVersion`. Wählen Sie den Schlüssel `RunOnce` aus. (Wenn dieser Schlüssel nicht vorhanden ist, klicken Sie mit der rechten Maustaste auf `CurrentVersion`, zeigen Sie auf New, wählen Sie die Option Schlüssel und benennen Sie den Schlüssel `RunOnce`.) Klicken Sie mit der rechten Maustaste auf den Schlüssel, zeigen Sie auf New und wählen Sie String Value. Geben Sie `Ec2Install` als den Namen und `C:\Temp\Ec2Install.exe -q` als die Daten ein.

   e. Wählen Sie den Schlüssel erneut aus und wählen Sie dann aus dem Menü File den Befehl Unload Hive.

7. (Optional) Wenn ihre temporäre Instance auf demselben AMI basiert wie die ursprüngliche Instance, müssen Sie die folgenden Schritte ausführen. Andernfalls werden Sie die ursprüngliche Instance nach der Wiederherstellung des Stamm-Volumes wegen einer Festplatten-Signaturkollision nicht booten können.

> **Warning**
>
> Im folgenden Verfahren wird beschrieben, wie Sie mit dem Registrierungs-Editor die Windows-Registrierung bearbeiten. Wenn Sie nicht mit der Windows-Registrierung vertraut sind oder nicht wissen, wie man Änderungen mit dem Registrierungs-Editor vornimmt, finden Sie weitere Informationen unter Konfigurieren der Registrierung.

a. Öffnen Sie eine Eingabeaufforderung, geben Sie regedit.exe ein und drücken Sie die Eingabetaste.

b. Wählen Sie im Registrierungs-Editor im Kontextmenü (rechte Maustaste) HKEY_LOCAL_MACHINE aus und dann Suchen.

c. Geben Sie Windows Boot Manager ein und klicken Sie dann auf Weiteresuchen.

d. Wählen Sie den Schlüssel aus `11000001`. Dieser Schlüssel ist ein gleichgeordnetes Element des Schlüssels, den Sie im vorherigen Schritt gefunden haben.

e. Klicken Sie im rechten Bereich auf `Element` und wählen Sie dann im Kontextmenü (rechte Maustaste) die Option Ändern aus.

f. Suchen Sie die 4-Byte-Datenträgersignatur bei Versatz 0x38 in den Daten. Kehren Sie die Bytes um, um die Datenträgersignatur zu erstellen, und notieren Sie diese. Die Datenträgersignatur der folgenden Daten lautet zum Beispiel `E9EB3AA5`:

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

g. Führen Sie in einem Eingabeaufforderungsfenster den folgenden Befehl aus, um Microsoft DiskPart zu starten.

```
diskpart
```

h. Führen Sie den folgenden DiskPart-Befehl aus, um das Volume auszuwählen. (Sie können mit dem Hilfsprogramm Datenträgerverwaltung überprüfen, ob die Datenträgernummer "1" ist.)

```
DISKPART> select disk 1
```

```
Disk 1 is now the selected disk.
```

i. Führen Sie den folgenden DiskPart-Befehl aus, um die Datenträgersignatur abzurufen.

```
DISKPART>  uniqueid disk

Disk ID: 0C764FA8
```

j. Wenn die im vorherigen Schritt angezeigte Datenträgersignatur nicht mit der zuvor notierten Datenträgersignatur von BCD übereinstimmt, verwenden Sie den folgenden DiskPart-Befehl, um die Datenträgersignatur entsprechend zu ändern:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

8. Bringen Sie das Laufwerk mit dem Datenträgerveraltung-Dienstprogramm offline.

> **Note**
>
> Das Laufwerk ist automatisch offline, wenn die temporäre Instance dasselbe Betriebssystem wie die betroffene Instance ausführt. Sie müssen es daher nicht manuell offline schalten.

9. Trennen Sie das Volume von der temporären Instance. Sie können die temporäre Instance beenden, falls Sie keine weitere Verwendung mehr dafür haben.
10. Stellen Sie das Stamm-Volume aus der betroffenen Instance wieder her, indem Sie es als anhänge `/dev/sda1`.
11. Starten Sie die betroffene Instance.

Wenn Sie mit der Instance verbunden sind, öffnen Sie auf der Instance einen Webbrowser und geben Sie den folgenden URL für den Metadaten-Server ein:

```
http://169.254.169.254/latest/meta-data/
```

Wenn Sie keine Verbindung zu dem Metadaten-Server herstellen können, versuchen Sie das Problem mit den folgenden Maßnahmen zu beheben.

- Laden Sie die aktuelle Version des EC2Config-Service herunter und installieren Sie sie. Weitere Informationen zum Installieren dieses Service erhalten Sie unter the section called “Installieren von EC2Config”.
- Überprüfen Sie, ob die Windows-Instance mit PV-Treibern von Red Hat ausgeführt wird. Wenn dies der Fall ist, führen Sie eine Treiberaktualisierung aus Citrix PV-Treiber durch. Weitere Informationen finden Sie unter the section called “Upgrade für PV-Treiber”.
- Überprüfen Sie, dass die Firewall-, IPSec- und Proxyeinstellungen nicht den ausgehenden Datenverkehr des Metadaten-Service (`169.254.169.254`) oder des AWS KMS-Servers (die Adressen sind in `TargetKMSServer`-Elementen in `C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml` angegeben) blockiert.
- Überprüfen Sie, ob Sie eine Route zu dem Metadaten-Server (`169.254.169.254`) haben, indem Sie den folgenden Befehl ausführen.

```
route print
```

- Überprüfen Sie, ob (allgemeine) Netzwerkprobleme vorliegen, die die Availability Zone für Ihre Instance betreffen. Gehen Sie zu http://status.aws.amazon.com/.

Windows kann nicht aktiviert werden

Windows-Instances verwenden Windows AWS KMS-Aktivierung. Sie können diese Meldung erhalten: `A problem occurred when Windows tried to activate. Error Code 0xC004F074`, wenn Ihre Instance nicht auf den AWS KMS-Server zugreifen kann. Windows muss alle 180 Tage aktiviert werden. EC2Config versucht, den AWS KMS-Server zu kontaktieren, bevor der Aktivierungszeitraum vorbei ist, um sicherzustellen, dass Windows durchgehend aktiviert bleibt.

Wenn Sie ein Problem bei der Windows-Aktivierung haben, gehen Sie wie folgt vor, um das Problem zu beheben.

Für EC2Config (Windows Server 2012 R2-AMIs und früher)

1. Laden Sie die aktuelle Version des EC2Config-Service herunter und installieren Sie sie. Weitere Informationen zum Installieren dieses Service erhalten Sie unter the section called “Installieren von EC2Config”.
2. Melden Sie sich an der Instance an und öffnen Sie die folgende Datei: `C:\Program Files\Amazon\Ec2ConfigService\Settings\config.xml`.

3. Suchen Sie in der Datei `config.xml` nach dem Plugin Ec2WindowsActivate. Ändern Sie den Status in Enabled und speichern Sie die Änderungen.
4. Starten Sie in dem Windows-Dienste-Snap-In den EC2Config-Service neu oder starten Sie die Instance neu.

Wenn dies das Aktivierungsproblem nicht behebt, führen Sie zusätzlich die folgenden Schritte aus.

1. Legen Sie das AWS KMS-Ziel fest: C:\> slmgr.vbs /skms 169.254.169.250:1688
2. Aktivieren Sie Windows: C:\> slmgr.vbs /ato

Für EC2Launch (Windows Server 2016-AMIs und höher)

1. Importieren des EC2Launch-Moduls über eine PowerShell-Eingabeaufforderung mit Administratorrechten:

```
PS C:\> Import-Module "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1"
```

2. Rufen Sie die Funktion Add-Routes auf, um die Liste der neuen Routen anzuzeigen:

```
PS C:\> Add-Routes
```

3. Rufen Sie die Set-ActivationSettings-Funktion auf:

```
PS C:\> Set-Activationsettings
```

4. Führen Sie das folgende Skript aus, um Windows zu aktivieren:

```
PS C:\> cscript "${env:SYSTEMROOT}\system32\slmgr.vbs" /ato
```

Sowohl für EC2Config als auch für EC2Launch: Wenn dann immer noch ein Aktivierungsfehler angezeigt wird, überprüfen Sie die folgenden Informationen.

- Überprüfen Sie, dass eine Route zu den AWS KMS-Servern vorhanden ist. Öffnen Sie die Datei `C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml` und suchen Sie die `TargetKMSServer`-Elemente. Führen Sie den folgenden Befehl aus und überprüfen Sie, ob die Adressen dieser AWS KMS-Server aufgelistet werden.

```
route print
```

- Überprüfen Sie, ob der AWS KMS-Clientschlüssel festgelegt ist. Führen Sie dazu den folgenden Befehl aus und überprüfen Sie die Ausgabe.

  ```
  C:\Windows\System32\slmgr.vbs /dlv
  ```

  Wenn die Ausgabe den Fehler Error: product key not found enthält, ist der AWS KMS-Clientschlüssel nicht festgelegt. Wenn der AWS KMS-Clientschlüssel nicht festgelegt ist, schlagen Sie den Clientschlüssel wie in dem folgenden Microsoft-Artikel beschrieben nach: AWS KMS-Client-Aktivierung und Produktschlüssel. Führen Sie dann den folgenden Befehl aus, um den AWS KMS-Clientschlüssel festzulegen.

  ```
  C:\Windows\System32\slmgr.vbs /ipk client_key
  ```

- Überprüfen Sie, ob für das System die Uhrzeit und die Zeitzone richtig eingestellt sind. Wenn Sie eine andere Zeitzone als UTC verwenden, fügen Sie den folgenden Registrierungsschlüssel hinzu und setzen ihn auf 1, um sicherzustellen, dass die Zeit korrekt ist: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\RealTimeIsUniversal`.
- Wenn die Windows-Firewall aktiviert ist, deaktivieren Sie sie vorübergehend mit dem folgenden Befehl.

  ```
  netsh advfirewall set allprofiles state off
  ```

Keine Original-Windows-Version (0x80070005)

Windows-Instances verwenden Windows AWS KMS-Aktivierung. Wenn eine Instance den Aktivierungsprozess nicht abschließen kann, wird gemeldet, dass diese Kopie von Windows keine Original-Windows-Version ist.

Versuchen Sie die Empfehlungen unter Windows kann nicht aktiviert werden.

Kein Terminal Server License-Server verfügbar, um eine Lizenz bereitzustellen

Standardmäßig ist Windows Server über Remotedesktopdienste für zwei gleichzeitige Benutzersitzungen lizenziert. Wenn Sie einen gleichzeitigen Zugriff auf Ihre Windows-Instance über Remotedesktopdienste für mehr als zwei Benutzer bereitstellen möchten, können Sie eine zusätzliche Remotedesktopdienst-CAL (Client Access License) erwerben und die Serverrollen Remotedesktop-Sitzungshost und Remotedesktop-Lizenzierungsserver installieren.

Überprüfen Sie, ob folgende Probleme auftreten:

- Sie haben die maximal zulässige Anzahl an gleichzeitigen RDP-Sitzungen überschritten.
- Sie haben die Windows-Remotedesktopdienste-Rolle installiert.
- Die Lizenz ist abgelaufen. Wenn die Lizenz abgelaufen ist, können Sie keine Verbindung mehr zu der Windows-Instance als Benutzer herstellen. Sie können die folgenden Gegenmaßnahmen versuchen:
  - Stellen Sie über die Befehlszeile unter Verwendung eines `/admin`-Parameters eine Verbindung zu der Instance her. Beispiel:

    ```
    mstsc /v:instance /admin
    ```

    Weitere Informationen finden Sie in dem folgenden Microsoft-Artikel: Access Remote Desktop Via Command Line.
  - Halten Sie die Instance an, lösen Sie die Amazon EBS-Volumes und hängen Sie sie an eine neue Instance in derselben Availability Zone an, um Ihre Daten wiederherzustellen.

„Einige Einstellungen werden von Ihrer Organisation verwaltet.“ (Windows 2019)

Bei Instances, die aus den neuesten Windows Server AMIs gestartet werden, wird möglicherweise die Windows Update-Dialogfeldmeldung „Einige Einstellungen werden von Ihrer Organisation verwaltet.“ angezeigt. Diese Meldung erscheint aufgrund von Änderungen in Windows Server und wirkt sich nicht auf das Verhalten von Windows Update oder Ihre Fähigkeit zur Verwendung von Einstellungen aus.

So entfernen Sie die Warnung

1. Öffnen Sie `gpedit.msc` und navigieren Sie zu Computerkonfiguration, Administrative Vorlagen, Windows-Komponenten, Windows-Updates. Bearbeiten Sie Automatisches Update konfigurieren und setzen Sie diese Option auf aktiviert.
2. Aktualisieren Sie in einer Eingabeaufforderung die Gruppenrichtlinie mit gpupdate /force.
3. Schließen Sie die Windows-Aktualisierungseinstellungen und öffnen Sie sie erneut. Ihnen wird in der obigen Nachricht mitgeteilt, das Ihre Einstellungen von Ihrer Organisation verwaltet werden, gefolgt von: „Wir laden Updates automatisch herunter, abgesehen von gemessenen Verbindungen (wofür Gebühren anfallen können). In diesem Fall laden wir die Updates, die für das reibungslose Ausführen von Windows erforderlich sind, automatisch herunter.“
4. Kehren Sie zu `gpedit.msc` zurück und setzen Sie die Gruppenrichtlinie zurück auf nicht konfiguriert. Führen Sie gpupdate /force erneut aus.
5. Schließen Sie die Befehlsaufforderung und warten Sie einige Minuten.
6. Öffnen Sie die Windows-Aktualisierungseinstellungen erneut. Sie sollten die Meldung „Einige Einstellungen werden von Ihrer Organisation verwaltet.“ nicht sehen.

Probleme bei Amazon-EC2-Windows-Instances beheben

Mithilfe der folgenden Tipps können Sie Probleme beheben, die bei der Verwendung von Amazon-EC2-Windows-Server-Instances auftreten.

Problembereiche

- AWS Systems Manager Sessions Manager kann nicht mit einer Windows Server 2025-Instance verbunden werden
- EBS-Volumes unter Windows Server 2016 und 2019 werden nicht initialisiert
- Starten einer EC2-Windows-Instance in die Verzeichnisdienstwiederherstellung (DSRM)
- Die Instance verliert die Netzwerkverbindung oder geplante Aufgaben werden nicht zu dem erwarteten Zeitpunkt ausgeführt
- Abrufen der Konsoleausgabe nicht möglich
- Windows Server 2012 R2 nicht im Netzwerk verfügbar
- Kollision der Festplattensignatur

AWS Systems Manager Sessions Manager kann nicht mit einer Windows Server 2025-Instance verbunden werden

Möglicherweise tritt beim Verbinden von AWS Systems Manager Sessions Manager mit einer Windows-Server-2025-Instance ein Problem auf. Um dieses Problem zu beheben, melden Sie sich bei der Instance an, navigieren Sie dann zu `Settings > Apps > Optional Features` und fügen Sie `WMIC` hinzu. Starten Sie den SSM-Agent-Service neu oder booten Sie die Instance neu und Sessions Manager sollte die Verbindung herstellen.

Sie können auch den folgenden PowerShell-Befehl verwenden, um dieselbe Aktion durchzuführen:

```
Start-Process -FilePath "$env:SystemRoot\system32\Dism.exe" -ArgumentList @('/
Online', '/Add-Capability', '/CapabilityName:WMIC~~~~') -Wait; Restart-Service -Name
 AmazonSSMAgent
```

EBS-Volumes unter Windows Server 2016 und 2019 werden nicht initialisiert

Instances, die über Amazon Machine Images (AMIs) für Windows Server 2016 und 2019 erstellt werden, nutzen für verschiedene Aufgaben beim Systemstart den Agent EC2Launch v1, darunter die Initialisierung von EBS-Volumes. Standardmäßig initialisiert EC2Launch v1 keine sekundären Volumes. Auf folgende Weise können Sie EC2Launch v1 jedoch zum automatischen Initialisieren dieser Datenträger konfigurieren.

Zuordnen von Laufwerkbuchstaben zu Volumes

1. Stellen Sie eine Verbindung zu der Instance her, um die Datei `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` in einem Texteditor zu öffnen und zu konfigurieren.
2. Geben Sie die Volume-Einstellungen wie folgt an:

```
{
"driveLetterMapping": [
 {
   "volumeName": "sample volume",
   "driveLetter": "H"
 }]
}
```

3. Speichern Sie Ihre Änderungen und schließen Sie die Datei.
4. Öffnen Sie Windows PowerShell und führen Sie mit dem folgenden Befehl das Skript von EC2Launch v1 aus, das die Datenträger initialisiert:

```
PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

Fügen Sie die Flag `-Schedule` wie folgt hinzu, um die Datenträger bei jedem Start der Instance zu initialisieren:

```
PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -
Schedule
```

Der Agent EC2Launch v1 kann Skripts zur Instance-Initialisierung wie etwa `initializeDisks.ps1` parallel zum Skript `InitializeInstance.ps1` ausführen. Wenn das Skript `InitializeInstance.ps1` die Instance neu startet, können dadurch andere geplante Aufgaben, die beim Start der Instance ausgeführt werden, unterbrochen werden. Um mögliche Konflikte zu vermeiden, sollten Sie dem Skript `initializeDisks.ps1` Logik hinzufügen, damit die Initialisierung der Instance zuerst abgeschlossen wird.

> **Note**
>
> Wenn das EC2Launch-Skript die Volumes nicht initialisiert, stellen Sie sicher, dass die Volumes online sind. Wenn die Volumes offline sind, führen Sie den folgenden Befehl aus, um alle Festplatten online zu schalten.
>
> ```
> PS C:\> Get-Disk | Where-Object IsOffline -Eq $True | Set-Disk -IsOffline
>  $False
> ```

Starten einer EC2-Windows-Instance in die Verzeichnisdienstwiederherstellung (DSRM)

Wenn eine Instance unter Microsoft Active Directory einen Systemausfall oder andere kritische Fehler hat, können Sie eine Fehlerbehebung für die Instance einleiten, indem Sie das System in einem besonderen, abgesicherten Modus starten, der als Verzeichnisdienstwiederherstellung (Directory

Services Restore Mode, DSRM) bezeichnet wird. In DSRM können Sie Active Directory reparieren oder wiederherstellen.

Treiberunterstützung für DSRM

Die Verfahren zur Aktivierung von DSRM und zum Starten der Instance richten sich nach den Treibern, die auf der Instance ausgeführt werden. In der EC2-Konsole können Sie im Systemprotokoll Detailinformationen zu den Treiberversionen für eine Instance anzeigen. In der folgenden Tabelle wird aufgeführt, welche Treiber für DSRM unterstützt werden.

Treiberversionen	DSRM-Unterstützung?	Nächste Schritte
Citrix PV 5.9	Nein	Stellen Sie die Instance anhand einer Sicherung wieder her. DSRM kann nicht aktiviert werden.
AWS PV 7.2.0	Nein	Zwar unterstützt dieser Treiber DSRM nicht, aber Sie können das Stamm-Volume von der Instance lösen, einen Snapshot des Volumes nehmen oder anhand des Volumes ein AMI erstellen und es dann einer anderen Instance in derselben Availability Zone als sekundäres Volume zuweisen. Anschließend können Sie DSRM (wie in diesem Abschnitt beschrieben) aktivieren.
AWS PV 7.2.2 und höher	Ja	Lösen Sie das Stamm-Volume, hängen Sie es an eine andere Instance an und aktivieren Sie DSRM (wie in diesem Abschnitt beschrieben).
Enhanced Networking	Ja	Lösen Sie das Stamm-Volume, hängen Sie es an eine andere Instance an und aktivieren Sie DSRM (wie in diesem Abschnitt beschrieben).

Weitere Informationen zum Aktivieren von Erweitertem Netzwerk finden Sie unter the section called “Elastic Network Adapter (ENA)”. Informationen zur Aktualisierung von AWS-PV-Treibern finden Sie unter Aktualisieren von PV-Treibern auf Windows-Instances.

Konfigurieren einer Instance zum Starten im Verzeichnisdienst-Wiederherstellungsmodus (DSRM)

EC2-Windows-Instances werden erst an das Netzwerk angebunden, wenn das Betriebssystem ausgeführt wird. Daher können Sie auch nicht die Taste F8 auf der Tastatur drücken, um eine Startoption auszuwählen. Sie müssen eine der folgenden Vorgehensweise verwenden, um eine EC2-Windows Server-Instance in DSRM zu starten.

Wenn Sie den Verdacht haben, dass Active Directory beschädigt ist, die Instance aber noch ausgeführt wird, können Sie die Instance über das Dialogfeld „Systemkonfiguration“ oder über die Eingabeaufforderung so konfigurieren, dass sie im Verzeichnisdienst-Wiederherstellungsmodus (DSRM) gestartet wird.

So starten Sie eine laufende Instance über das Dialogfeld „Systemkonfiguration“ im Verzeichnisdienst-Wiederherstellungsmodus (DSRM)

1. Geben Sie im Dialogfeld Ausführen den Befehl `msconfig` ein und drücken Sie die Eingabetaste.
2. Wählen Sie die Registerkarte Start aus.
3. Aktivieren Sie unter Startoptionen das Kontrollkästchen Abgesicherter Start.
4. Wählen Sie die Option Active Directory-Wiederherstellung und klicken Sie dann auf OK. Sie werden aufgefordert, den Server neu zu starten.

So starten Sie eine laufende Instance über die Eingabeaufforderung im Verzeichnisdienst-Wiederherstellungsmodus (DSRM)

Führen Sie in einem Eingabeaufforderungsfenster den folgenden Befehl aus:

```
bcdedit /set safeboot dsrepair
```

Wenn eine Instance offline und damit nicht erreichbar ist, müssen Sie das Stamm-Volume von der Instance lösen und es an eine andere Instance anbinden, um den Verzeichnisdienst-Wiederherstellungsmodus (DSRM) zu aktivieren.

So starten Sie eine Offline-Instance im Verzeichnisdienst-Wiederherstellungsmodus (DSRM)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.

3. Suchen Sie die betroffene Instance und wählen Sie sie aus. Wählen Sie Instance state (Instance-Status), Stop instance (Instance anhalten).
4. Wählen Sie Launch Instance (Instance starten) aus und erstellen Sie eine temporäre Instance in derselben Availability Zone wie die betroffene Instance. Wählen Sie einen Instance-Typ, der eine andere Version von Windows verwendet. Wenn Ihre Instance zum Beispiel Windows Server 2016 ist, wählen Sie eine Windows-Server-2019-Instance.

   > **Important**
   >
   > Wenn Sie die Instance nicht in der gleichen Availability Zone wie die betroffene Instance erstellen, können Sie das Stamm-Volume der betroffenen Instance nicht der neuen Instance anfügen.

5. Wählen Sie im Navigationsbereich Volumes aus.
6. Lokalisieren Sie das Stamm-Volume der betroffenen Instance. Trennen Sie das Volume und fügen Sie es der neu erstellten temporären Instance an. Fügen Sie es dem standardmäßigen Gerätenamen (xvdf) an.
7. Stellen Sie über Remote Desktop eine Verbindung mit der temporären Instance her und verwenden Sie anschließend das Dienstprogramm für die Datenträgerverwaltung, um das Volume verfügbar zu machen und es zu verwenden.
8. Öffnen Sie eine Eingabeaufforderung und führen Sie den folgenden Befehl aus. Ersetzen Sie dabei D durch den Laufwerkbuchstaben, den Sie dem gerade angefügten sekundären Volume zugewiesen haben:

   ```
   bcdedit /store D:\Boot\BCD /set {default} safeboot dsrepair
   ```

9. Wählen Sie im Dienstprogramm für die Datenträgerverwaltung das Laufwerk aus, das Sie zugewiesen haben, öffnen Sie das Kontextmenü (rechte Maustaste) und wählen Sie die Option Offline aus.
10. Trennen Sie in der EC2-Konsole das betroffene Volume von der temporären Instance und ordnen Sie es wieder der ursprünglichen Instance mit den Gerätenamen z `/dev/sda1`. Sie müssen diesen Gerätenamen angeben, um das Volume als Stamm-Volume hinzufügen zu können.
11. Starten Sie die Instance.

12. Wenn die Instance die Zustandsprüfungen in der EC2-Konsole bestanden hat, stellen Sie eine Remotedesktopverbindung mit der Instance her und überprüfen Sie, ob die Instance im Verzeichnisdienst-Wiederherstellungsmodus (DSRM) startet.
13. (Optional) Halten Sie die in dieser Prozedur erstellte temporäre Instance an bzw. löschen Sie sie.

Die Instance verliert die Netzwerkverbindung oder geplante Aufgaben werden nicht zu dem erwarteten Zeitpunkt ausgeführt

Wenn Sie Ihre Instance neu starten, und die Netzwerkverbindung Ihrer Instance getrennt wird, besteht die Möglichkeit, dass die Instance eine falsche Uhrzeit hat.

Windows-Instances verwenden standardmäßig UTC (Universal Time Coordinated). wenn Sie die Zeit für Ihre Instance auf eine andere Zeitzone einstellen und sie neu starten, ergibt sich ein Zeitversatz, und die Instance verliert vorübergehend ihre IP-Adresse. Die Instance erhält zwar nach einiger Zeit ihre Netzwerkverbindung zurück, aber dies kann einige Stunden dauern. Die Dauer, bis die Instance wieder ihre Netzwerkverbindung erhält, hängt von der Zeitdifferenz zwischen der UTC und der eingestellten Zeitzone ab.

Dasselbe Problem mit der Uhrzeit kann dazu führen, dass geplante Aufgaben zu einem unerwarteten Zeitpunkt ausgeführt werden. In diesem Fall werden die geplanten Aufgaben nicht zu dem erwarteten Zeitpunkt ausgeführt, weil die Instance eine andere Uhrzeit vorgeben.

Wenn Sie dauerhaft eine andere Zeitzone als UTC verwenden möchten, müssen Sie den Registrierungsschlüssel RealTimeIsUniversal einstellen. Ohne diesen Schlüssel verwendet die Instance nach jedem Neustart wieder UTC.

So beheben Sie Probleme bei der Zeiteinstellung, die zu einem Verlust der Netzwerkverbindung führen

1. Stellen Sie sicher, dass Sie die empfohlenen PV-Treiber verwenden. Weitere Informationen finden Sie unter the section called “Upgrade für PV-Treiber”.
2. Überprüfen Sie, ob der folgende Registrierungsschlüssel existiert und auf 1 festgelegt ist: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation \RealTimeIsUniversal

Abrufen der Konsoleausgabe nicht möglich

Bei Windows-Instances zeigt die Konsole der Instance die Ausgabe von Aufgaben, die während des Windows-Startprozesses durchgeführt werden. Wenn Windows erfolgreich gestartet wurde, wird als letzte Meldung protokollier `Windows is Ready to use`. Sie können in der Konsole auch die Meldungen des Ereignisprotokolls anzeigen, aber dieses Feature ist je nach Windows-Version möglicherweise deaktiviert. Weitere Informationen finden Sie unter the section called “Windows-Start-Agenten”.

Um die Ausgabe der Konsole für Ihre Instance mit der Amazon EC2-Konsole abzurufen, wählen Sie die Instance aus, wählen Sie dann Actions (Aktionen), Monitor and troubleshoot (Überwachung und Fehlerbehebung), Get System Log (Systemprotokoll abrufen). Um die Ausgabe der Konsole über die Befehlszeile abzurufen, verwenden Sie einen der folgenden Befehle: get-console-output (AWS CLI) oder Get-EC2ConsoleOutput (AWS Tools for Windows PowerShell).

Für Instances, auf denen Windows Server 2012 R2 und früher ausgeführt werden: Wenn die Ausgabe der Konsole leer ist, kann dies auf ein Problem mit dem EC2Config-Service hinweisen, beispielsweise auf Fehler in einer Konfigurationsdatei oder einen fehlerhaften Windows-Start. Um dieses Problem zu beheben, laden Sie die neueste Version von EC2Config herunter und installieren Sie sie. Weitere Informationen finden Sie unter the section called “Installieren von EC2Config”.

Windows Server 2012 R2 nicht im Netzwerk verfügbar

Weitere Informationen zur Fehlerbehebung einer Windows-Server-2012-R2-Instances, die im Netzwerk nicht verfügbar sind, finden Sie unter Windows Server 2012 R2 verliert nach dem Neustart der Instances die Netzwerk- und Speicherkonnektivität.

Kollision der Festplattensignatur

Sie können mithilfe von EC2Rescue for Windows Server nach Kollisionen der Festplattensignatur suchen und diese beheben. Oder Sie können Probleme mit der Festplattensignatur manuell beheben, indem Sie die folgenden Schritte ausführen:

> **Warning**
>
> Im folgenden Verfahren wird beschrieben, wie Sie mit dem Registrierungs-Editor die Windows-Registrierung bearbeiten. Wenn Sie nicht mit der Windows-Registrierung vertraut

sind oder nicht wissen, wie man Änderungen mit dem Registrierungs-Editor vornimmt, finden Sie weitere Informationen unter Konfigurieren der Registrierung.

1. Öffnen Sie eine Eingabeaufforderung, geben Sie regedit.exe ein und drücken Sie die Eingabetaste.
2. Wählen Sie im Registrierungs-Editor im Kontextmenü (rechte Maustaste) HKEY_LOCAL_MACHINE aus und dann Suchen.
3. Geben Sie Windows Boot Manager ein und klicken Sie dann auf Weiteresuchen.
4. Wählen Sie den Schlüssel aus `11000001`. Dieser Schlüssel ist ein gleichgeordnetes Element des Schlüssels, den Sie im vorherigen Schritt gefunden haben.
5. Klicken Sie im rechten Bereich auf `Element` und wählen Sie dann im Kontextmenü (rechte Maustaste) die Option Ändern aus.
6. Suchen Sie die 4-Byte-Datenträgersignatur bei Versatz 0x38 in den Daten. Dies ist die Boot Configuration Database-Signatur (BCD). Kehren Sie die Bytes um, um die Datenträgersignatur zu erstellen, und notieren Sie diese. Die Datenträgersignatur der folgenden Daten lautet zum Beispiel `E9EB3AA5`:

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

7. Führen Sie in einem Eingabeaufforderungsfenster den folgenden Befehl aus, um Microsoft DiskPart zu starten.

```
diskpart
```

8. Führen Sie den Befehl `select disk`-DiskPart aus und geben Sie die Festplattennummer für das Volume an, bei dem die Festplattensignaturkollision aufgetreten ist.

> **Tip**
>
> Verwenden Sie das Dienstprogramm Datenträgerverwaltung, um die Datenträgernummer des Datenträgers zu überprüfen, bei dem eine Kollision mit der Signatur aufgetreten ist. Öffnen Sie eine Eingabeaufforderung, geben Sie `compmgmt.msc` ein und

drücken Sie die Eingabetaste. Doppelklicken Sie im linken Navigationsbereich auf Datenträgerverwaltung. Verwenden Sie das Dienstprogramm Datenträgerverwaltung, um die Datenträgernummer des Datenträgers zu überprüfen, bei dem eine Kollision mit der Signatur aufgetreten ist.

```
DISKPART> select disk 1
Disk 1 is now the selected disk.
```

9. Führen Sie den folgenden DiskPart-Befehl aus, um die Datenträgersignatur abzurufen.

```
DISKPART>  uniqueid disk
Disk ID: 0C764FA8
```

10. Wenn die im vorherigen Schritt angezeigte Datenträgersignatur nicht mit der zuvor notierten Datenträgersignatur übereinstimmt, verwenden Sie den folgenden DiskPart-Befehl, um die Datenträgersignatur entsprechend zu ändern:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

Zurücksetzen des Windows-Administratorpassworts für eine Amazon-EC2-Windows-Instance

Wenn Sie nicht länger Zugriff auf die Amazon-EC2-Windows-Instance haben, da Sie das Windows-Administratorpasswort verloren haben oder das Passwort abgelaufen ist, können Sie das Passwort zurücksetzen.

> **Note**
>
> Es gibt ein AWS Systems Manager-Automatisierungsdokument, das automatisch die manuellen Schritte zum Zurücksetzen des lokalen Administratorpassworts anwendet. Weitere Informationen finden Sie unter Zurücksetzen von Passwörtern und SSH-Schlüsseln auf Amazon-EC2-Instances im AWS Systems Manager-Benutzerhandbuch.

Für die manuellen Methoden zum Zurücksetzen des Administratorpassworts wird EC2Launch v2, EC2Config oder EC2Launch verwendet.

- Verwenden Sie für alle unterstützten Windows-AMIs, die den EC2Launch-v2-Agenten enthalten, EC2Launch v2.
- Verwenden Sie für Windows-AMIs vor Windows Server 2016 den EC2Config-Service.
- Für AMIs ab Windows Server 2016 und höher verwenden Sie den EC2Launch-Service.

In diesen Verfahren wird auch beschrieben, wie Sie eine Verbindung zu einer Instance herstellen können, wenn Sie das Schlüsselpaar verloren haben, das zum Erstellen der Instance verwendet wurde. Amazon EC2 verwendet öffentliche Schlüssel, um Daten (z. B. ein Passwort) zu verschlüsseln. Mithilfe eines privaten Schlüssels werden die Daten entschlüsselt. Der öffentliche und der private Schlüssel werden als Schlüsselpaar bezeichnet. Bei Windows-Instances verwenden Sie ein Schlüsselpaar, um das Administratorpasswort zu erhalten und sich dann mit RDP anzumelden.

> **Note**
>
> Wenn Sie das lokale Administratorkonto für die Instance deaktiviert haben und Ihre Instance für Systems Manager konfiguriert ist, können Sie auch EC2Rescue und Run Command verwenden, um das lokale Administratorpasswort wieder zu aktivieren und zurückzusetzen. Weitere Informationen finden Sie unter Verwendung von EC2Rescue für Windows Server mit dem Systems-Manager-Befehl Run.

Inhalt

- Das Windows-Administratorpasswort für EC2-Instance mithilfe von EC2Launch v2 zurücksetzen
- Das Windows-Administratorpasswort für EC2-Instance mithilfe von EC2Launch zurücksetzen
- Das Windows-Administratorkennwort für die EC2-Instance mithilfe von EC2Config zurücksetzen

Das Windows-Administratorpasswort für EC2-Instance mithilfe von EC2Launch v2 zurücksetzen

Wenn Sie Ihr Windows-Administratorpasswort verloren haben und ein unterstütztes Windows-AMI verwenden, das EC2Launch v2 Agent enthält, können Sie EC2Launch v2 verwenden, um ein neues Passwort zu generieren.

Wenn Sie ein AMI für Windows Server 2016 oder höher verwenden, das EC2Launch v2 Agent nicht enthält, siehe Das Windows-Administratorpasswort für EC2-Instance mithilfe von EC2Launch zurücksetzen.

Wenn Sie eine ältere Version des Windows Server AMI als Windows Server 2016 verwenden, die EC2Launch v2-Agent nicht enthält, siehe Das Windows-Administratorkennwort für die EC2-Instance mithilfe von EC2Config zurücksetzen.

> **Note**
>
> Wenn Sie das lokale Administratorkonto für die Instance deaktiviert haben und Ihre Instance für Systems Manager konfiguriert ist, können Sie auch EC2Rescue und Run Command verwenden, um das lokale Administratorpasswort wieder zu aktivieren und zurückzusetzen. Weitere Informationen finden Sie unter Verwendung von EC2Rescue für Windows Server mit dem Systems-Manager-Befehl Run.

> **Note**
>
> Es gibt ein AWS Systems Manager-Automatisierungsdokument, das automatisch die manuellen Schritte zum Zurücksetzen des lokalen Administratorpassworts anwendet. Weitere Informationen finden Sie unter Zurücksetzen von Passwörtern und SSH-Schlüsseln auf Amazon-EC2-Instances im AWS Systems Manager-Benutzerhandbuch.

So setzen Sie Ihr Windows-Administratorpasswort mithilfe von EC2Launch v2 zurück:

- Schritt 1: Stellen Sie sicher, dass der EC2Launch-v2-Agent ausgeführt wird
- Schritt 2: Trennen des Stamm-Volumes von der Instance
- Schritt 3: Anfügen des Volumes an eine temporäre Instance
- Schritt 4: Löschen der .run-once-Datei
- Schritt 5: Starten Sie die Original-Instance neu

Schritt 1: Stellen Sie sicher, dass der EC2Launch-v2-Agent ausgeführt wird

Bevor Sie versuchen, das Administratorpasswort zurückzusetzen, überprüfen Sie, ob der EC2Launch-v2-Agent installiert ist und ausgeführt wird. Sie werden den EC2Launch-v2-Agent weiter unten in diesem Abschnitt zum Zurücksetzen des Administratorpassworts verwenden.

Sicherstellen, dass der EC2Launch-v2-Agent ausgeführt wird

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und anschließend die Instance aus, für die das Passwort zurückgesetzt werden muss. Diese Instance wird in diesem Verfahren als Original-Instance bezeichnet.
3. Wählen Sie Actions (Aktionen), Monitor and Troubleshoot (Überwachung und Fehlerbehebung), Get system log (Systemprotokoll abrufen).
4. Suchen Sie den Eintrag „EC2 Launch“, z. B. Launch: EC2Launch v2 service v2.0.124. Wenn dieser Eintrag angezeigt wird, wird der EC2Launch v2-Service ausgeführt.

   Wenn die System-Protokoll-Ausgabe leer ist oder wenn der EC2Launch-v2-Agent nicht ausgeführt wird, führen Sie auf der Instance eine Problembehebung mithilfe des Instance-Console-Screenshot-Services durch. Weitere Informationen finden Sie unter Aufnehmen eines Screenshots einer nicht erreichbaren Instance.

Schritt 2: Trennen des Stamm-Volumes von der Instance

Sie können ein Administratorpasswort mit EC2Launch v2 nicht zurücksetzen, wenn das Volume, auf dem das Passwort gespeichert ist, als Stamm-Volume an einer Instance angefügt ist. Sie müssen das Volume von der ursprünglichen Instance trennen, bevor Sie es als sekundäres Volume an eine temporäre Instance anfügen können.

Trennen des Stamm-Volumes von der Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Markieren Sie die Instance, deren Kennwort zurückgesetzt werden muss, und wählen Sie Instance-Status, Instance anhalten. Nachdem sich der Status der Instance in Angehalten geändert hat, können Sie mit dem nächsten Schritt fortfahren.
4. (Optional) Wenn Sie über den privaten Schlüssel verfügen, den Sie beim Start dieser Instance angegeben haben, fahren Sie mit dem nächsten Schritt fort. Führen Sie andernfalls die folgenden Schritte aus, um die Instance durch eine neue Instance mit einem neuen Schlüsselpaar zu ersetzen.

a. Erstellen Sie ein neues Schlüsselpaar mit der Amazon EC2-Konsole. Wenn der Name des neuen Schlüsselpaars dem des verlorenen privaten Schlüssels genau entsprechen soll, müssen Sie das vorhandene Schlüsselpaar erst löschen.

b. Wählen Sie die zu ersetzende Instance aus. Notieren Sie sich den Instance-Typ, die VPC, das Subnetz, die Sicherheitsgruppe und die IAM-Rolle der Instance.

c. Wählen Sie die Instance und wählen Sie Aktionen, Image und Vorlagen, Image erstellen aus. Geben Sie einen Namen und eine Beschreibung für das Image ein und wählen Sie anschließend Create image (Image erstellen) aus.

d. Wählen Sie im Navigationsbereich die Option AMIs. Warten Sie, bis sich der Status des Images auf verfügbar ändert. Wählen Sie dann das Image aus und wählen Sie Instance aus AMI starten.

e. Füllen Sie die Felder aus, um eine Instance zu starten, und stellen Sie sicher, dass Sie denselben Instance-Typ, dieselbe VPC, dasselbe Subnetz, dieselbe Sicherheitsgruppe und dieselbe IAM-Rolle wie die zu ersetzende Instance auswählen, und wählen Sie dann Instance starten.

f. Wenn Sie dazu aufgefordert werden, wählen Sie das Schlüsselpaar, das Sie für die neue Instance erstellt haben, und wählen Sie dann Instance starten.

g. (Optional) Wenn die ursprüngliche Instance über eine zugeordnete elastische IP-Adresse verfügt, sollten Sie sie auf die neue Instance übertragen. Wenn die ursprüngliche Instance zusätzlich zum Stamm-Volume EBS-Volumes enthält, übertragen Sie diese auf die neue Instance.

5. Trennen Sie das Stamm-Volume wie folgt von der ursprünglichen Instance:

a. Wählen Sie die ursprüngliche Instance und dann die Registerkarte Speicher aus. Notieren Sie sich den Namen des Root-Geräts unter Root-Gerätename. Suchen Sie unter Blockgeräte nach dem Volume mit diesem Gerätenamen und notieren Sie sich die Volume-ID.

b. Wählen Sie im Navigationsbereich Volumes aus.

c. Wählen Sie in der Liste der Volumes das im vorigen Schritt notierte Volume aus und wählen Sie anschließend Aktionen, Volume trennen. Nachdem der Status des Volumes in available (verfügbar) geändert wurde, fahren Sie mit dem nächsten Schritt fort.

6. Wenn Sie eine neue Instance erstellt haben, um Ihre ursprüngliche Instance zu ersetzen, können Sie die ursprüngliche Instance jetzt beenden. Sie wird nicht mehr benötigt. Für den Rest dieses Verfahrens gelten alle Verweise zur ursprünglichen Instance auf diese gerade erstellte Instance.

Schritt 3: Anfügen des Volumes an eine temporäre Instance

Starten Sie als Nächstes eine temporäre Instance, um das Volume als sekundäres Volume an sie anzufügen. Dies ist die Instance, die Sie zum Bearbeiten der Konfigurationsdatei verwenden.

So starten Sie eine temporäre Instance und fügen das Volume an

1. Starten Sie die temporäre Instance wie folgt:

   a. Wählen Sie im Navigationsbereich die Option Instances und dann Launch Instances (Instances starten) aus. Wählen Sie dann ein AMI aus.

   > **Important**
   >
   > Um Datenträger-Signaturkollisionen zu vermeiden, müssen Sie ein AMI für eine andere Version von Windows auswählen. Wenn die ursprüngliche Instance beispielsweise Windows Server 2019 verwendet, starten Sie die temporäre Instance mit dem Basis-AMI für Windows Server 2016.

   b. Übernehmen Sie den standardmäßigen Instance-Typen und wählen Next: Configure Instance Details (Weiter: Konfigurieren von Instance-Details) aus.

   c. Wählen Sie auf der Seite Configure Instance Details (Konfigurieren von Instance-Details) für Subnet (Subnetz) dieselbe Availability Zone aus wie für die ursprüngliche Instance und klicken Sie auf Review and Launch (Überprüfen und starten).

   > **Important**
   >
   > Die temporäre Instance muss sich in derselben Availability Zone befinden wie die ursprüngliche Instance. Wenn sich Ihre temporäre Instance in einer anderen Availability Zone befindet, können Sie ihr nicht das Stamm-Volume der ursprünglichen Instance anfügen.

   d. Klicken Sie auf der Seite Review Instance Launch auf Launch.

   e. Wenn Sie dazu aufgefordert werden, erstellen Sie ein neues Schlüsselpaar, laden Sie es an einen sicheren Speicherort auf Ihrem Computer herunter und wählen Sie dann Launch Instances (Instances starten) aus.

2. Fügen Sie das Volume der temporären Instance wie folgt als sekundäres Volume an:

a. Wählen Sie im Navigationsbereich Volumes und dann das Stamm-Volume aus, das Sie von der ursprünglichen Instance getrennt haben. Klicken Sie dann auf Actions (Aktionen) und Attach Volume (Volume anfügen).

b. Geben Sie im Dialogfeld Attach Volume (Volume anfügen) für Instances den Namen oder die ID der temporären Instance ein und wählen Sie die Instance aus der Liste aus.

c. Geben Sie für Device (Gerät) **`xvdf`** ein (wenn es noch nicht vorhanden ist) und wählen Sie Attach (Anfügen) aus.

Schritt 4: Löschen der .run-once-Datei

Sie müssen nun die Datei `.run-once` von dem mit der Instance verbundenen Offline-Volume löschen. Hierdurch wird EC2Launch v2 angewiesen, alle Aufgaben mit einer Häufigkeit von `once` auszuführen, wozu auch das Festlegen des Administratorpassworts gehört. Der Dateipfad auf dem sekundären Volume, das Sie angehängt haben, wird ähnlich sein wie `D:\ProgramData\Amazon\EC2Launch\state\.run-once`.

So löschen Sie die .run-once-Datei

1. Öffnen Sie das Serviceprogramm Datenträgerverwaltung und bringen Sie das Laufwerk mithilfe dieser Anweisungen online: Ein Amazon-EBS-Volume für die Verwendung verfügbar machen.
2. Suchen Sie die Datei `.run-once` auf dem Datenträger, den Sie online gestellt haben.
3. Löschen Sie die Datei „.run-once“.

> **Important**
>
> Alle Skripte, die einmal ausgeführt werden, werden durch diese Aktion ausgelöst.

Schritt 5: Starten Sie die Original-Instance neu

Nachdem Sie die `.run-once`-Datei gelöscht haben, fügen Sie das Volume wieder als Stamm-Volume an die ursprüngliche Instance an. Stellen Sie dann mithilfe ihres Schlüsselpaars eine Verbindung zur Instance her, um das Administratorpasswort abzurufen.

1. Fügen Sie das Volume wie folgt wieder der ursprünglichen Instance an:

a. Wählen Sie im Navigationsbereich Volumes und dann das Stamm-Volume aus, das Sie von der temporären Instance getrennt haben. Klicken Sie dann auf Actions (Aktionen) und Attach Volume (Volume anfügen).

b. Geben Sie im Dialogfeld Attach Volume (Volume anfügen) für Instances den Namen oder die ID der ursprünglichen Instance ein und wählen Sie die Instance aus.

c. Geben Sie für Device (Gerät) **`/dev/sda1`** ein.

d. Wählen Sie Attach (Anfügen) aus. Nachdem sich der Status des Volumes in `in-use` (In Verwendung) geändert hat, fahren Sie mit dem nächsten Schritt fort.

2. Wählen Sie im Navigationsbereich Instances aus. Wählen Sie die ursprüngliche Instance aus und klicken Sie auf Instance state (Instance-Zustand), Start instance (Instance starten). Nachdem sich der Status der Instance in `Running` (Wird ausgeführt) geändert hat, fahren Sie mit dem nächsten Schritt fort.

3. Rufen Sie Ihr neues Windows-Administratorpasswort mit dem privaten Schlüssel für das neue Schlüsselpaar ab und stellen Sie eine Verbindung mit der Instance her. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von RDP.

> **Important**
>
> Die Instance erhält eine neue öffentliche IP-Adresse, nachdem Sie sie stoppen und starten. Stellen Sie sicher, dass Sie sich mit der Instance unter deren aktuellem öffentlichen DNS-Namen verbinden. Weitere Informationen finden Sie unter Amazon-EC2-Instance-Statusänderungen.

4. (Optional) Sie können die temporäre Instance beenden, wenn Sie sie nicht mehr benötigen. Wählen Sie die temporäre Instance aus und klicken Sie auf Instance state (Instance-Zustand), Terminate instance (Instance beenden).

Das Windows-Administratorpasswort für EC2-Instance mithilfe von EC2Launch zurücksetzen

Wenn Sie das Windows-Administratorpasswort verloren haben und ein AMI für Windows Server 2016 oder höher verwenden, können Sie das EC2Rescue-Tool verwenden, das den EC2Launch-Service nutzt, um ein neues Passwort zu generieren.

Wenn Sie ein AMI mit Windows Server 2016 oder höher verwenden, das nicht den EC2Launch-v2-Agenten enthält, können Sie EC2Launch v2 verwenden, um ein neues Passwort zu generieren.

Wenn Sie ein Windows Server-AMI vor Windows Server 2016 verwenden, finden Sie weitere Informationen unter Das Windows-Administratorkennwort für die EC2-Instance mithilfe von EC2Config zurücksetzen.

Warning

Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

Note

Wenn Sie das lokale Administratorkonto für die Instance deaktiviert haben und Ihre Instance für Systems Manager konfiguriert ist, können Sie auch EC2Rescue und Run Command verwenden, um das lokale Administratorpasswort wieder zu aktivieren und zurückzusetzen. Weitere Informationen finden Sie unter Verwendung von EC2Rescue für Windows Server mit dem Systems-Manager-Befehl Run.

Note

Es gibt ein AWS Systems Manager-Automatisierungsdokument, das automatisch die manuellen Schritte zum Zurücksetzen des lokalen Administratorpassworts anwendet. Weitere Informationen finden Sie unter Zurücksetzen von Passwörtern und SSH-Schlüsseln auf Amazon-EC2-Instances im AWS Systems Manager-Benutzerhandbuch.

So setzen Sie Ihr Windows-Administratorpasswort mithilfe von EC2Launch zurück:

- Schritt 1: Trennen des Stamm-Volumes von der Instance
- Schritt 2: Anfügen des Volumes an eine temporäre Instance
- Schritt 3: Zurücksetzen des Administratorpassworts
- Schritt 4: Starten Sie die ursprüngliche Instance neu

Schritt 1: Trennen des Stamm-Volumes von der Instance

Sie können ein Administratorpasswort mit EC2Launch nicht zurücksetzen, wenn das Volume, auf dem das Passwort gespeichert ist, als Stamm-Volume an einer Instance angefügt ist. Sie müssen das Volume von der ursprünglichen Instance trennen, bevor Sie es als sekundäres Volume an eine temporäre Instance anfügen können.

Trennen des Stamm-Volumes von der Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Markieren Sie die Instance, deren Kennwort zurückgesetzt werden muss, und wählen Sie Instance-Status, Instance anhalten. Nachdem sich der Status der Instance in Angehalten geändert hat, können Sie mit dem nächsten Schritt fortfahren.
4. (Optional) Wenn Sie über den privaten Schlüssel verfügen, den Sie beim Start dieser Instance angegeben haben, fahren Sie mit dem nächsten Schritt fort. Führen Sie andernfalls die folgenden Schritte aus, um die Instance durch eine neue Instance mit einem neuen Schlüsselpaar zu ersetzen.

    a. Erstellen Sie ein neues Schlüsselpaar mit der Amazon EC2-Konsole. Wenn der Name des neuen Schlüsselpaars dem des verlorenen privaten Schlüssels genau entsprechen soll, müssen Sie das vorhandene Schlüsselpaar erst löschen.

    b. Wählen Sie die zu ersetzende Instance aus. Notieren Sie sich den Instance-Typ, die VPC, das Subnetz, die Sicherheitsgruppe und die IAM-Rolle der Instance.

    c. Wählen Sie die Instance und wählen Sie Aktionen, Image und Vorlagen, Image erstellen aus. Geben Sie einen Namen und eine Beschreibung für das Image ein und wählen Sie anschließend Create image (Image erstellen) aus.

    d. Wählen Sie im Navigationsbereich die Option AMIs. Warten Sie, bis sich der Status des Images auf verfügbar ändert. Wählen Sie dann das Image aus und wählen Sie Instance aus AMI starten.

    e. Füllen Sie die Felder aus, um eine Instance zu starten, und stellen Sie sicher, dass Sie denselben Instance-Typ, dieselbe VPC, dasselbe Subnetz, dieselbe Sicherheitsgruppe und dieselbe IAM-Rolle wie die zu ersetzende Instance auswählen, und wählen Sie dann Instance starten.

    f. Wenn Sie dazu aufgefordert werden, wählen Sie das Schlüsselpaar, das Sie für die neue Instance erstellt haben, und wählen Sie dann Instance starten.

g. (Optional) Wenn die ursprüngliche Instance über eine zugeordnete elastische IP-Adresse verfügt, sollten Sie sie auf die neue Instance übertragen. Wenn die ursprüngliche Instance zusätzlich zum Stamm-Volume EBS-Volumes enthält, übertragen Sie diese auf die neue Instance.

5. Trennen Sie das Stamm-Volume wie folgt von der ursprünglichen Instance:

   a. Wählen Sie die ursprüngliche Instance und dann die Registerkarte Speicher aus. Notieren Sie sich den Namen des Root-Geräts unter Root-Gerätename. Suchen Sie unter Blockgeräte nach dem Volume mit diesem Gerätenamen und notieren Sie sich die Volume-ID.

   b. Wählen Sie im Navigationsbereich Volumes aus.

   c. Wählen Sie in der Liste der Volumes das im vorigen Schritt notierte Volume aus und wählen Sie anschließend Aktionen, Volume trennen. Nachdem der Status des Volumes in available (verfügbar) geändert wurde, fahren Sie mit dem nächsten Schritt fort.

6. Wenn Sie eine neue Instance erstellt haben, um Ihre ursprüngliche Instance zu ersetzen, können Sie die ursprüngliche Instance jetzt beenden. Sie wird nicht mehr benötigt. Für den Rest dieses Verfahrens gelten alle Verweise zur ursprünglichen Instance auf diese gerade erstellte Instance.

Schritt 2: Anfügen des Volumes an eine temporäre Instance

Starten Sie als Nächstes eine temporäre Instance, um das Volume als sekundäres Volume an sie anzufügen. Dies ist die Instance, mit der Sie EC2Launch ausführen.

So starten Sie eine temporäre Instance und fügen das Volume an

1. Starten Sie die temporäre Instance wie folgt:

   a. Wählen Sie im Navigationsbereich die Option Instances und dann Launch Instances (Instances starten) aus. Wählen Sie dann ein AMI aus.

> **Important**
>
> Um Datenträger-Signaturkollisionen zu vermeiden, müssen Sie ein AMI für eine andere Version von Windows auswählen. Wenn die ursprüngliche Instance beispielsweise Windows Server 2019 verwendet, starten Sie die temporäre Instance mit dem Basis-AMI für Windows Server 2016.

b. Übernehmen Sie den standardmäßigen Instance-Typen und wählen Next: Configure Instance Details (Weiter: Konfigurieren von Instance-Details) aus.

c. Wählen Sie auf der Seite Configure Instance Details (Konfigurieren von Instance-Details) für Subnet (Subnetz) dieselbe Availability Zone aus wie für die ursprüngliche Instance und klicken Sie auf Review and Launch (Überprüfen und starten).

> **Important**
>
> Die temporäre Instance muss sich in derselben Availability Zone befinden wie die ursprüngliche Instance. Wenn sich Ihre temporäre Instance in einer anderen Availability Zone befindet, können Sie ihr nicht das Stamm-Volume der ursprünglichen Instance anfügen.

d. Klicken Sie auf der Seite Review Instance Launch auf Launch.

e. Wenn Sie dazu aufgefordert werden, erstellen Sie ein neues Schlüsselpaar, laden Sie es an einen sicheren Speicherort auf Ihrem Computer herunter und wählen Sie dann Launch Instances (Instances starten) aus.

2. Fügen Sie das Volume der temporären Instance wie folgt als sekundäres Volume an:

a. Wählen Sie im Navigationsbereich Volumes und dann das Stamm-Volume aus, das Sie von der ursprünglichen Instance getrennt haben. Klicken Sie dann auf Actions (Aktionen) und Attach Volume (Volume anfügen).

b. Geben Sie im Dialogfeld Attach Volume (Volume anfügen) für Instances den Namen oder die ID der temporären Instance ein und wählen Sie die Instance aus der Liste aus.

c. Geben Sie für Device (Gerät) **`xvdf`** ein (wenn es noch nicht vorhanden ist) und wählen Sie Attach (Anfügen) aus.

Schritt 3: Zurücksetzen des Administratorpassworts

Verbinden Sie sich als Nächstes mit der temporären Instance und setzen Sie mit EC2Launch das Administratorpasswort zurück.

Zum Zurücksetzen des Administratorpassworts

1. Stellen Sie eine Verbindung mit der temporären Instance her und verwenden Sie das EC2Rescue for Windows Server-Tool auf der Instance, um das Administratorpasswort wie folgt zurückzusetzen:

a. Laden Sie die Zip-Datei EC2Rescue for Windows Server herunter, extrahieren Sie den Inhalt und führen Sie EC2Rescue.exe aus.

b. Lesen Sie die Lizenzvereinbarung im Bildschirm License Agreement (Lizenzvereinbarung). Wenn Sie den Bedingungen zustimmen, wählen Sie I Agree (Ich stimme zu).

c. Klicken Sie im Bildschirm Welcome to EC2Rescue for Windows Server (Willkommen bei EC2Rescue for Windows Server) auf Next (Weiter).

d. Wählen Sie im Bildschirm Select mode (Modus auswählen) die Option Offline instance (Offline-Instance).

e. Wählen Sie im Bildschirm Select a disk (Datenträger auswählen) das Gerät xvdf aus und klicken Sie auf Next (Weiter).

f. Bestätigen Sie die Festplattenauswahl und wählen Sie Yes aus.

g. Nachdem das Volume geladen wurde, klicken Sie auf OK.

h. Wählen Sie im Bildschirm Select Offline Instance Option (Offline-Instance-Option auswählen) die Option Diagnose and Rescue (Diagnose und Datenrettung).

i. Überprüfen Sie die Informationen im Bildschirm Summary (Übersicht) und klicken Sie auf Next (Weiter).

j. Wählen Sie im Bildschirm Detected possible issues (Mögliche Probleme erkennen) die Option Reset Administrator Password (Administratorpasswort zurücksetzen) und klicken Sie auf Next (Weiter).

k. Klicken Sie im Bildschirm Confirm (Bestätigen) auf Rescue (Datenrettung) und danach auf OK.

l. Klicken Sie im Bildschirm Done (Fertig) auf Finish (Beenden).

m. Schließen Sie das Tool EC2Rescue for Windows Server, trennen Sie die Verbindung mit der temporären Instance und kehren Sie zur Amazon EC2-Konsole zurück.

2. Trennen Sie das sekundäre Volume (`xvdf`) wie folgt von der temporären Instance:

a. Klicken Sie im Navigationsbereich auf Instances und wählen Sie die temporäre Instance aus.

b. Notieren Sie sich auf der Registerkarte Storage (Speicher) der temporären Instance die ID des EBS-Volumes, die als xvdf aufgelistet wird.

c. Wählen Sie im Navigationsbereich Volumes aus.

d. Wählen Sie in der Liste der Volumes das im vorigen Schritt notierte Volume aus und wählen Sie anschließend Actions (Aktionen), Detach Volume (Volume trennen). Nachdem der

Status des Volumes in available (verfügbar) geändert wurde, fahren Sie mit dem nächsten Schritt fort.

Schritt 4: Starten Sie die ursprüngliche Instance neu

Nachdem Sie das Administratorpasswort mit EC2Launch zurückgesetzt haben, fügen Sie das Volume wieder als Stamm-Volume an die ursprüngliche Instance an. Stellen Sie dann mithilfe ihres Schlüsselpaars eine Verbindung zur Instance her, um das Administratorpasswort abzurufen.

So starten Sie die ursprüngliche Instance neu

1. Fügen Sie das Volume wie folgt wieder der ursprünglichen Instance an:

   a. Wählen Sie im Navigationsbereich Volumes und dann das Stamm-Volume aus, das Sie von der temporären Instance getrennt haben. Klicken Sie dann auf Actions (Aktionen) und Attach Volume (Volume anfügen).

   b. Geben Sie im Dialogfeld Attach Volume (Volume anfügen) für Instances den Namen oder die ID der ursprünglichen Instance ein und wählen Sie die Instance aus.

   c. Geben Sie für Device (Gerät) **`/dev/sda1`** ein.

   d. Wählen Sie Attach (Anfügen) aus. Nachdem sich der Status des Volumes in `in-use` (In Verwendung) geändert hat, fahren Sie mit dem nächsten Schritt fort.

2. Wählen Sie im Navigationsbereich Instances aus. Wählen Sie die ursprüngliche Instance aus und klicken Sie auf Instance state (Instance-Zustand), Start instance (Instance starten). Nachdem sich der Status der Instance in `Running` (Wird ausgeführt) geändert hat, fahren Sie mit dem nächsten Schritt fort.

3. Rufen Sie Ihr neues Windows-Administratorpasswort mit dem privaten Schlüssel für das neue Schlüsselpaar ab und stellen Sie eine Verbindung mit der Instance her. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von RDP.

4. (Optional) Sie können die temporäre Instance beenden, wenn Sie sie nicht mehr benötigen. Wählen Sie die temporäre Instance aus und klicken Sie auf Instance state (Instance-Zustand), Terminate instance (Instance beenden).

Das Windows-Administratorkennwort für die EC2-Instance mithilfe von EC2Config zurücksetzen

Wenn Sie das Windows-Administratorpasswort verloren haben und ein Windows-AMI für Windows Server 2016 verwenden, können Sie EC2Config-Agent verwenden, um ein neues Passwort zu generieren.

Wenn Sie ein AMI für Windows Server 2016 oder höher verwenden, siehe Das Windows-Administratorpasswort für EC2-Instance mithilfe von EC2Launch zurücksetzen. Andernfalls können Sie das EC2Rescue-Tool verwenden, das den EC2Launch-Service nutzt, um ein neues Kennwort zu generieren.

> **Note**
>
> Wenn Sie das lokale Administratorkonto für die Instance deaktiviert haben und Ihre Instance für Systems Manager konfiguriert ist, können Sie auch EC2Rescue und Run Command verwenden, um das lokale Administratorpasswort wieder zu aktivieren und zurückzusetzen. Weitere Informationen finden Sie unter Verwendung von EC2Rescue für Windows Server mit dem Systems-Manager-Befehl Run.

> **Note**
>
> Es gibt ein AWS Systems Manager-Automatisierungsdokument, das automatisch die manuellen Schritte zum Zurücksetzen des lokalen Administratorpassworts anwendet. Weitere Informationen finden Sie unter Zurücksetzen von Passwörtern und SSH-Schlüsseln auf Amazon-EC2-Instances im AWS Systems Manager-Benutzerhandbuch.

So setzen Sie Ihr Windows-Administratorpasswort mithilfe von EC2Config zurück:

- Schritt 1: Überprüfen, ob der EC2Config-Service ausgeführt wird
- Schritt 2: Trennen des Stamm-Volumes von der Instance
- Schritt 3: Anfügen des Volumes an eine temporäre Instance
- Schritt 4: Bearbeiten der Konfigurationsdatei
- Schritt 5: Starten Sie die Original-Instance neu

Schritt 1: Überprüfen, ob der EC2Config-Service ausgeführt wird

Bevor Sie versuchen, das Administratorpasswort zurückzusetzen, überprüfen Sie, ob der EC2Config-Service installiert ist und ausgeführt wird. Sie werden den EC2Config-Service weiter unten in diesem Abschnitt zum Zurücksetzen des Administratorpassworts verwenden.

So überprüfen Sie, ob der EC2Config-Service ausgeführt wird

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und anschließend die Instance aus, für die das Passwort zurückgesetzt werden muss. Diese Instance wird in diesem Verfahren als Original-Instance bezeichnet.
3. Wählen Sie Actions (Aktionen), Monitor and Troubleshoot (Überwachung und Fehlerbehebung), Get system log (Systemprotokoll abrufen).
4. Suchen Sie den EC2 Agent-Eintrag, z. B. EC2 Agent: Ec2Config Service v3.18.1118. Wenn Sie diesen Eintrag sehen, läuft der EC2Config-Service.

   Wenn die System-Log-Ausgabe leer ist oder wenn der EC2Config-Service nicht läuft, führen Sie auf der Instance eine Problembehebung mithilfe des Instance Console Screenshot-Service durch. Weitere Informationen finden Sie unter Aufnehmen eines Screenshots einer nicht erreichbaren Instance.

Schritt 2: Trennen des Stamm-Volumes von der Instance

Sie können ein Administratorpasswort mit EC2Config nicht zurücksetzen, wenn das Volume, auf dem das Passwort gespeichert ist, als Stamm-Volume an einer Instance angefügt ist. Sie müssen das Volume von der ursprünglichen Instance trennen, bevor Sie es als sekundäres Volume an eine temporäre Instance anfügen können.

Trennen des Stamm-Volumes von der Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Markieren Sie die Instance, deren Kennwort zurückgesetzt werden muss, und wählen Sie Instance-Status, Instance anhalten. Nachdem sich der Status der Instance in Angehalten geändert hat, können Sie mit dem nächsten Schritt fortfahren.

4. (Optional) Wenn Sie über den privaten Schlüssel verfügen, den Sie beim Start dieser Instance angegeben haben, fahren Sie mit dem nächsten Schritt fort. Führen Sie andernfalls die folgenden Schritte aus, um die Instance durch eine neue Instance mit einem neuen Schlüsselpaar zu ersetzen.

   a. Erstellen Sie ein neues Schlüsselpaar mit der Amazon EC2-Konsole. Wenn der Name des neuen Schlüsselpaars dem des verlorenen privaten Schlüssels genau entsprechen soll, müssen Sie das vorhandene Schlüsselpaar erst löschen.

   b. Wählen Sie die zu ersetzende Instance aus. Notieren Sie sich den Instance-Typ, die VPC, das Subnetz, die Sicherheitsgruppe und die IAM-Rolle der Instance.

   c. Wählen Sie die Instance und wählen Sie Aktionen, Image und Vorlagen, Image erstellen aus. Geben Sie einen Namen und eine Beschreibung für das Image ein und wählen Sie anschließend Create image (Image erstellen) aus.

   d. Wählen Sie im Navigationsbereich die Option AMIs. Warten Sie, bis sich der Status des Images auf verfügbar ändert. Wählen Sie dann das Image aus und wählen Sie Instance aus AMI starten.

   e. Füllen Sie die Felder aus, um eine Instance zu starten, und stellen Sie sicher, dass Sie denselben Instance-Typ, dieselbe VPC, dasselbe Subnetz, dieselbe Sicherheitsgruppe und dieselbe IAM-Rolle wie die zu ersetzende Instance auswählen, und wählen Sie dann Instance starten.

   f. Wenn Sie dazu aufgefordert werden, wählen Sie das Schlüsselpaar, das Sie für die neue Instance erstellt haben, und wählen Sie dann Instance starten.

   g. (Optional) Wenn die ursprüngliche Instance über eine zugeordnete elastische IP-Adresse verfügt, sollten Sie sie auf die neue Instance übertragen. Wenn die ursprüngliche Instance zusätzlich zum Stamm-Volume EBS-Volumes enthält, übertragen Sie diese auf die neue Instance.

5. Trennen Sie das Stamm-Volume wie folgt von der ursprünglichen Instance:

   a. Wählen Sie die ursprüngliche Instance und dann die Registerkarte Speicher aus. Notieren Sie sich den Namen des Root-Geräts unter Root-Gerätename. Suchen Sie unter Blockgeräte nach dem Volume mit diesem Gerätenamen und notieren Sie sich die Volume-ID.

   b. Wählen Sie im Navigationsbereich Volumes aus.

c. Wählen Sie in der Liste der Volumes das im vorigen Schritt notierte Volume aus und wählen Sie anschließend Aktionen, Volume trennen. Nachdem der Status des Volumes in available (verfügbar) geändert wurde, fahren Sie mit dem nächsten Schritt fort.

6. Wenn Sie eine neue Instance erstellt haben, um Ihre ursprüngliche Instance zu ersetzen, können Sie die ursprüngliche Instance jetzt beenden. Sie wird nicht mehr benötigt. Für den Rest dieses Verfahrens gelten alle Verweise zur ursprünglichen Instance auf diese gerade erstellte Instance.

Schritt 3: Anfügen des Volumes an eine temporäre Instance

Starten Sie als Nächstes eine temporäre Instance, um das Volume als sekundäres Volume an sie anzufügen. Dies ist die Instance, die Sie zum Bearbeiten der Konfigurationsdatei verwenden.

So starten Sie eine temporäre Instance und fügen das Volume an

1. Starten Sie die temporäre Instance wie folgt:

   a. Wählen Sie im Navigationsbereich die Option Instances und dann Launch Instances (Instances starten) aus. Wählen Sie dann ein AMI aus.

   > **Important**
   >
   > Um Datenträger-Signaturkollisionen zu vermeiden, müssen Sie ein AMI für eine andere Version von Windows auswählen. Wenn die ursprüngliche Instance beispielsweise Windows Server 2019 verwendet, starten Sie die temporäre Instance mit dem Basis-AMI für Windows Server 2016.

   b. Übernehmen Sie den standardmäßigen Instance-Typen und wählen Next: Configure Instance Details (Weiter: Konfigurieren von Instance-Details) aus.

   c. Wählen Sie auf der Seite Configure Instance Details (Konfigurieren von Instance-Details) für Subnet (Subnetz) dieselbe Availability Zone aus wie für die ursprüngliche Instance und klicken Sie auf Review and Launch (Überprüfen und starten).

   > **Important**
   >
   > Die temporäre Instance muss sich in derselben Availability Zone befinden wie die ursprüngliche Instance. Wenn sich Ihre temporäre Instance in einer

anderen Availability Zone befindet, können Sie ihr nicht das Stamm-Volume der ursprünglichen Instance anfügen.

d. Klicken Sie auf der Seite Review Instance Launch auf Launch.

e. Wenn Sie dazu aufgefordert werden, erstellen Sie ein neues Schlüsselpaar, laden Sie es an einen sicheren Speicherort auf Ihrem Computer herunter und wählen Sie dann Launch Instances (Instances starten) aus.

2. Fügen Sie das Volume der temporären Instance wie folgt als sekundäres Volume an:

   a. Wählen Sie im Navigationsbereich Volumes und dann das Stamm-Volume aus, das Sie von der ursprünglichen Instance getrennt haben. Klicken Sie dann auf Actions (Aktionen) und Attach Volume (Volume anfügen).

   b. Geben Sie im Dialogfeld Attach Volume (Volume anfügen) für Instances den Namen oder die ID der temporären Instance ein und wählen Sie die Instance aus der Liste aus.

   c. Geben Sie für Device (Gerät) **`xvdf`** ein (wenn es noch nicht vorhanden ist) und wählen Sie Attach (Anfügen) aus.

Schritt 4: Bearbeiten der Konfigurationsdatei

Nachdem Sie das Volume der temporären Instance als sekundäres Volume angefügt haben, ändern Sie das `Ec2SetPassword`-Plugin in der Konfigurationsdatei.

So bearbeiten Sie die Konfigurationsdatei

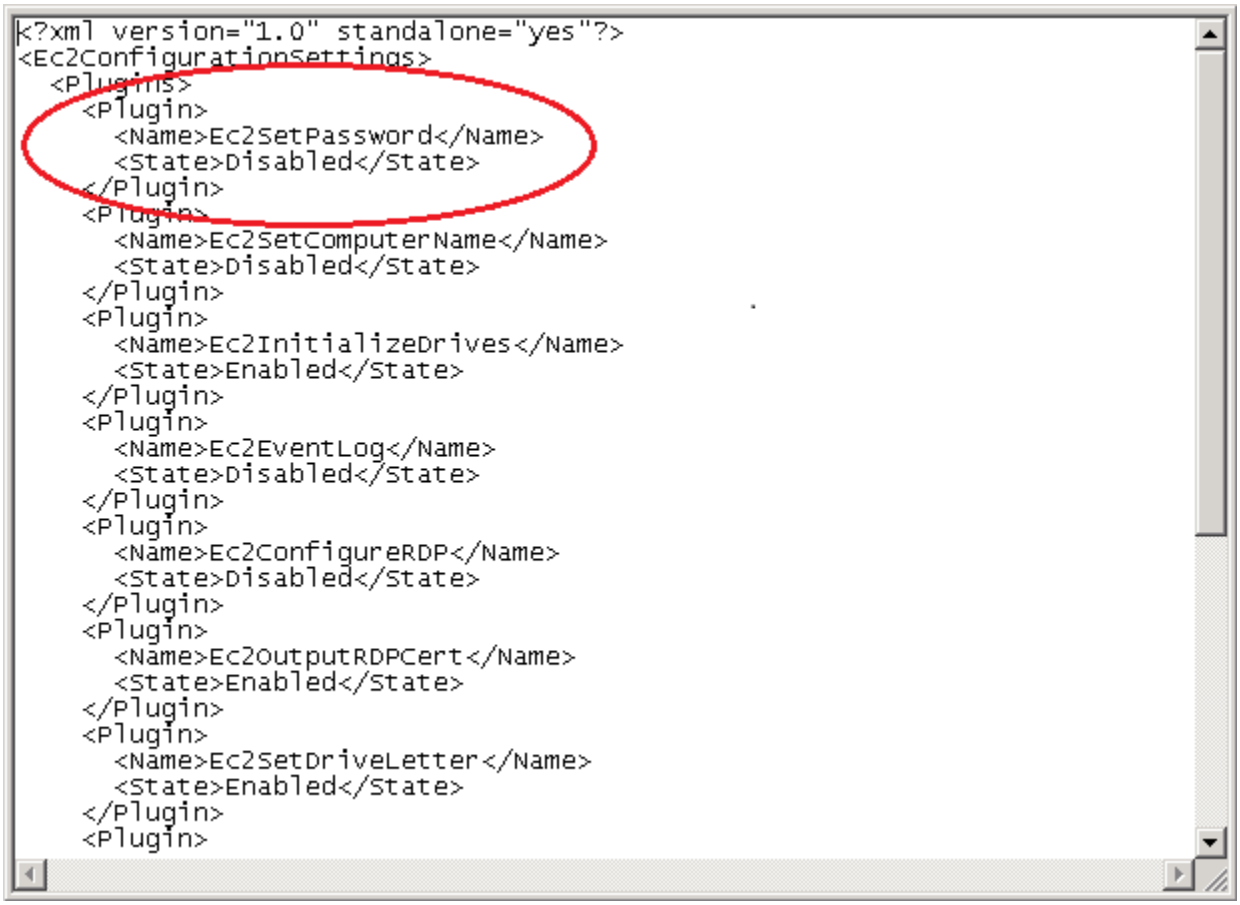
1. Bearbeiten Sie die Konfigurationsdatei auf dem sekundären Volume wie folgt über die temporäre Instance:

   a. Starten Sie die temporäre Instance und stellen Sie eine Verbindung mit ihr her.

   b. Gehen Sie wie folgt vor, um das Laufwerk online zu bringen: Amazon-EBS-Volume für die Verwendung verfügbar machen.

   c. Navigieren Sie zum sekundären Volume und öffnen Sie `\Program Files\Amazon \Ec2ConfigService\Settings\config.xml` mithilfe eines Texteditors, wie Notepad.

   d. Suchen Sie am Anfang der Datei das Plugin mit dem Namen `Ec2SetPassword`, wie im Screenshot dargestellt. Ändern Sie den Status von `Disabled` in `Enabled` und speichern Sie die Datei.



2. Nachdem Sie die Konfigurationsdatei bearbeitet haben, trennen Sie das sekundäre Volume wie folgt von der temporären Instance:

   a. Mit dem Disk Management (Datenträgerverwaltung)-Tool bringen Sie das Volume offline.

   b. Trennen Sie es von der temporären Instance und kehren Sie zur Amazon EC2-Konsole zurück.

   c. Wählen Sie im Navigationsbereich Volumes und dann das Stamm-Volume aus. Klicken Sie dann auf Actions (Aktionen) und Detach Volume (Volume trennen). Nachdem der Status der Volume zu available (verfügbar) geändert wurde, fahren Sie fort mit dem nächsten Schritt.

Schritt 5: Starten Sie die Original-Instance neu

Nachdem Sie die Konfigurationsdatei bearbeitet haben, fügen Sie das Volume wieder als Stamm-Volume an die ursprüngliche Instance an. Stellen Sie dann mithilfe ihres Schlüsselpaars eine Verbindung zur Instance her, um das Administratorpasswort abzurufen.

1. Fügen Sie das Volume wie folgt wieder der ursprünglichen Instance an:

a. Wählen Sie im Navigationsbereich Volumes und dann das Stamm-Volume aus, das Sie von der temporären Instance getrennt haben. Klicken Sie dann auf Actions (Aktionen) und Attach Volume (Volume anfügen).

b. Geben Sie im Dialogfeld Attach Volume (Volume anfügen) für Instances den Namen oder die ID der ursprünglichen Instance ein und wählen Sie die Instance aus.

c. Geben Sie für Device (Gerät) **`/dev/sda1`** ein.

d. Wählen Sie Attach (Anfügen) aus. Nachdem sich der Status des Volumes in `in-use` (In Verwendung) geändert hat, fahren Sie mit dem nächsten Schritt fort.

2. Wählen Sie im Navigationsbereich Instances aus. Wählen Sie die ursprüngliche Instance aus und klicken Sie auf Instance state (Instance-Zustand), Start instance (Instance starten). Nachdem sich der Status der Instance in `Running` (Wird ausgeführt) geändert hat, fahren Sie mit dem nächsten Schritt fort.

3. Rufen Sie Ihr neues Windows-Administratorpasswort mit dem privaten Schlüssel für das neue Schlüsselpaar ab und stellen Sie eine Verbindung mit der Instance her. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von RDP.

> **Important**
>
> Die Instance erhält eine neue öffentliche IP-Adresse, nachdem Sie sie stoppen und starten. Stellen Sie sicher, dass Sie sich mit der Instance unter deren aktuellem öffentlichen DNS-Namen verbinden. Weitere Informationen finden Sie unter Amazon-EC2-Instance-Statusänderungen.

4. (Optional) Sie können die temporäre Instance beenden, wenn Sie sie nicht mehr benötigen. Wählen Sie die temporäre Instance aus und klicken Sie auf Instance state (Instance-Zustand), Terminate instance (Instance beenden).

Behebung von Sysprep-Problemen mit Amazon Windows-Instances EC2

Wenn Sie Probleme bei der Vorbereitung von Images haben oder Fehlermeldungen ausgegeben werden, prüfen Sie folgende Protokolle. Der Speicherort der Protokolle hängt davon ab, ob Sie EC2 Config, EC2 Launch v1 oder EC2 Launch v2 mit Sysprep ausführen.

- `%WINDIR%\Panther\Unattendgc`(EC2Config, EC2 Launch v1 und EC2 Launch v2)

- `%WINDIR%\System32\Sysprep\Panther`(EC2Config, EC2 Launch v1 und EC2 Launch v2)
- `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt`(Nur EC2 Config)
- `C:\ProgramData\Amazon\Ec2Config\Logs`(Nur EC2 Config)
- `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\EC2Launch.log`(Nur Version 1 EC2 starten)
- `%ProgramData%\Amazon\EC2Launch\log\agent.log`(Nur Version 2 EC2 starten)

Wenn bei der Vorbereitung von Images mit Sysprep eine Fehlermeldung ausgegeben wird, ist das Betriebssystem möglicherweise nicht erreichbar. Um die Protokolldateien zu überprüfen, halten Sie die Instance an, fügen Sie das Root-Volume einer anderen fehlerfreien Instance als sekundäres Volume an und prüfen Sie anschließend die zuvor erwähnten Protokolle für das sekundäre Volume. Weitere Informationen zum Zweck der Protokolldateien nach Namen finden Sie unter Windows Setup-bezogene Protokolldateien in der Microsoft-Dokumentation.

Wenn in der Unattendgc-Protokolldatei Fehler aufgeführt sind, verwenden Sie das Fehlersuchtool von Microsoft, um weitere Details zum Fehler zu erfahren. Das folgende in der Unattendgc-Protokolldatei aufgeführte Problem ergibt sich normalerweise aus einem oder mehreren fehlerhaften Benutzerprofilen in der Instance:

```
Error [Shell Unattend] _FindLatestProfile failed (0x80070003) [gle=0x00000003]
Error [Shell Unattend] CopyProfile failed (0x80070003) [gle=0x00000003]
```

Dieses Problem lässt sich auf zwei Arten lösen:

Option 1

Suchen Sie mit Regedit in der Instance nach folgendem Schlüssel. Überprüfen Sie, ob Profilregistrierungsschlüssel für gelöschte Benutzer vorhanden sind.

`[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\`

Option 2

1. Aktualisieren Sie die relevante Datei wie folgt:
   - Windows Server 2012 R2 und früher — Bearbeiten Sie die EC2 Config-Antwortdatei (`C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml`).

- Windows Server 2016 und 2019 – bearbeiten Sie die Antwortdatei „unattend.xml“ (`C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml`).
- Windows Server 2022 – bearbeiten Sie die Antwortdatei „unattend.xml“ (`C:\ProgramData\Amazon\EC2Launch\sysprep\unattend.xml`).

2. Ändern Sie `<CopyProfile>true</CopyProfile>` zu `<CopyProfile>false</CopyProfile>`.
3. Führen Sie Sysprep erneut aus. Hinweis: Mit dieser Konfigurationsänderung wird das integrierte Administratorbenutzerprofil nach Abschluss von Sysprep gelöscht.

Fehlerbehebung einer beeinträchtigten Amazon-EC2-Linux-Instance mithilfe von EC2Rescue

EC2Rescue für Linux ist ein leicht bedienbares Open-Source-Tool, das Sie in einer Amazon-EC2-Linux-Instance zur Diagnose und Behebung häufiger Probleme ausführen können. Dazu verwendet es eine Bibliothek mit über 100 Modulen. Module sind YAML-Dateien, die entweder ein BASH- oder ein Python-Skript und die erforderlichen Metadaten enthalten.

Einige allgemeine Anwendungsfälle für EC2Rescue für Linux-Instances umfassen:

- Sammeln von Syslog- und Paketmanager-Protokollen
- Erfassung von Daten zur Ressourcennutzung
- Diagnose und Behebung bekannter problematischer Kernel-Parameter und häufiger OpenSSH-Probleme

> **Note**
>
> Das `AWSSupport-TroubleshootSSH`-AWS Systems Manager-Automations-Runbook installiert EC2Rescue für Linux und verwendet dann das Tool, um häufig auftretende Probleme zu beheben, die eine SSH-Verbindung zu einer Linux-Instance verhindern. Weitere Informationen finden Sie unter AWSSupport-TroubleshootSSH.

Wenn Sie eine Windows-Instance verwenden, siehe the section called “EC2Rescue für Windows-Instances”.

Themen

- EC2Rescue auf einer Amazon-EC2-Linux-Instance installieren
- EC2Rescue auf einer Amazon-EC2-Linux-Instance ausführen
- EC2Rescue-Module für Amazon-EC2-Linux-Instances entwickeln

EC2Rescue auf einer Amazon-EC2-Linux-Instance installieren

Das Tool EC2Rescue für Linux kann in einer Amazon EC2-Linux-Instance installiert werden, die die folgenden Voraussetzungen erfüllt.

Voraussetzungen

- Unterstützte Betriebssysteme:
  - Amazon Linux 2
  - Amazon Linux 2016.09+
  - SUSE Linux Enterprise Server 12+
  - RHEL 7+
  - Ubuntu 16.04+
- Software-Anforderungen:
  - Python 2.7.9+ oder 3.2+

EC2Rescue installieren

Die `AWSSupport-TroubleshootSSH`-Runbook installiert EC2Rescue für Linux und verwendet dann das Tool, um häufig auftretende Probleme zu beheben, die eine Remote-Verbindung zu einem Linux-Computer über SSH verhindern. Weitere Informationen und zum Ausführen dieser Automatisierung finden Sie unter Support-Support-TroubleshootSSH .

Falls Ihr System die erforderliche Python-Version besitzt, können Sie den Standard-Build installieren. Andernfalls können Sie den Bundle-Build installieren, der eine minimale Kopie von Python enthält.

Installieren des Standard-Builds

1. Laden Sie in einer funktionierenden Linux-Instance das Tool EC2Rescue für Linux herunter:

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz
```

2. (Optional) Überprüfen Sie die Signatur der Installationsdatei von EC2Rescue für Linux. Weitere Informationen finden Sie unter (Optional) Überprüfen der Signatur von EC2Rescue für Linux.
3. Laden Sie die sha256-Hash-Datei herunter:

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sha256
```

4. Überprüfen Sie die Integrität des Tarballs:

```
sha256sum -c ec2rl.tgz.sha256
```

5. Extrahieren Sie den Tarball:

```
tar -xzvf ec2rl.tgz
```

6. Überprüfen Sie die Installation, indem Sie die Hilfedatei aufrufen:

```
cd ec2rl-<version_number>
./ec2rl help
```

Installieren des Bundle-Builds

Einen Link zum Download und eine Liste der Einschränkungen finden Sie unter EC2Rescue für Linux auf Github.

(Optional) Überprüfen der Signatur von EC2Rescue für Linux

Der empfohlene Prozess zur Überprüfung der Gültigkeit des EC2Rescue für Linux-Pakets für Linux-basierte Betriebssysteme:

Wenn Sie eine Anwendung aus dem Internet herunterladen, empfehlen wir Ihnen, die Identität des Software-Publishers zu authentifizieren und sicherzustellen, dass die Anwendung nach ihrer Veröffentlichung nicht verändert oder beschädigt wurde. Dies schützt Sie davor, eine Version der Anwendung zu installieren, die einen Virus oder einen anderen bösartigen Code enthält.

Wenn Sie nach dem Ausführen der Schritte in diesem Thema feststellen, dass die Software für EC2Rescue für Linux verändert oder beschädigt wurde, führen Sie die Installationsdatei nicht aus. Wenden Sie sich stattdessen an Amazon Web Services.

EC2Rescue für Linux-Dateien für Linux-basierte Betriebssysteme werden unter Verwendung von GnuPG, einer Open-Source-Implementierung des Pretty Good Privacy (OpenPGP)-Standards

für sichere digitale Signaturen, signiert. GnuPG (auch als GPG bekannt) bietet Authentifizierung und Integritätsprüfung durch eine digitale Signatur. AWS veröffentlicht den öffentlichen Schlüssel und Signaturen zur Bestätigung des heruntergeladenen EC2Rescue für Linux-Pakets. Weitere Informationen zu PGP und GnuPG (GPG) finden Sie unter https://www.gnupg.org/.

Der erste Schritt besteht darin, eine Vertrauensstellung mit dem Software-Publisher zu schaffen. Laden Sie den öffentlichen Schlüssel des Software-Publisher herunter, überprüfen Sie, ob der Besitzer des öffentlichen Schlüssels derjenige ist, der er behauptet zu sein, und fügen Sie dann den öffentlichen Schlüssel zu Ihrem Schlüsselbund hinzu. Ihr Schlüsselbund ist eine Sammlung von bekannten öffentlichen Schlüsseln. Nachdem Sie die Echtheit des öffentlichen Schlüssels überprüft haben, können Sie ihn verwenden, um die Signatur der Anwendung zu überprüfen.

Aufgaben

- Authentifizieren und Importieren des öffentlichen Schlüssels
- Verifizieren der Signatur des Pakets

Authentifizieren und Importieren des öffentlichen Schlüssels

Der nächste Schritt des Vorgangs besteht darin, den öffentlichen Schlüssel von EC2Rescue für Linux zu authentifizieren und ihn als vertrauenswürdigen Schlüssel Ihrem GPG-Schlüsselbund hinzuzufügen.

So authentifizieren und importieren Sie den öffentlichen Schlüssel von EC2Rescue für Linux

1. Verwenden Sie in einer Eingabeaufforderung den folgenden Befehl, um eine Kopie Ihres öffentlichen GPG-Schlüssels zu erhalten:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.key
   ```

2. Verwenden Sie bei einer Eingabeaufforderung in dem Verzeichnis, in dem Sie `ec2rl.key` gespeichert haben, den folgenden Befehl zum Importieren des öffentlichen Schlüssels EC2Rescue für Linux in den Schlüsselbund:

   ```
   gpg2 --import ec2rl.key
   ```

   Der Befehl gibt Ergebnisse wie die folgenden zurück:

   ```
   gpg: /home/ec2-user/.gnupg/trustdb.gpg: trustdb created
   ```

```
gpg: key 2FAE2A1C: public key "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
 imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

> **Tip**
>
> Wenn Sie eine Fehlermeldung sehen, die besagt, dass der Befehl nicht gefunden werden kann, installieren Sie das GnuPG-Hilfsprogramm mit `apt-get install gnupg2` (Debian-basiertes Linux) oder `yum install gnupg2` (Red Hat-basiertes Linux).

Verifizieren der Signatur des Pakets

Nachdem Sie die GPG-Tools installiert, den öffentlichen Schlüssel von EC2Rescue für Linux authentifiziert, importiert und überprüft haben, ob der öffentliche Schlüssel von EC2Rescue für Linux vertrauenswürdig ist, sind Sie bereit, die Signatur des EC2Rescue für Linux-Installationsskripts zu überprüfen.

So überprüfen Sie die Signatur des EC2Rescue für Linux-Installationsskripts

1. Führen Sie bei einer Eingabeaufforderung den folgenden Befehl aus, um die Signaturdatei für das Installationsskript herunterzuladen:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sig
   ```

2. Überprüfen Sie die Signatur, indem Sie den folgenden Befehl an einer Eingabeaufforderung in dem Verzeichnis ausführen, in dem Sie `ec2rl.tgz.sig` und die EC2Rescue für Linux-Installationsdatei gespeichert haben. Beide Dateien müssen vorhanden sein.

   ```
   gpg2 --verify ./ec2rl.tgz.sig
   ```

   Die Ausgabe sollte wie folgt aussehen:

   ```
   gpg: Signature made Thu 12 Jul 2018 01:57:51 AM UTC using RSA key ID 6991ED45
   gpg: Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
   gpg: WARNING: This key is not certified with a trusted signature!
   gpg:          There is no indication that the signature belongs to the owner.
   Primary key fingerprint: E528 BCC9 0DBF 5AFA 0F6C  C36A F780 4843 2FAE 2A1C
   ```

```
Subkey fingerprint: 966B 0D27 85E9 AEEC 1146  7A9D 8851 1153 6991 ED45
```

Wenn die Ausgabe den Begriff `Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"` enthält, bedeutet dies, dass die Signatur erfolgreich überprüft wurde und Sie mit der Ausführung des EC2Rescue für Linux-Installationsskripts fortfahren können.

Wenn die Ausgabe die Bezeichnung `BAD signature`enthält, überprüfen Sie, ob Sie das Verfahren korrekt durchgeführt haben. Wenn Sie diese Antwort weiterhin erhalten, kontaktieren Sie Amazon Web Services und führen Sie die Installationsdatei, die Sie zuvor heruntergeladen haben, nicht aus.

Im Folgenden finden Sie Details zu den Warnungen, die möglicherweise angezeigt werden:

- WARNING: This key is not certified with a trusted signature! There is no indication that the signature belongs to the owner. Dies bezieht sich auf Ihr persönliches Vertrauen im Glauben, dass Sie einen authentischen öffentlichen Schlüssel für EC2Rescue für Linux besitzen. In einer idealen Welt würden Sie ein Amazon Web Services-Büro aufsuchen und den Schlüssel persönlich erhalten. Doch häufiger laden Sie ihn von einer Website herunter. In diesem Fall handelt es sich bei der Website um eine Amazon Web Services-Website.
- gpg2: no ultimately trusted keys found. Dies bedeutet, dass der bestimmte Schlüssel nicht "endgültig vertrauenswürdig" für Sie oder für andere Personen ist, denen Sie vertrauen.

Weitere Informationen finden Sie unter https://www.gnupg.org/.

EC2Rescue auf einer Amazon-EC2-Linux-Instance ausführen

EC2Rescue ist ein Befehlszeilen-Tool. Nachdem Sie EC2Rescue auf Ihrer Linux-Instance installiert haben, erhalten Sie allgemeine Hilfe zur Verwendung des Tools, indem Sie `./ec2rl help` ausführen. Sie können sich die verfügbaren Module ansehen, indem Sie `./ec2rl list` ausführen. Sie können Hilfe zu einem bestimmten Modul erhalten, indem Sie `./ec2rl help` *`module_name`* ausführen.

Die folgenden Aufgaben können Sie als erste Schritte mit diesem Tool durchführen.

Aufgaben

- EC2Rescue-Module ausführen
- Laden Sie die Ergebnisse des EC2Rescue-Moduls hoch

- Erstellen von Backups einer Amazon-EC2-Linux-Instance

EC2Rescue-Module ausführen

So führen Sie alle EC2Rescue-Module aus

Verwenden Sie den Befehl ./ec2rl run ohne Angabe von Parametern oder Filtern. Einige Module erfordern Root-Zugriff. Falls Sie kein Root-Benutzer sind, verwenden Sie sudo, wenn Sie den Befehl ausführen.

```
./ec2rl run
```

So führen Sie ein bestimmtes EC2Rescue-Modul aus

Verwenden Sie den ./ec2rl run-Befehl und geben Sie für `--only-modules` den Namen des Moduls an, das ausgeführt werden soll. Einige Module benötigen Argumente, um sie zu verwenden.

```
./ec2rl run --only-modules=module_name --arguments
```

Verwenden Sie beispielsweise den folgenden Befehl, um das dig-Modul zur Abfrage der `amazon.com`-Domain auszuführen.

```
./ec2rl run --only-modules=dig --domain=amazon.com
```

So zeigen Sie die Ergebnisse eines EC2Rescue-Moduls an

Führen Sie das Modul aus und zeigen Sie dann die Protokolldatei in `cat /var/tmp/ec2rl/`*`logfile_location`* an. Die Protokolldatei für das dig-Modul befindet sich beispielsweise im folgenden Verzeichnis:

```
cat /var/tmp/ec2rl/timestamp/mod_out/run/dig.log
```

Laden Sie die Ergebnisse des EC2Rescue-Moduls hoch

Wenn Support die Ergebnisse für ein EC2Rescue-Modul angefordert hat, können Sie die Protokolldatei mit dem EC2Rescue-Tool hochladen. Sie können die Ergebnisse entweder an einen von Support zur Verfügung gestellten Ort oder in einen Amazon-S3-Bucket hochladen, den Sie besitzen.

So laden Sie Ergebnisse an einen von Support bereitgestellten Speicherort hoch

Verwenden Sie den ./ec2rl upload-Befehl. Geben Sie für `--upload-directory` den Speicherort der Protokolldatei an. Geben Sie für `--support-url` die URL an, die von Support bereitgestellt wurde.

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/logfile_location --support-
url="url_provided_by_aws_support"
```

So laden Sie Ergebnisse in einen Amazon-S3-Bucket hoch

Verwenden Sie den ./ec2rl upload-Befehl. Geben Sie für `--upload-directory` den Speicherort der Protokolldatei an. Geben Sie für `--presigned-url` eine vorsignierte URL für den S3-Bucket an. Weitere Informationen zum Generieren vorsignierter URLs für Amazon S3 finden Sie unter Hochladen von Objekten mithilfe vorsignierter URLs.

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/logfile_location --presigned-
url="presigned_s3_url"
```

Erstellen von Backups einer Amazon-EC2-Linux-Instance

Sie können EC2Rescue verwenden, um Ihre Linux-Instance zu sichern, indem Sie ein AMI oder Snapshots der angefügten Volumes erstellen.

So erstellen Sie ein AMI

Verwenden Sie den `./ec2rl run`-Befehl und geben Sie für `backup ami` an.

```
./ec2rl run --backup=ami
```

So erstellen Sie Multi-Volume-Snapshots aller angefügten Volumes

Verwenden Sie den `./ec2rl run`-Befehl und geben Sie für `backup allvolumes` an.

```
./ec2rl run --backup=allvolumes
```

So erstellen Sie einen Snapshot eines bestimmten angefügten Volumes

Verwenden Sie den `./ec2rl run`-Befehl und geben Sie für `backup` die ID des Volumes an, das gesichert werden soll.

```
./ec2rl run --backup=vol-01234567890abcdef
```

EC2Rescue-Module für Amazon-EC2-Linux-Instances entwickeln

Module werden in YAML geschrieben, einem Datenserialisierungsstandard. Die YAML-Datei für ein Modul besteht aus einem einzigen Dokument für die Beschreibung des Moduls und seiner Attribute.

Hinzufüge von Modulattributen

In der folgenden Tabelle werden die verfügbaren Modulattribute aufgeführt.

Attribut	Beschreibung
name	Der Name des Moduls. Die Länge des Namens sollte höchstens 18 Zeichen betragen.
Version	Die Versionsnummer des Moduls
Titel	Eine kurze, aussagekräftige Beschreibung des Moduls. Die Länge dieses Werts sollte höchstens 50 Zeichen betragen.

helptext	Die ausführliche Beschreibung des Moduls. Die Länge jeder Zeile sollte höchstens 75 Zeichen betragen. Wenn das Modul mit (obligatorischen oder optionalen) Argumenten aufgerufen wird, sollten sie in dem helptext-Wert einhalten sein.
	
	Beispiel:
	
	`helptext: !!str |`
	`  Collect output from ps for system analysis`
	`  Consumes --times= for number of times to repeat`
	`  Consumes --period= for time period between repetition`

placement	Die Stufe, in der das Modul ausgeführt werden sollte. Unterstützte Werte: • prediagnostic

Attribut	Beschreibung
	• run • postdiagnostic
language	Die Sprache, in der das Modul geschrieben wurde. Unterstützte Werte: • bash • python **Note** Python-Code muss sowohl mit Python 2.7.9+ als auch mit Python 3.2+ kompatibel sein.
remediation	Zeit an, ob das Modul eine Problembehebung unterstützt. Unterstützte Werte sind `True` oder `False`. Das Modul ist standardmäßig `False`, wenn diese Angabe fehlt, womit sie zu einem optionalen Attribut für Module wird, die keine Problembehebung unterstützen.
content	Der gesamte Code für das Skript.
constraint	Der Name des Objekts, das Werte für die Beschränkung enthält.

Attribut	Beschreibung
Domain	Eine Beschreibung, wie das Modul gruppiert oder klassifiziert wird. Die enthaltenen Module verwenden die folgenden Bereiche: • Anwendung • net • os • Leistung
class	Eine Beschreibung der Aufgabe, die von dem Modul durchgeführt wird. Die enthaltenen Module verwenden die folgenden Klassen: • collect (erfasste die Ausgabe von Programmen) • diagnose (bestanden/durchgefallen auf Basis einer Reihe von Kriterien) • gather (kopiert Dateien und schriebt in bestimmte Dateien)
distro	Die Liste der Linux-Distributionen, die dieses Modul unterstützt. Die enthaltenen Module verwenden die folgenden Distributionen: • alami (Amazon Linux) • rhel • ubuntu • suse
Erforderlich	Die obligatorischen Argumente für den Aufruf des Moduls mit dem CLI.
optional	Die optionalen Argumente für den Aufruf des Moduls.

Attribut	Beschreibung
software	Die ausführbare Software, die in dem Modul verwendet wird. Dieses Attribut dient der Spezifikation von Software, die nicht standardmäßig installiert ist. Die Logik von EC2Rescue für Linux stellt vor der Ausführung des Moduls sicher, dass diese Programme vorhanden sind und ausgeführt werden können.
package	Das Quellcode-Paket für eine ausführbare Software. Dieses Attribut dient der Spezifikation ausführlicher Details zu dem Softwarepaket, einschließlich einer URL, unter der weitere Informationen heruntergeladen oder abgerufen werden können.
sudo	Zeigt an, ob für die Ausführung des Moduls Root-Berechtigungen erforderlich sind. Sie müssen keine sudo-Checks in dem Skript für das Modul implementieren. Wenn dieser Wert auf „true” gesetzt wird, führt die EC2Rescue für Linux-Logik das Modul nur aus, wenn der ausführende Benutzer über Root-Berechtigungen verfügt.
perfimpact	Zeigt an, ob das Modul signifikante Auswirkungen auf die Leistung in der Umgebung haben kann, in der es ausgeführt wird. Wenn dieser Wert auf „true” gesetzt und das `--perfimpact=true` -Argument nicht aufgerufen wird, dann wird das Modul übersprungen.
parallelexclusive	Spezifiziert ein Programm, dass gegenseitige Exklusivität erfordert. So können z. B. alle Module, für die hier „bpf” angegeben wird, nur nacheinander ausgeführt werden.

Hinzufügen von Umgebungsvariablen

In der folgenden Tabelle werden die verfügbaren Umgebungsvariablen aufgeführt.

Umgebungsvariable	Beschreibung
`EC2RL_CALLPATH`	Der Pfad zu `ec2rl.py`. Anhand dieses Pfades können Sie das Lib-Verzeichnis finden und von Anbietern bereitgestellte Python-Module benutzen.
`EC2RL_WORKDIR`	Das primäre temporäre Verzeichnis für das Diagnosetool Standardwer: `/var/tmp/ec2rl` .
`EC2RL_RUNDIR`	Das Verzeichnis, in dem alle Ausgaben gespeichert werden Standardwer: `/var/tmp/ec2rl/<date&timestamp>` .
`EC2RL_GATHEREDDIR`	Das Stammverzeichnis für die erfassten Moduldaten Standardwer:`/var/tmp/ec2rl/<date&timestamp>/mod_out/gathered/` .
`EC2RL_NET_DRIVER`	Der Treiber für die erste, alphabetisch sortierte , nicht virtuelle Netzwerkschnittstelle in der Instance Beispiele: • xen_netfront • ixgbevf • ena

Umgebungsvariable	Beschreibung
`EC2RL_SUDO`	„true”, wenn EC2Rescue für Linux mit Root-Berechtigungen ausgeführt wird; andernfalls „false”
`EC2RL_VIRT_TYPE`	Der Virtualisierungstyp gemäß der bereitgestellten Instance-Metadaten Beispiele: • default-hvm • default-paravirtual
`EC2RL_INTERFACES`	Eine nummerierte List der Schnittstellen in dem System. Der Wert besteht aus einer Zeichenfolge, die Namen wie `eth0`, `eth1` usw. enthält. Er wird über `functions.bash` generiert und ist nur für Module verfügbar, die diese aufgerufen haben.

Verwenden des YAML-Syntax

Beachten Sie unbedingt die folgenden Punkte, wenn Sie die YAML-Dateien für ein Modul erstellen:

- Drei Bindestriche hintereinander (`---`) zeigen den Beginn eines Dokuments explizit an.
- Der Tag `!ec2rlcore.module.Module` zeigt dem YAML-Parser an, welcher Konstruktor aufgerufen werden soll, um das Objekt aus dem Datenstrom zu erstellen. Sie finden den Konstruktor in der Datei `module.py`.
- Der Tag `!!str` weist den YAML-Parser an, keinen Versuch zur Bestimmung des Datentyps zu unternehmen, sondern den Inhalt als Zeichenfolgeliteral zu interpretieren.
- Das Pipe-Zeichen (`|`) zeigt dem YAML-Parser an, dass es sich um einen skalaren Wert handelt – ähnlich einem Literal. In diesem Fall übernimmt der Parser alle Leerraumzeichen. Dies ist im Zusammenhang mit Modulen sehr wichtig, da Einrückungen und Zeilenumbrüche erhalten bleiben.
- Die Standardeinrückung in YAML besteht aus zwei Leerzeichen, wie in den folgenden Beispielen gezeigt. Stellen Sie sicher, dass Sie in Ihrem Skript mit den jeweiligen Standard-Einrückungen

arbeiten (z. B. vier Leerzeichen in Python) und den gesamten Inhalt anschließend in der Moduldatei um zwei Leerzeichen einrücken.

Beispielmodule

Beispiel 1 (`mod.d/ps.yaml`):

```
--- !ec2rlcore.module.Module
# Module document. Translates directly into an almost-complete Module object
name: !!str ps
path: !!str
version: !!str 1.0
title: !!str Collect output from ps for system analysis
helptext: !!str |
  Collect output from ps for system analysis
  Requires --times= for number of times to repeat
  Requires --period= for time period between repetition
placement: !!str run
package:
  - !!str
language: !!str bash
content: !!str |
  #!/bin/bash
  error_trap()
  {
      printf "%0.s=" {1..80}
      echo -e "\nERROR: "$BASH_COMMAND" exited with an error on line ${BASH_LINENO[0]}"
      exit 0
  }
  trap error_trap ERR

  # read-in shared function
  source functions.bash
  echo "I will collect ps output from this $EC2RL_DISTRO box for $times times every
 $period seconds."
  for i in $(seq 1 $times); do
      ps auxww
      sleep $period
  done
constraint:
  requires_ec2: !!str False
  domain: !!str performance
  class: !!str collect
```

```
  distro: !!str alami ubuntu rhel suse
  required: !!str period times
  optional: !!str
  software: !!str
  sudo: !!str False
  perfimpact: !!str False
  parallelexclusive: !!str
```

Problembehebung einer beeinträchtigten Amazon EC2 Windows-Instance mithilfe von EC2 Rescue

EC2Rescue for Windows Server ist ein easy-to-use Tool, das Sie auf einer Amazon EC2 Windows Server-Instance ausführen, um mögliche Probleme zu diagnostizieren und zu beheben. Das Tool ist nützlich zum Sammeln von Protokolldateien, zur Behebung von Problemen und zur proaktiven Suche nach möglichen Problembereichen. Es kann sogar Amazon EBS-Stamm-Volumes von anderen Instances untersuchen und relevante Protokolle zur Fehlerbehebung bei Windows-Server-Instances mithilfe des entsprechenden Volumes erfassen. Im Folgenden sind einige häufig auftretende Probleme aufgeführt, die mit EC2 Rescue behoben werden können:

- Verbindungsprobleme mit Instances aufgrund der Konfigurationen der Firewall, des Remote Desktop Protocol (RDP) oder der Netzwerkschnittstelle
- Probleme beim Starten des Betriebssystems aufgrund eines Stoppfehlers, einer Startschleife oder einer beschädigten Registrierung
- Probleme, für die möglicherweise eine erweiterte Protokollanalyse und Fehlerbehebung erforderlich ist

EC2Rescue für Windows Server besteht aus zwei verschiedenen Modulen:

- Ein Datensammelmodul, das Daten aus allen verschiedenen Quellen sammelt
- Ein Analysemodul, das die gesammelten Daten nach einer Reihe vordefinierter Regeln analysiert, um Probleme zu erfassen und Vorschläge zu unterbreiten

Das EC2 Rescue for Windows Server-Tool kann nur auf EC2 Amazon-Instances ausgeführt werden, auf denen Windows Server 2012 und höher ausgeführt wird. Wenn das Tool gestartet wird, prüft es, ob es auf einer EC2 Amazon-Instance läuft.

> **Note**
>
> Das `AWSSupport-ExecuteEC2Rescue` AWS Systems Manager Automation-Runbook verwendet das EC2 Rescue-Tool, um allgemeine Verbindungsprobleme mit der angegebenen EC2 Instance zu beheben und, sofern möglich, zu beheben. Weitere Informationen und Informationen zum Ausführen dieser Automatisierung finden Sie unter > AWSSupport-ExecuteEC 2Rescue.

Wenn Sie eine Linux-Instance verwenden, siehe the section called “EC2Rescue für Linux-Instances”.

Themen

- Beheben Sie eine beeinträchtigte Windows-Instanz mit der EC2 Rescue-GUI
- Beheben Sie eine beeinträchtigte Windows-Instanz mit der EC2 Rescue-CLI
- Beheben Sie eine beeinträchtigte Windows-Instanz mit EC2 Rescue und Systems Manager

Beheben Sie eine beeinträchtigte Windows-Instanz mit der EC2 Rescue-GUI

EC2Rescue for Windows Server kann die folgenden Analysen für Offline-Instances durchführen:

Option	Beschreibung
Diagnose und Datenrettung	EC2Rescue for Windows Server kann Probleme mit den folgenden Diensteinstellungen erkennen und beheben: • Systemzeit • RealTimeisUniversal- Erkennt, ob der `RealTimeisUniversal` Registrierungsschlüssel aktiviert ist. Andernfalls weicht die Windows-Systemzeit ab, wenn die Zeitzone auf einen anderen Wert als UTC eingestellt ist. • Windows-Firewall

Option	Beschreibung
	• Domain networks – Erkennt, ob dieses Windows-Firewall-Profil aktiviert oder deaktiviert ist. • Private networks – Erkennt, ob dieses Windows-Firewall-Profil aktiviert oder deaktiviert ist. • Guest or public networks – Erkennt, ob dieses Windows-Firewall-Profil aktiviert oder deaktiviert ist. • Remotedesktop • Service Start – Erkennt, ob der Remote Desktop Service aktiviert ist. • Remote Desktop Connections – Erkennt, ob diese Funktion aktiviert ist. • TCP Port – Erkennt, welchen Port der Remote Desktop Service überwacht. • EC2Config (Windows Server 2012 R2 und früher) • Installation - Erkennt, welche EC2 Config-Version installiert ist. • Service Start - Erkennt, ob der EC2 Config-Dienst aktiviert ist. • Ec2 SetPassword - Generiert ein neues Administratorkennwort. • Ec2 HandleUserData - Ermöglicht es Ihnen, beim nächsten Start der Instance ein Benutzerdatenskript auszuführen. • EC2Starten (Windows Server 2016 und höher)

Option	Beschreibung

	• Installation - Erkennt, welche EC2 Launch-Version installiert ist.
	• Ec2 SetPassword - Generiert ein neues Administratorkennwort.
	
	• Netzwerkschnittstelle
	  • DHCP Service Startup – Erkennt, ob der DHCP-Service aktiviert ist.
	  • Ethernet detail – Zeigt Informationen zur Netzwerktreiber-Version an, falls diese erkannt wird.
	  • DHCP on Ethernet – Erkennt, ob DHCP aktiviert ist.
	• Festplattensignaturstatus
	  • Signature on disk und Signature on Boot Configuration Database (BCD) – erkennt, ob die Festplattensignatur und die BCD-Signatur identisch sind. Wenn die Werte unterschiedlich sind, versucht EC2 Rescue, die Festplattensignatur mit der Signatur auf BCD zu überschreiben.

Wiederherstellen	Durchführen einer der folgenden Aktionen: • Last Known Good Configuration – Versucht, die Instance im letzten bekannten bootfähig en Zustand zu starten. • Restore registry from backup – Stellt die Registrierung aus `\Windows\System32\config\RegBack` wieder her.
Erfassen von Protokollen	Erlaubt das Erfassen von Protokollen in der Instance zur Analyse.

EC2Rescue for Windows Server kann die folgenden Daten von aktiven und Offline-Instanzen sammeln:

Item	Beschreibung
Ereignisprotokoll	Sammelt Anwendungs-, System- und EC2 Konfigurationsereignisprotokolle.
Registrierung	Sammelt `SYSTEM`- und `SOFTWARE`-Hives.
Windows-Aktualisierungsprotokoll	Sammelt vom Windows Update generierte Protokolldateien. **Note** In Windows Server 2016 und höher wird das Protokoll im Format Ereignisablaufverfolgung für Windows (ETW) gesammelt.
Sysprep-Protokoll	Sammelt vom Windows-Systemvorbereitungs-Tool generierte Protokolldateien.
Driver-Setup-Protokoll	Sammelt Windows-SetupAPI-Protokolle (`setupapi.dev.log` und `setupapi.setup.log`).
Boot-Konfiguration	Sammelt `HKEY_LOCAL_MACHINE\BCD00000000` -Hive.
Speicherabbild	Sammelt alle existierenden Speicherabbilddateien in der Instance.
EC2Config-Datei	Sammelt vom EC2 Config-Dienst generierte Protokolldateien.
EC2Datei starten	Sammelt Protokolldateien, die von den EC2 Launch-Skripten generiert wurden.

Item	Beschreibung
SSM-Agent-Datei	Sammelt vom SSM-Agenten generierte Protokolldateien und Patch-Manager-Protokolle.
EC2 Elastische GPUs Datei	Sammelt Ereignisprotokolle im Zusammenhang mit Elastic GPUs.
ECS	Sammelt Protokolle im Zusammenhang mit Amazon ECS.
CloudEndure	Sammelt Protokolldateien, die sich auf CloudEndure Agent beziehen.
AWS Replication Agent für MGN- oder DRS-Protokolldateien	Sammelt Protokolldateien, die sich auf AWS Application Migration Service oder AWS Elastic Disaster Recovery beziehen.

EC2Rescue for Windows Server kann die folgenden zusätzlichen Daten von aktiven Instanzen sammeln:

Item	Beschreibung
Systeminformationen	Sammelt MSInfo32.
Ergebnis der Gruppenrichtlinie	Erfasst einen Bericht zu einer Gruppenrichtlinie.

Analysieren einer Offline-Instance

Die Offline Instance-Option ist nützlich zur Fehlerbehebung von Startproblemen bei Windows-Instances.

So führen Sie eine Aktion bei einer Offline-Instance aus

1. Laden Sie das EC2Rescue for Windows Server-Tool von einer funktionierenden Windows Server-Instanz herunter und extrahieren Sie die Dateien.

Sie können den folgenden PowerShell Befehl ausführen, um EC2 Rescue herunterzuladen, ohne Ihre verstärkte Sicherheitskonfiguration (ESC) für Internet Explorer zu ändern:

```
Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
```

Mit diesem Befehl wird die EC2 Rescue-ZIP-Datei auf den Desktop des aktuell angemeldeten Benutzers heruntergeladen.

> **Note**
>
> Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 oder eine frühere Version verwenden, muss TLS 1.2 möglicherweise für Ihr PowerShell Terminal aktiviert werden. Sie können TLS 1.2 für die aktuelle PowerShell Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

2. Halten Sie die fehlerhafte Instance an, falls Sie das noch nicht getan haben.
3. Trennen Sie das EBS-Root-Volume von der fehlerhaften Instance und fügen Sie das Volume einer funktionierenden Windows-Instance hinzu, auf der EC2 Rescue for Windows Server installiert ist.
4. Führen Sie das EC2 Rescue for Windows Server-Tool auf der funktionierenden Instanz aus und wählen Sie Offline-Instanz.
5. Wählen Sie die Festplatte mit dem neu gemounteten Volume und anschließend Next aus.
6. Bestätigen Sie die Festplattenauswahl und wählen Sie Yes aus.
7. Wählen Sie die Offline-Instance-Option zur Durchführung und anschließend Next aus.

Das Tool EC2 Rescue for Windows Server scannt das Volume und sammelt Informationen zur Fehlerbehebung auf der Grundlage der ausgewählten Protokolldateien.

Sammeln von Daten aus einer aktiven Instance

Sie können Protokolle und andere Daten aus einer aktiven Instance sammeln.

So sammeln Sie Daten aus einer aktiven Instance

1. Herstellen einer Verbindung mit Ihrer Windows-Instance.
2. Laden Sie das EC2Rescue for Windows Server-Tool auf Ihre Windows-Instanz herunter und extrahieren Sie die Dateien.

   Sie können den folgenden PowerShell Befehl ausführen, um EC2 Rescue herunterzuladen, ohne Ihre verstärkte Sicherheitskonfiguration (ESC) für Internet Explorer zu ändern:

   ```
   Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
   OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
   ```

   Mit diesem Befehl wird die EC2 Rescue-ZIP-Datei auf den Desktop des aktuell angemeldeten Benutzers heruntergeladen.

   > **Note**
   >
   > Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 oder eine frühere Version verwenden, muss TLS 1.2 möglicherweise für Ihr PowerShell Terminal aktiviert werden. Sie können TLS 1.2 für die aktuelle PowerShell Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:
   >
   > ```
   > [Net.ServicePointManager]::SecurityProtocol =
   >  [Net.SecurityProtocolType]::Tls12
   > ```

3. Öffnen Sie die Anwendung EC2 Rescue for Windows Server und akzeptieren Sie die Lizenzvereinbarung.
4. Wählen Sie Next, Current instance, Capture logs.
5. Wählen Sie die Datenelemente, die gesammelt werden sollen, und anschließend Collect... aus. Lesen Sie den Warnhinweis, und wählen Sie zum Fortfahren Yes aus.
6. Wählen Sie einen Dateinamen und einen Speicherort für die ZIP-Datei und anschließend Save aus.

7. Nachdem EC2 Rescue for Windows Server den Vorgang abgeschlossen hat, wählen Sie „Übergeordneten Ordner öffnen“, um die ZIP-Datei anzuzeigen.
8. Wählen Sie Finish (Abschließen).

Beheben Sie eine beeinträchtigte Windows-Instanz mit der EC2 Rescue-CLI

Mit der Befehlszeilenschnittstelle (CLI) von EC2 Rescue for Windows Server können Sie ein EC2 Rescue for Windows Server-Plug-In (als „Aktion“ bezeichnet) programmgesteuert ausführen.

Das Tool EC2 Rescue für Windows Server verfügt über zwei Ausführungsmodi:

- /online — Auf diese Weise können Sie auf der Instanz, auf der EC2 Rescue for Windows Server installiert ist, Aktionen ausführen, z. B. Protokolldateien sammeln.
- /offline: <device_id>—Auf diese Weise können Sie Aktionen auf dem Offline-Root-Volume ausführen, das an eine separate Amazon EC2 Windows-Instance angehängt ist, auf der Sie EC2 Rescue for Windows Server installiert haben.

Laden Sie das Tool EC2Rescue for Windows Server EC2 auf Ihre Windows-Instance herunter und extrahieren Sie die Dateien. Sie können die Hilfedatei mit dem folgenden Befehl anzeigen:

```
EC2RescueCmd.exe /help
```

EC2Rescue for Windows Server kann die folgenden Aktionen auf einer Amazon EC2 Windows-Instance ausführen:

- Erfassen-Aktion
- Rettungsaktion
- Wiederherstellen-Aktion

Erfassen-Aktion

> **Note**
>
> Sie können alle Protokolle, eine ganze Protokollgruppe oder ein einzelnes Protokoll in einer Gruppe erfassen.

EC2Rescue for Windows Server kann die folgenden Daten von aktiven und Offline-Instances sammeln.

Gruppe protokollieren	Verfügbare Protokolle	Beschreibung
`all`		Erfasst alle verfügbaren Protokolle.
`eventlog`	• `'Application'` • `'System'` • `'EC2ConfigService'`	Sammelt Anwendungs-, System- und EC2 Konfigurationsereignisprotokolle.
`memory-dump`	• `'Memory Dump File'` • `'Mini Dump Files'`	Sammelt alle existierenden Speicherabbilddateien in der Instance.
`ec2config`	• `'Log Files'` • `'Configuration Files'`	Sammelt vom EC2 Config-Dienst generierte Protokolldateien.
`ec2launch`	• `'Logs'` • `'Config'`	Sammelt Protokolldateien, die von den EC2 Launch-Skripten generiert wurden.
`ssm-agent`	• `'Log Files'` • `'Patch Baseline Logs'` • `'InstanceData'`	Sammelt vom SSM-Agenten generierte Protokolldateien und Patch-Manager-Protokolle.
`sysprep`	`'Log Files'`	Sammelt vom Windows-Systemvorbereitungs-Tool generierte Protokolldateien.
`driver-setup`	• `'SetupAPI Log Files'` • `'DPInst Log File'` • `'AWS PV Setup Log File'`	Sammelt Windows-SetupAPI-Protokolle (`setupapi.dev.log` und `setupapi.setup.log`).

Gruppe protokollieren	Verfügbare Protokolle	Beschreibung
`registry`	• `'SYSTEM'` • `'SOFTWARE'` • `'BCD'`	Sammelt `SYSTEM`- und `SOFTWARE`-Hives.
`egpu`	• `'Event Log'` • `'System Files'`	Sammelt Ereignisprotokolle im Zusammenhang mit Elastic GPUs.
`boot-config`	`'BCDEDIT Output'`	Sammelt `HKEY_LOCAL_MACHINE\BCD00000000` -Hive.
`windows-update`	`'Log Files'`	Sammelt vom Windows Update generierte Protokoll dateien. **Note** In Windows Server 2016 und höher wird das Protokoll im Format Ereignisablaufverfolgung für Windows (ETW) gesammelt.
`cloudendure`	• `'Migrate Script Logs'` • `'Driver Logs'` • `'CloudEndure File List'`	Sammelt Protokolldateien, die sich auf CloudEndure Agent beziehen.

EC2Rescue for Windows Server kann die folgenden zusätzlichen Daten von aktiven Instanzen sammeln.

Gruppe protokollieren	Verfügbare Protokolle	Beschreibung
`system-info`	`'MSInfo32 Output'`	Sammelt `MSInfo32`.
`gpresult`	`'GPResult Output'`	Erfasst einen Bericht zu einer Gruppenrichtlinie.

Die folgenden Optionen sind verfügbar:

- /output: < outputFilePath > - Erforderlicher Pfad zur Zieldatei, um die gesammelten Protokolldateien im ZIP-Format zu speichern.
- /no-offline – Optionales Attribut, das im Offline-Modus verwendet wird. Setzt das Volume nach Abschluss der Aktion nicht auf offline.
- /no-fix-signature- Optionales Attribut, das im Offline-Modus verwendet wird. Korrigiert eine mögliche Datenträger-Signaturkollision nach Abschluss der Aktion nicht.

Beispiele

Im Folgenden finden Sie Beispiele für die Verwendung der EC2 Rescue for Windows Server-CLI.

Beispiele für den Online-Modus

Erfassen aller verfügbaren Protokolle:

```
EC2RescueCmd /accepteula /online /collect:all /output:<outputFilePath>
```

Erfassen nur einer bestimmten Protokollgruppe:

```
EC2RescueCmd /accepteula /online /collect:ec2config /output:<outputFilePath>
```

Erfassen einzelner Protokolle in einer Protokollgruppe:

```
EC2RescueCmd /accepteula /online /collect:'ec2config.Log Files,driver-setup.SetupAPI
 Log Files' /output:<outputFilePath>
```

Beispiele für den Offline-Modus

Erfassen aller verfügbaren Protokolle in einem EBS-Volume. Das Volume wird durch den device_id-Wert angegeben.

```
EC2RescueCmd /accepteula /offline:xvdf /collect:all /output:<outputFilePath>
```

Erfassen nur einer bestimmten Protokollgruppe:

```
EC2RescueCmd /accepteula /offline:xvdf /collect:ec2config /output:<outputFilePath>
```

Rettungsaktion

EC2Rescue für Windows Server kann Probleme mit den folgenden Diensteinstellungen erkennen und beheben:

Servicegruppe	Verfügbare Aktionen	Beschreibung
`all`		
`system-time`	`'RealTimeIsUniversal'`	Systemzeit • RealTimeisUniversal-Erkennt, ob der `RealTimeisUniversal` Registrierungsschlüssel aktiviert ist. Andernfalls weicht die Windows-Systemzeit ab, wenn die Zeitzone auf einen anderen Wert als UTC eingestellt ist.
`firewall`	• `'Domain networks'` • `'Private networks'` • `'Guest or public networks'`	Windows-Firewall • Domain networks – Erkennt, ob dieses Windows-Firewall-Profil aktiviert oder deaktiviert ist.

Servicegruppe	Verfügbare Aktionen	Beschreibung
		• Private networks – Erkennt, ob dieses Windows-Firewall-Profil aktiviert oder deaktiviert ist. • Guest or public networks – Erkennt, ob dieses Windows-Firewall-Profil aktiviert oder deaktiviert ist.
rdp	• `'Service Start'` • `'Remote Desktop Connections'` • `'TCP Port'`	Remotedesktop • Service Start – Erkennt, ob der Remote Desktop Service aktiviert ist. • Remote Desktop Connections – Erkennt, ob diese Funktion aktiviert ist. • TCP Port – Erkennt, welchen Port der Remote Desktop Service überwacht.
`ec2config`	• `'Service Start'` • `'Ec2SetPassword'` • `'Ec2HandleUserData'`	EC2Config • Service Start - Erkennt, ob der EC2 Config-Dienst aktiviert ist. • Ec2 SetPassword - Generiert ein neues Administratorkennwort. • Ec2 HandleUserData - Ermöglicht es Ihnen, beim nächsten Start der Instance ein Benutzerdatenskript auszuführen.

Servicegruppe	Verfügbare Aktionen	Beschreibung
`ec2launch`	`'Reset Administrator Password'`	Generiert ein neues Windows-Administratorpasswort.
`network`	`'DHCP Service Startup'`	Netzwerkschnittstelle • DHCP Service Startup – Erkennt, ob der DHCP-Service aktiviert ist.

Die folgenden Optionen sind verfügbar:

- /level:<level> – Optionales Attribut für die Prüfstufe, die durch die Aktion ausgelöst werden sollte. Die zulässigen Werte lauten: `information`, `warning`, `error`, `all`. Standardmäßig ist der Wert eingestell `error`.
- /check-only – Optionales Attribut, das einen Bericht generiert, aber keine Änderungen am Offline-Volume vornimmt.

  > **Note**
  >
  > Wenn EC2 Rescue for Windows Server eine mögliche Kollision mit der Festplattensignatur erkennt, wird die Signatur standardmäßig nach Abschluss des Offline-Vorgangs korrigiert, auch wenn Sie die `/check-only` Option verwenden. Sie müssen die `/no-fix-signature`-Option verwenden, um die Korrektur zu verhindern.

- /no-offline – Optionales Attribut, das verhindert, dass das Volume nach Abschluss der Aktion auf offline gesetzt wird.
- /no-fix-signature- Optionales Attribut, das eine mögliche Kollision mit der Festplattensignatur nach Abschluss der Aktion nicht behebt.

Beispiele für Rettungen

Im Folgenden finden Sie Beispiele für die Verwendung der EC2 Rescue for Windows Server-CLI. Das Volume wird durch den device_id-Wert angegeben.

Der Versuch, alle erkannten Probleme auf einem Volume zu beheben:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:all
```

Der Versuch, alle Probleme in einer Servicegruppe auf einem Volume zu beheben:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:firewall
```

Der Versuch, ein bestimmtes Problem in einer Servicegruppe auf einem Volume zu beheben:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:rdp.'Service Start'
```

Der Versuch, mehrere Probleme anzugeben und auf einem Volume zu beheben:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:'system-
time.RealTimeIsUniversal,ec2config.Service Start'
```

Wiederherstellen-Aktion

EC2Rescue für Windows Server kann Probleme mit den folgenden Diensteinstellungen erkennen und beheben:

Servicegruppe	Verfügbare Aktionen	Beschreibung
Wiederherstellen der letzten bekannten funktionierenden Konfiguration	`lkgc`	Last Known Good Configuration – Versucht, die Instance im letzten bekannten bootfähigen Zustand zu starten.
Wiederherstellen der Windows-Registrierung aus der letzten Sicherung	`regback`	Restore registry from backup – Stellt die Registrierung aus `\Windows\System32\config\RegBack` wieder her.

Die folgenden Optionen sind verfügbar:

- /no-offline — Optionales Attribut, das verhindert, dass das Volume nach Abschluss der Aktion auf offline gesetzt wird.

- /no-fix-signature— Optionales Attribut, das eine mögliche Kollision mit der Festplattensignatur nach Abschluss der Aktion nicht behebt.

Beispiele für Wiederherstellungen

Im Folgenden finden Sie Beispiele für die Verwendung der EC2 Rescue for Windows Server-CLI. Das Volume wird durch den device_id-Wert angegeben.

Wiederherstellen der letzten bekannten funktionierenden Konfiguration für ein Volume:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:lkgc
```

Wiederherstellen der letzten Sicherung der Windows-Registrierung eines Volumes:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:regback
```

Beheben Sie eine beeinträchtigte Windows-Instanz mit EC2 Rescue und Systems Manager

Support stellt Ihnen ein Systems Manager Run Command-Dokument zur Verfügung, das eine Schnittstelle zu Ihrer Systems Manager-fähigen Instanz bildet, um EC2 Rescue für Windows Server auszuführen. Das Run Command-Dokument hat den Namen `AWSSupport-RunEC2RescueForWindowsTool`.

Dieses Systems Manager Run Command-Dokument führt die folgenden Aufgaben aus:

- Lädt EC2 Rescue für Windows Server herunter und verifiziert es.
- Importiert ein PowerShell Modul, um Ihnen die Interaktion mit dem Tool zu erleichtern.
- Läuft EC2 RescueCmd mit dem angegebenen Befehl und den angegebenen Parametern.

Das Systems Manager Run Command-Dokument akzeptiert drei Parameter:

- Befehl — Die Aktion EC2 Rescue for Windows Server. Die aktuell zulässigen Werte sind:
  - ResetAccess— Setzt das lokale Administratorkennwort zurück. Das lokale Administratorpasswort der aktuellen Instance wird zurückgesetzt und das zufallsgeneriert Passwort wird in Parameter Store als sicher gespeicher `/EC2Rescue/Password/<INSTANCE_ID>`. Wenn Sie diese Aktion auswählen und keine Parameter angeben, werden Passwörter automatisch mit dem

Standard-Verschlüsselung verschlüsselt. Sie können in den Parametern optional die ID eines Verschlüsselung angeben, um das Passwort mit einem eigenen Schlüssel zu verschlüsseln.

- CollectLogs— Führt EC2 Rescue für Windows Server mit der Aktion aus. `/collect:all` Wenn Sie diese Aktion auswählen, müssen die `Parameters` des Amazon S3-Buckets, auf den die Protokolle hochgeladen werden sollen, in den Logs enthalten sein.
- FixAll— Führt EC2 Rescue für Windows Server mit der Aktion aus`/rescue:all`. Wenn Sie diese Aktion auswählen, muss der Name des zu rettenden Blockgerätes in den `Parameters` enthalten sein.

- Parameter — Die PowerShell Parameter, die für den angegebenen Befehl übergeben werden sollen.

Voraussetzungen

Um die ResetAccessAktion auszuführen, muss Ihrer EC2 Amazon-Instance eine Richtlinie angehängt sein, die Berechtigungen zum Schreiben des verschlüsselten Passworts in den Parameter Store gewährt. Warten Sie ein paar Minuten, bevor Sie versuchen, das Passwort einer Instance zurückzusetzen, nachdem Sie diese Richtlinie der zugehörigen IAM-Rolle zugeordnet haben.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:us-east-1:111122223333:parameter/EC2Rescue/
Passwords/<instanceid>"
      ]
    }
  ]
}
```

Wenn Sie einen benutzerdefinierten KMS-Schlüssel und nicht den Standard-KMS-Schlüssel verwenden, verwenden Sie stattdessen diese Richtlinie.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:us-east-1:111122223333:parameter/EC2Rescue/
Passwords/<instanceid>"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:111122223333:key/<kmskeyid>"
      ]
    }
  ]
}
```

JSON-Daten für das Dokument anzeigen

Im folgenden Verfahren wird beschrieben, wie Sie die JSON-Daten für diesen Dokument anzeigen können.

So zeigen Sie die JSON-Daten für das Systems Manager Run Command-Dokument an

1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.

2. Erweitern Sie im Navigationsbereich die Option Verwaltungs-Tools ändern und wählen Sie Dokumente aus.
3. Geben Sie `AWSSupport-RunEC2RescueForWindowsTool` in der Suchleiste ein und wählen Sie dann das Dokument `AWSSupport-RunEC2RescueForWindowsTool` aus.
4. Wählen Sie die Registerkarte Content aus.

Beispiele

Im Folgenden finden Sie einige Beispiele zur Verwendung des Systems Manager Manager-Dokuments Run Command zum Ausführen von EC2 Rescue für Windows Server mithilfe von AWS CLI. Weitere Informationen zum Senden von Befehlen mit dem finden Sie AWS CLI unter send-command.

Beispiele

- Der Versuch, alle erkannten Probleme auf einem Offline-Stamm-Volume zu beheben
- Protokolle von der aktuellen Amazon EC2 Windows-Instance sammeln
- Zurücksetzen des lokalen Administratorpassworts

Der Versuch, alle erkannten Probleme auf einem Offline-Stamm-Volume zu beheben

Versuchen Sie, alle identifizierten Probleme auf einem Offline-Root-Volume zu beheben, das an eine Amazon EC2 Windows-Instance angehängt ist:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --parameters "Command=FixAll, Parameters='xvdf'" --output
 text
```

Protokolle von der aktuellen Amazon EC2 Windows-Instance sammeln

Sammeln Sie alle Protokolle der aktuellen Online-Amazon EC2 Windows-Instance und laden Sie sie in einen Amazon S3-Bucket hoch:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --parameters "Command=CollectLogs, Parameters='amzn-s3-
demo-bucket'" --output text
```

Zurücksetzen des lokalen Administratorpassworts

In den folgenden Beispielen werden Methoden gezeigt, mit denen Sie das lokale Administratorpasswort zurücksetzen können. Die Ausgabe enthält einen Link zum Parameter Store, wo Sie das zufällig generierte sichere Passwort finden, das Sie dann als lokaler Administrator für RDP zu Ihrer Amazon EC2 Windows-Instance verwenden können.

Setzen Sie das lokale Administratorkennwort einer Online-Instance mithilfe der Standardeinstellung zurück AWS KMS key alias/aws/ssm:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --parameters "Command=ResetAccess" --output text
```

Zurücksetzen des lokalen Administratorpassworts für eine Online-Instance mithilfe eines Verschlüsselung:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --parameters "Command=ResetAccess, Parameters=a133dc3c-
a2g4-4fc6-a873-6c0720104bf0" --output text
```

> **Note**
>
> In diesem Beispiel lautet Verschlüsselung `a133dc3c-a2g4-4fc6-a873-6c0720104bf0`.

EC2 Serielle Konsole für Instanzen

Mit der EC2 seriellen Konsole haben Sie Zugriff auf die serielle Schnittstelle Ihrer EC2 Amazon-Instance, über die Sie Boot-, Netzwerkkonfigurations- und andere Probleme beheben können. Die serielle Konsole erfordert nicht, dass Ihre Instance über Netzwerkfähigkeiten verfügt. Mit der seriellen Konsole können Sie Befehle für eine Instance eingeben, als ob Ihre Tastatur und Ihr Monitor direkt an die serielle Schnittstelle der Instance angeschlossen wären. Die Sitzung der seriellen Konsole dauert während des Neustarts und Stopps der Instance. Während des Neustarts können Sie alle Boot-Meldungen von Anfang an anzeigen.

Der Zugriff auf die serielle Konsole ist standardmäßig nicht verfügbar. Ihre Organisation muss Kontozugriff auf die serielle Konsole gewähren und IAM-Richtlinien konfigurieren, um Ihren Benutzern Zugriff auf die serielle Konsole zu gewähren. Der Zugriff auf die serielle Konsole kann mithilfe

von Instance IDs, Resource Tags und anderen IAM-Hebeln detailliert gesteuert werden. Weitere Informationen finden Sie unter Konfigurieren Sie den Zugriff auf die EC2 serielle Konsole.

Auf die serielle Konsole kann über die EC2 Konsole oder die zugegriffen werden. AWS CLI

Die serielle Konsole ist ohne zusätzliche Kosten verfügbar.

Themen

- Voraussetzungen für die EC2 serielle Konsole
- Konfigurieren Sie den Zugriff auf die EC2 serielle Konsole
- Connect zur EC2 seriellen Konsole her
- Trennen Sie die Verbindung zur seriellen Konsole EC2
- Beheben Sie Probleme mit Ihrer EC2 Amazon-Instance mithilfe der EC2 seriellen Konsole

Voraussetzungen für die EC2 serielle Konsole

Um eine Verbindung zur EC2 seriellen Konsole herzustellen und das von Ihnen gewählte Tool zur Fehlerbehebung zu verwenden, müssen die folgenden Voraussetzungen erfüllt sein:

- AWS-Regionen
- Wavelength-Zonen und AWS -Außenposten
- Local Zones
- Instance-Typen
- Gewähren von Zugriff
- Unterstützung für browserbasierte Clients
- Instance-Status
- EC2 Amazon-Systemmanager
- Konfigurieren des von Ihnen gewählten Tools für die Fehlerbehebung

AWS-Regionen

Wird in allen Ländern AWS-Regionen außer im asiatisch-pazifischen Raum (Taipeh) unterstützt.

Wavelength-Zonen und AWS -Außenposten

Nicht unterstützt

Local Zones

Unterstützt in allen lokalen Zonen.

Instance-Typen

Unterstützte Instance-Typen:

- Linux
  - Alle virtualisierten Instances, die auf dem Nitro System aufgebaut sind.
  - Alle Bare-Metal-Instances außer:
    - Universell: `a1.metal`, `mac1.metal`, `mac2.metal`
    - Beschleunigte Datenverarbeitung: `g5g.metal`
    - RAM-optimiert: `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal`, `u-24tb1.metal`
- Windows

  Alle virtualisierten Instances, die auf dem Nitro System aufgebaut sind. Wird nicht auf Bare-Metal-Instances unterstützt.

Gewähren von Zugriff

Sie müssen die Konfigurationsaufgaben abschließen, um Zugriff auf die EC2 serielle Konsole zu gewähren. Weitere Informationen finden Sie unter Konfigurieren Sie den Zugriff auf die EC2 serielle Konsole.

Unterstützung für browserbasierte Clients

Um über den browserbasierten Client eine Verbindung zur seriellen Konsole herzustellen, muss Ihr Browser dies unterstützen WebSocket. Wenn Ihr Browser dies nicht unterstützt WebSocket, stellen Sie mit Ihrem eigenen Schlüssel und einem SSH-Client eine Verbindung zur seriellen Konsole her.

Instance-Status

Der Wert muss `running` sein.

Wenn sich die Instance in den `pending`-, `stopping`-, `stopped`-, `shutting-down`- oder `terminated`-Status befindet, können Sie keine Verbindung mit der seriellen Konsole herstellen.

Weitere Informationen zum Instance-Status finden Sie unter Amazon-EC2-Instance-Statusänderungen.

EC2 Amazon-Systemmanager

Wenn die Instance Amazon EC2 Systems Manager verwendet, muss SSM Agent Version 3.0.854.0 oder höher auf der Instance installiert sein. Informationen zu SSM Agent finden Sie unter Arbeiten mit SSM Agent im AWS Systems Manager -Benutzerhandbuch.

Konfigurieren des von Ihnen gewählten Tools für die Fehlerbehebung

Um Fehler bei Ihrer Instance mithilfe der seriellen Konsole zu beheben, können Sie GRUB oder SysRq auf Linux-Instances und Special Admin Console (SAC) auf Windows-Instances verwenden. Bevor Sie diese Tools verwenden können, müssen Sie zunächst Konfigurationsschritte für jede Instance ausführen, auf der Sie sie verwenden möchten.

Verwenden Sie die Anleitung für das Betriebssystem Ihrer Instance, um das von Ihnen gewählte Tool zur Fehlerbehebung zu konfigurieren.

(Linux-Instances) GRUB konfigurieren

Um GRUB zu konfigurieren, wählen Sie eines der folgenden Verfahren basierend auf dem AMI, das zum Starten der Instance verwendet wurde.

Amazon Linux 2

So konfigurieren Sie GRUB für eine Amazon Linux 2-Instance

1. Herstellen einer Verbindung zu Ihrer Linux-Instance mit SSH
2. Fügen Sie die folgenden Optionen hinzu oder ändern Sie sie in `/etc/default/grub`:
   - Set `GRUB_TIMEOUT=1`.
   - Add `GRUB_TERMINAL="console serial"`.
   - Fügen Sie `GRUB_SERIAL_COMMAND="serial --speed=115200"` hinzu.

   Es folgt ein Beispiel für `/etc/default/grub`. Möglicherweise müssen Sie die Konfiguration basierend auf Ihrem System-Setup ändern.

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0
 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.shell=0"
```

```
GRUB_TIMEOUT=1
GRUB_DISABLE_RECOVERY="true"
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed=115200"
```

3. Übernehmen Sie die aktualisierte Konfiguration, indem Sie den folgenden Befehl ausführen.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

Ubuntu

So konfigurieren Sie GRUB auf einer Ubuntu-Instance

1. Verbinden Sie sich mit der Instance.
2. Fügen Sie die folgenden Optionen hinzu oder ändern Sie sie in `/etc/default/grub.d/50-cloudimg-settings.cfg`:
   - Set `GRUB_TIMEOUT=1`.
   - Add `GRUB_TIMEOUT_STYLE=menu`.
   - Fügen Sie `GRUB_TERMINAL="console serial"` hinzu.
   - Entfernen Sie `GRUB_HIDDEN_TIMEOUT`.
   - Fügen Sie `GRUB_SERIAL_COMMAND="serial --speed=115200"` hinzu.

   Es folgt ein Beispiel für `/etc/default/grub.d/50-cloudimg-settings.cfg`. Möglicherweise müssen Sie die Konfiguration basierend auf Ihrem System-Setup ändern.

```
# Cloud Image specific Grub settings for Generic Cloud Images
# CLOUD_IMG: This file was created/modified by the Cloud Image build process

# Set the recordfail timeout
GRUB_RECORDFAIL_TIMEOUT=0

# Do not wait on grub prompt
GRUB_TIMEOUT=1
GRUB_TIMEOUT_STYLE=menu

# Set the default commandline
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
 nvme_core.io_timeout=4294967295"
```

```
# Set the grub console type
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed 115200"
```

3. Übernehmen Sie die aktualisierte Konfiguration, indem Sie den folgenden Befehl ausführen.

```
[ec2-user ~]$ sudo update-grub
```

RHEL

So konfigurieren Sie GRUB auf einer RHEL-Instance

1. Verbinden Sie sich mit der Instance.
2. Fügen Sie die folgenden Optionen hinzu oder ändern Sie sie in `/etc/default/grub`:
   - Entfernen Sie `GRUB_TERMINAL_OUTPUT`.
   - Add `GRUB_TERMINAL="console serial"`.
   - Fügen Sie `GRUB_SERIAL_COMMAND="serial --speed=115200"` hinzu.

   Es folgt ein Beispiel für `/etc/default/grub`. Möglicherweise müssen Sie die Konfiguration basierend auf Ihrem System-Setup ändern.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_CMDLINE_LINUX="console=tty0 console=ttyS0,115200n8 net.ifnames=0
 rd.blacklist=nouveau nvme_core.io_timeout=4294967295 crashkernel=auto"
GRUB_DISABLE_RECOVERY="true"
GRUB_ENABLE_BLSCFG=true
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed=115200"
```

3. Übernehmen Sie die aktualisierte Konfiguration, indem Sie den folgenden Befehl ausführen.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg --update-bls-cmdline
```

Verwenden Sie unter RHEL 9.2 und älter den folgenden Befehl.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

CentOS

Für Instances, die mit einem CentOS-AMI gestartet werden, ist GRUB standardmäßig für die serielle Konsole konfiguriert.

Es folgt ein Beispiel für `/etc/default/grub`. Ihre Konfiguration kann je nach Systemeinrichtung unterschiedlich sein.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL="serial console"
GRUB_SERIAL_COMMAND="serial --speed=115200"
GRUB_CMDLINE_LINUX="console=tty0 crashkernel=auto console=ttyS0,115200"
GRUB_DISABLE_RECOVERY="true"
```

(Linux-Instanzen) Konfigurieren SysRq

Zur Konfiguration SysRq aktivieren Sie die SysRq Befehle für den aktuellen Startzyklus. Um die Konfiguration dauerhaft zu machen, können Sie die SysRq Befehle auch für nachfolgende Starts aktivieren.

Um alle SysRq Befehle für den aktuellen Startzyklus zu aktivieren

1. Verbinden Sie sich mit der Instance.
2. Führen Sie den folgenden Befehl aus.

```
[ec2-user ~]$ sudo sysctl -w kernel.sysrq=1
```

Diese Einstellung wird beim nächsten Neustart gelöscht.

Um alle SysRq Befehle für nachfolgende Starts zu aktivieren

1. Erstellen Sie die Datei `/etc/sysctl.d/99-sysrq.conf` und öffnen Sie sie in Ihrem Lieblingseditor.

   ```
   [ec2-user ~]$ sudo vi /etc/sysctl.d/99-sysrq.conf
   ```

2. Fügen Sie die folgende Zeile zu.

   ```
   kernel.sysrq=1
   ```

3. Starten Sie die Instance neu, um die Änderungen zu übernehmen.

   ```
   [ec2-user ~]$ sudo reboot
   ```

4. Geben Sie an der `login`-Eingabeaufforderung den Benutzernamen des passwortbasierten Benutzers ein, den Sie vorher eingerichtet haben, und drücken Sie dann die Eingabetaste.
5. Geben Sie an der `Password`-Eingabeaufforderung das Passwort ein und drücken Sie dann die Eingabetaste.

(Windows-Instances) SAC und Boot-Menü einrichten

> **Note**
>
> Wenn Sie SAC auf einer Instance aktivieren, funktionieren die EC2 Dienste, die auf den Kennwortabruf angewiesen sind, nicht von der EC2 Amazon-Konsole aus. Die EC2 Startagenten von Windows auf Amazon (EC2Config, EC2 Launch v1 und EC2 Launch v2) benötigen die serielle Konsole, um verschiedene Aufgaben auszuführen. Diese Aufgaben werden nicht erfolgreich ausgeführt, wenn Sie SAC für eine Instance aktivieren. Weitere Informationen zu Windows on Amazon EC2 Launch Agents finden Sie unterthe section called “Konfigurieren Ihrer Windows-Instance”. Wenn Sie SAC aktivieren, können Sie es später deaktivieren. Weitere Informationen finden Sie unter Deaktivieren von SAC und vom Boot-Menü.

Verwenden Sie eine der folgenden Methoden, um SAC und das Bootmenü einer Instance zu aktivieren.

PowerShell

Aktivieren von SAC und dem Boot-Menü auf einer Windows-Instance

1. Connect zu Ihrer Instance her und führen Sie die folgenden Schritte von einer PowerShell Befehlszeile mit erhöhten Rechten aus.
2. Aktivieren Sie SAC.

```
bcdedit /ems '{current}' on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Aktivieren Sie das Boot-Menü.

```
bcdedit /set '{bootmgr}' displaybootmenu yes
bcdedit /set '{bootmgr}' timeout 15
bcdedit /set '{bootmgr}' bootems yes
```

4. Wenden Sie die aktualisierte Konfiguration an, indem Sie die Instance neu starten.

```
shutdown -r -t 0
```

Command prompt

Aktivieren von SAC und dem Boot-Menü auf einer Windows-Instance

1. Stellen Sie eine Verbindung mit Ihrer Instance her und führen Sie die folgenden Schritte an der Eingabeaufforderung aus.
2. Aktivieren Sie SAC.

```
bcdedit /ems {current} on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Aktivieren Sie das Boot-Menü.

```
bcdedit /set {bootmgr} displaybootmenu yes
bcdedit /set {bootmgr} timeout 15
bcdedit /set {bootmgr} bootems yes
```

4. Wenden Sie die aktualisierte Konfiguration an, indem Sie die Instance neu starten.

```
shutdown -r -t 0
```

Konfigurieren Sie den Zugriff auf die EC2 serielle Konsole

Um den Zugriff auf die serielle Konsole zu konfigurieren, müssen Sie den Zugriff auf die serielle Konsole auf Kontoebene gewähren und dann IAM-Richtlinien konfigurieren, um Ihren Benutzern Zugriff zu gewähren. Sie müssen für Linux-Instances auch einen passwortbasierten Benutzer für jede Instance konfigurieren, damit Ihre Benutzer die serielle Konsole zur Fehlerbehebung verwenden können.

EC2 Die serielle Konsole verwendet eine virtuelle serielle Schnittstelle, um mit einer Instanz zu interagieren. Diese Verbindung ist unabhängig von der Instance-VPC, sodass Sie mit dem Instance-Betriebssystem arbeiten und Tools zur Fehlerbehebung ausführen können, auch wenn Startfehler oder Probleme mit der Netzwerkkonfiguration auftreten. Da sich diese Verbindung außerhalb des VPC-Netzwerks befindet, verwendet EC2 Serial Console weder die Instance-Sicherheitsgruppe noch die Subnetz-Netzwerk-ACL, um den Datenverkehr zur Instance zu autorisieren.

Bevor Sie beginnen

Stellen Sie sicher, dass die Voraussetzungen erfüllt sind.

Inhalt

- Zugriffsebenen auf die serielle Konsole EC2
- Verwalten Sie den Kontozugriff auf die EC2 serielle Konsole
- Konfigurieren Sie IAM-Richtlinien für den Zugriff auf die EC2 serielle Konsole
- Benutzerkennwort des Betriebssystems auf einer Linux-Instance festlegen

Zugriffsebenen auf die serielle Konsole EC2

Standardmäßig gibt es auf Kontoebene keinen Zugriff auf die serielle Konsole. Sie müssen explizit Zugriff auf die serielle Konsole auf Kontoebene gewähren. Weitere Informationen finden Sie unter Verwalten Sie den Kontozugriff auf die EC2 serielle Konsole.

Sie können eine Service-Kontroll-Richtlinie (SCP) verwenden, um den Zugriff auf die serielle Konsole in Ihrem Unternehmen zu ermöglichen. Sie können dann eine differenzierte Zugriffskontrolle auf

Benutzerebene vornehmen, indem Sie eine IAM-Richtlinie zur Zugriffskontrolle verwenden. Durch die Verwendung einer Kombination von SCP- und IAM-Richtlinien haben Sie unterschiedliche Zugriffskontrollstufen für die serielle Konsole.

Organisationsebene

Sie können eine Service-Kontroll-Richtlinie (SCP) verwenden, um Mitgliedskonten in Ihrer Organisation den Zugriff auf die serielle Konsole zu ermöglichen. Weitere Informationen zu SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.

Instance-Ebene

Sie können die Zugriffsrichtlinien für serielle Konsolen mithilfe von IAM PrincipalTag und ResourceTag Konstruktionen konfigurieren und Instanzen anhand ihrer ID angeben. Weitere Informationen finden Sie unter Konfigurieren Sie IAM-Richtlinien für den Zugriff auf die EC2 serielle Konsole.

Benutzerebene

Sie können den Zugriff auf die Benutzerebene konfigurieren, indem Sie eine IAM-Richtlinie konfigurieren, um einem bestimmten Benutzer die Berechtigung zu erteilen oder zu verweigern, den öffentlichen SSH-Schlüssel an den seriellen Konsolendienst einer bestimmten Instance zu übertragen. Weitere Informationen finden Sie unter Konfigurieren Sie IAM-Richtlinien für den Zugriff auf die EC2 serielle Konsole.

Betriebssystemebene (nur Linux-Instances)

Sie können ein Benutzerpasswort auf der Ebene des Gastbetriebssystems festlegen. Dies ermöglicht für einige Anwendungsfälle Zugriff auf die serielle Konsole. Um die Protokolle zu überwachen, benötigen Sie jedoch keinen passwortbasierten Benutzer. Weitere Informationen finden Sie unter Benutzerkennwort des Betriebssystems auf einer Linux-Instance festlegen.

Verwalten Sie den Kontozugriff auf die EC2 serielle Konsole

Standardmäßig gibt es auf Kontoebene keinen Zugriff auf die serielle Konsole. Sie müssen explizit Zugriff auf die serielle Konsole auf Kontoebene gewähren.

Diese Einstellung wird auf Kontoebene konfiguriert, entweder direkt im Konto oder mithilfe einer deklarativen Richtlinie. Es muss in allen Bereichen konfiguriert werden, in AWS-Region denen Sie Zugriff auf die serielle Konsole gewähren möchten. Mithilfe einer deklarativen Richtlinie können Sie

die Einstellung auf mehrere Regionen gleichzeitig sowie auf mehrere Konten gleichzeitig anwenden. Wenn eine deklarative Richtlinie verwendet wird, können Sie die Einstellung nicht direkt in einem Konto ändern. In diesem Thema wird beschrieben, wie Sie die Einstellung direkt in einem Konto konfigurieren. Informationen zur Verwendung deklarativer Richtlinien finden Sie unter Deklarative Richtlinien im AWS Organizations -Benutzerhandbuch.

Inhalt

- Gewähren von Berechtigungen für Benutzer zur Verwaltung des Kontozugriffs
- Anzeigen des Kontozugriffsstatus für die serielle Konsole
- Erteilen des Kontozugriffs auf die serielle Konsole
- Kontozugriff auf die serielle Konsole verweigern

Gewähren von Berechtigungen für Benutzer zur Verwaltung des Kontozugriffs

Damit Ihre Benutzer den Kontozugriff auf die EC2 serielle Konsole verwalten können, müssen Sie ihnen die erforderlichen IAM-Berechtigungen gewähren.

Die folgende Richtlinie gewährt Berechtigungen zur Anzeige des Kontostatus sowie zum Zulassen und Unterbinden des Kontozugriffs auf die EC2 serielle Konsole.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:EnableSerialConsoleAccess",
                "ec2:DisableSerialConsoleAccess"
            ],
            "Resource": "*"
        }
    ]
}
```

Weitere Informationen finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Anzeigen des Kontozugriffsstatus für die serielle Konsole

Console

So zeigen Sie den Kontozugriff in der seriellen Konsole an

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich EC2 Dashboard aus.
3. Wählen Sie unter Kontoattribute die Option EC2 Serial Console aus.
4. Auf der Registerkarte EC2 Serielle Konsole ist der Wert für Zugriff auf EC2 serielle Konsole entweder zugelassen oder verhindert.

AWS CLI

So zeigen Sie den Kontozugriff in der seriellen Konsole an

Verwenden Sie den Befehl get-serial-console-access-status.

```
aws ec2 get-serial-console-access-status
```

Es folgt eine Beispielausgabe. Ein Wert von `true` zeigt an, dass dem Konto Zugriff auf die serielle Konsole gewährt wird.

```
{
    "SerialConsoleAccessEnabled": true,
    "ManagedBy": "account"
}
```

Das `ManagedBy`-Feld gibt die Entität an, die die Einstellung konfiguriert hat. Die möglichen Werte sind `account` (direkt konfiguriert) oder `declarative-policy`. Weitere Informationen finden Sie unter Deklarative Richtlinien im AWS Organizations -Benutzerhandbuch.

PowerShell

So zeigen Sie den Kontozugriff in der seriellen Konsole an

Verwenden Sie das cmdlet Get-EC2SerialConsoleAccessStatus.

```
Get-EC2SerialConsoleAccessStatus -Select *
```

Es folgt eine Beispielausgabe. Ein Wert von `True` zeigt an, dass dem Konto Zugriff auf die serielle Konsole gewährt wird.

```
ManagedBy SerialConsoleAccessEnabled
--------- --------------------------
account   True
```

Das `ManagedBy`-Feld gibt die Entität an, die die Einstellung konfiguriert hat. Die möglichen Werte sind `account` (direkt konfiguriert) oder `declarative-policy`. Weitere Informationen finden Sie unter verwaltete Richtlinien im AWS Organizations -Benutzerhandbuch.

Erteilen des Kontozugriffs auf die serielle Konsole

Console

So gewähren Sie den Kontozugriff auf die serielle Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich EC2 Dashboard aus.
3. Wählen Sie unter Kontoattribute die Option EC2 Serial Console aus.
4. Wählen Sie Manage (Verwalten).
5. Um allen Instanzen im Konto Zugriff auf die EC2 serielle Konsole zu gewähren, aktivieren Sie das Kontrollkästchen Zulassen.
6. Wählen Sie Aktualisieren aus.

AWS CLI

So gewähren Sie den Kontozugriff auf die serielle Konsole

Verwenden Sie den Befehl enable-serial-console-access.

```
aws ec2 enable-serial-console-access
```

Es folgt eine Beispielausgabe.

```
{
    "SerialConsoleAccessEnabled": true
}
```

PowerShell

So gewähren Sie den Kontozugriff auf die serielle Konsole

Verwenden Sie das cmdlet Enable-EC2SerialConsoleAccess.

```
Enable-EC2SerialConsoleAccess
```

Es folgt eine Beispielausgabe.

```
True
```

Kontozugriff auf die serielle Konsole verweigern

Console

So verweigern Sie den Kontozugriff auf die serielle Konsole

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich EC2 Dashboard aus.
3. Wählen Sie unter Kontoattribute die Option EC2 Serial Console aus.
4. Wählen Sie Manage (Verwalten).
5. Um den Zugriff aller Instanzen im Konto auf die EC2 serielle Konsole zu verhindern, deaktivieren Sie das Kontrollkästchen Zulassen.
6. Wählen Sie Aktualisieren aus.

AWS CLI

So verweigern Sie den Kontozugriff auf die serielle Konsole

Verwenden Sie den Befehl disable-serial-console-access.

```
aws ec2 disable-serial-console-access
```

Es folgt eine Beispielausgabe.

```
{
    "SerialConsoleAccessEnabled": false
```

```
}
```

PowerShell

So verweigern Sie den Kontozugriff auf die serielle Konsole

Verwenden Sie das cmdlet Disable-EC2SerialConsoleAccess.

```
Disable-EC2SerialConsoleAccess
```

Es folgt eine Beispielausgabe.

```
False
```

Konfigurieren Sie IAM-Richtlinien für den Zugriff auf die EC2 serielle Konsole

Standardmäßig haben Ihre Benutzer keinen Zugriff auf die serielle Konsole. Ihre Organisation muss IAM-Richtlinien konfigurieren, um Ihren Benutzern den erforderlichen Zugriff zu gewähren. Weitere Informationen finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Für den seriellen Konsolenzugriff erstellen Sie ein JSON-Richtliniendokument, das die `ec2-instance-connect:SendSerialConsoleSSHPublicKey`-Aktion enthält. Diese Aktion gewährt einem Benutzer die Berechtigung, den öffentlichen Schlüssel an den seriellen Konsolenservice zu übertragen, der eine serielle Konsolensitzung startet. Wir empfehlen, den Zugriff auf bestimmte EC2 Instanzen zu beschränken. Andernfalls können sich alle Benutzer mit dieser Berechtigung mit der seriellen Konsole aller EC2 Instanzen verbinden.

IAM-Beispielrichtlinien

- Zulassen des Zugriffs auf die serielle Konsole
- Explizites Verweigern des Zugriffs auf die serielle Konsole
- Verwenden von Ressourcen-Tags (Markierungen), um den Zugriff auf die serielle Konsole zu kontrollieren

Zulassen des Zugriffs auf die serielle Konsole

Standardmäßig hat niemand Zugriff auf die serielle Konsole. Um den Zugriff auf die serielle Konsole zu gewähren, müssen Sie eine Richtlinie konfigurieren, um den Zugriff explizit zuzulassen. Wir empfehlen, eine Richtlinie zu konfigurieren, die den Zugriff auf bestimmte Instances einschränkt.

Die folgende Richtlinie ermöglicht den Zugriff auf die serielle Konsole einer bestimmten Instance, die durch ihre Instance-ID identifiziert wird.

Beachten Sie, dass die `DescribeInstances`-, `DescribeInstanceTypes`-, und `GetSerialConsoleAccessStatus`-Aktionen keine Berechtigungen auf Ressourcenebene unterstützen. Daher müssen alle Ressourcen, die durch ein * (Sternchen) gekennzeichnet sind, für diese Aktionen spezifiziert werden.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
             "Resource": "*"
        },
        {
            "Sid": "AllowinstanceBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:us-
east-1:111122223333:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Explizites Verweigern des Zugriffs auf die serielle Konsole

Die folgende IAM-Richtlinie ermöglicht den Zugriff auf die serielle Konsole aller Instances, die durch das * (Sternchen) gekennzeichnet ist, und verweigert ausdrücklich den Zugriff auf die serielle Konsole einer bestimmten Instance, die durch ihre ID identifiziert wird.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DenySerialConsoleAccess",
            "Effect": "Deny",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:us-
east-1:111122223333:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Verwenden von Ressourcen-Tags (Markierungen), um den Zugriff auf die serielle Konsole zu kontrollieren

Sie können Ressourcen-Tags (Markierungen) verwenden, um den Zugriff auf die serielle Konsole einer Instance zu steuern.

Die attributbasierte Zugriffskontrolle ist eine Autorisierungsstrategie, bei der Berechtigungen auf der Grundlage von Tags definiert werden, die Benutzern und Ressourcen zugewiesen werden können. AWS Beispielsweise ermöglicht die folgende Richtlinie einem Benutzer, eine serielle Konsolenverbindung für eine Instance nur dann zu initiieren, wenn das Ressourcen-Tag dieser Instance und das Tag des Prinzipals denselben `SerialConsole`-Wert für den Tag-Schlüssel haben.

Weitere Informationen zur Verwendung von Tags zur Steuerung des Zugriffs auf Ihre AWS Ressourcen finden Sie unter Steuern des Zugriffs auf AWS Ressourcen im IAM-Benutzerhandbuch.

Beachten Sie, dass die `DescribeInstances`-, `DescribeInstanceTypes`-, und `GetSerialConsoleAccessStatus`-Aktionen keine Berechtigungen auf Ressourcenebene unterstützen. Daher müssen alle Ressourcen, die durch ein * (Sternchen) gekennzeichnet sind, für diese Aktionen spezifiziert werden.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowTagBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SerialConsole":
 "${aws:PrincipalTag/SerialConsole}"
                }
            }
        }
    ]
}
```

Benutzerkennwort des Betriebssystems auf einer Linux-Instance festlegen

Sie können sich ohne Passwort mit der seriellen Konsole verbinden. Um jedoch die serielle Konsole für die Fehlerbehebung einer Instance verwenden zu können, muss die Instance über einen passwortbasierten Betriebssystem-Benutzer verfügen.

Sie können das Kennwort für jeden Betriebssystembenutzer festlegen, einschließlich des Stammbenutzers. Beachten Sie, dass der Stammbenutzer alle Dateien ändern kann, während jeder Betriebssystembenutzer möglicherweise eingeschränkte Berechtigungen hat.

Sie müssen für jede Instance, für die Sie die serielle Konsole verwenden, ein Benutzerkennwort festlegen. Dies ist eine einmalige Anforderung für jede Instance.

> **Note**
>
> Standardmäßig AWS sind AMIs provided by nicht mit einem kennwortbasierten Benutzer konfiguriert. Wenn Sie Ihre Instance mit einem AMI gestartet haben, für das das Root-Benutzerkennwort bereits konfiguriert ist, können Sie diese Anweisungen überspringen.

Benutzerkennwort des Betriebssystems auf einer Linux-Instance festlegen

1. Verbinden Sie sich mit der Instance. Sie können jede Methode verwenden, um eine Verbindung zu Ihrer Instance herzustellen, mit Ausnahme der Verbindungsmethode EC2 Serial Console.
2. Verwenden Sie den passwd-Befehl, um das Kennwort für einen Benutzer festzulegen. Im folgenden Beispiel ist der Benutzer `root`.

   ```
   [ec2-user ~]$ sudo passwd root
   ```

   Es folgt eine Beispielausgabe.

   ```
   Changing password for user root.
   New password:
   ```

3. Geben Sie an der `New password`-Eingabeaufforderung das neue Passwort ein.
4. Geben Sie an der Eingabeaufforderung das Passwort erneut ein.

Connect zur EC2 seriellen Konsole her

Sie können über die Amazon-Konsole oder über SSH eine Verbindung zur seriellen EC2 Konsole Ihrer EC2 Instance herstellen. Nachdem Sie eine Verbindung zur seriellen Konsole hergestellt haben, können Sie sie zur Fehlerbehebung bei Booten, Netzwerkkonfiguration und anderen Problemen verwenden. Weitere Informationen zur Fehlerbehebung finden Sie unter Beheben Sie Probleme mit Ihrer EC2 Amazon-Instance mithilfe der EC2 seriellen Konsole.

Überlegungen

- Pro Instance wird nur 1 aktive serielle Konsolenverbindung unterstützt.
- Die Verbindung zur seriellen Konsole dauert normalerweise 1 Stunde, außer Sie trennen die Verbindung. Während der Systemwartung unterbricht Amazon jedoch EC2 die serielle Konsolensitzung.

  Die Dauer der Verbindung wird nicht durch die Dauer Ihrer IAM-Anmeldeinformationen bestimmt. Wenn Ihre IAM-Anmeldeinformationen ablaufen, bleibt die Verbindung bestehen, bis die maximale Dauer der seriellen Konsolenverbindung erreicht ist. Wenn Sie die EC2 serielle Konsole verwenden und Ihre IAM-Anmeldeinformationen ablaufen, beenden Sie die Verbindung, indem Sie die Browserseite schließen.
- Es dauert 30 Sekunden, um eine Sitzung abzubrechen, nachdem Sie die Verbindung zur seriellen Konsole getrennt haben, um eine neue Sitzung zuzulassen.
- Unterstützte serielle Konsolenanschlüsse: `ttyS0` (Linux-Instances) und `COM1` (Windows-Instances)
- Wenn Sie eine Verbindung zur seriellen Konsole herstellen, können Sie einen leichten Rückgang des Durchsatzes Ihrer Instance feststellen.

Themen

- Herstellen von Verbindungen über den browserbasierten Client
- Herstellen von Verbindungen über Ihren eigenen Schlüssel und einen SSH-Client
- EC2 Endpunkte und Fingerabdrücke der seriellen Konsole

Herstellen von Verbindungen über den browserbasierten Client

Sie können mithilfe des browserbasierten Clients eine Verbindung zur seriellen Konsole Ihrer EC2 Instance herstellen. Wählen Sie dazu die Instance in der EC2 Amazon-Konsole aus und wählen

Sie, ob Sie eine Verbindung zur seriellen Konsole herstellen möchten. Der browserbasierte Client verarbeitet die Berechtigungen und stellt eine erfolgreiche Verbindung bereit.

EC2 Die serielle Konsole funktioniert in den meisten Browsern und unterstützt Tastatur- und Mauseingaben.

Stellen Sie vor dem Verbinden sicher, dass Sie die Voraussetzungen erfüllt haben.

So stellen Sie mithilfe des browserbasierten Clients (EC2Amazon-Konsole) eine Verbindung zur seriellen Schnittstelle Ihrer Instance her

1. Öffnen Sie die EC2 Amazon-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instanz aus und wählen Sie Aktionen, Überwachung und Fehlerbehebung, EC2 Serielle Konsole, Connect aus.

   Wählen Sie alternativ die Instanz aus und wählen Sie Connect, EC2 Serial Console, Connect.

   Ein Terminalfenster im Browser wird geöffnet.
4. Drücken Sie die Eingabetaste. Wenn eine Anmeldeaufforderung zurückkehrt, sind Sie mit der seriellen Konsole verbunden.

   Wenn der Bildschirm schwarz bleibt, können Sie die folgenden Informationen verwenden, um Probleme bei der Verbindung mit der seriellen Konsole zu beheben:

   - Stellen Sie sicher, dass Sie den Zugriff auf die serielle Konsole konfiguriert haben. Weitere Informationen finden Sie unter Konfigurieren Sie den Zugriff auf die EC2 serielle Konsole.
   - (Nur Linux-Instances) Verwenden Sie diese SysRq Option, um eine Verbindung zur seriellen Konsole herzustellen. SysRq erfordert nicht, dass Sie die Verbindung über den browserbasierten Client herstellen. Weitere Informationen finden Sie unter (Linux-Instanzen) Verwenden Sie diese Option SysRq , um Fehler in Ihrer Instanz zu beheben.
   - (Nur Linux-Instances) Starten Sie getty neu. Wenn Sie SSH-Zugriff auf Ihre Instance haben, stellen Sie mithilfe von SSH eine Verbindung zu Ihrer Instance her und starten Sie Getty mit dem folgenden Befehl neu.

     ```
     [ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
     ```
   - Starten Sie Ihre Instance neu. Sie können Ihre Instance mithilfe von SysRq (Linux-Instances), der EC2 Konsole oder dem AWS CLI neu starten. Weitere Informationen finden Sie unter

(Linux-Instanzen) Verwenden Sie diese Option SysRq , um Fehler in Ihrer Instanz zu beheben (Linux-Instances) oder Eine Amazon-EC2-Instance neu starten.

5. (Nur Linux-Instances) Geben Sie an der `login`-Eingabeaufforderung den Benutzernamen des passwortbasierten Benutzers ein, den Sie zuvor eingerichtet haben, und drücken Sie dann die Eingabetaste.
6. (Nur Linux-Instances) Geben Sie an der `Password`-Eingabeaufforderung das Passwort ein und drücken Sie dann die Eingabetaste.

Herstellen von Verbindungen über Ihren eigenen Schlüssel und einen SSH-Client

Sie können mittels Ihres eigenen SSH-Schlüssels über einen SSH-Client Ihrer Wahl Verbindungen mit Ihrer Instance herstellen, während Sie die serielle Konsolen-API verwenden. Auf diese Weise können Sie die serielle Konsolenfunktion für die Push-Übergabe öffentlicher Schlüssel an Instances nutzen.

Nachdem Sie den SSH-Schlüssel auf die Instance übertragen haben, unterliegt die SSH-Verbindung nicht den IAM-Richtlinien, die Sie konfiguriert haben, um Benutzern Zugriff auf die EC2 serielle Konsole zu gewähren.

Bevor Sie beginnen

Stellen Sie sicher, dass die Voraussetzungen erfüllt sind.

So stellen Sie eine Verbindung mit der seriellen Konsole einer Instance über SSH her

1. Schieben Sie Ihren öffentlichen SSH-Schlüssel auf die Instance, um eine Sitzung der seriellen Konsole zu starten

   Verwenden Sie den Befehl send-serial-console-ssh-public-key, um Ihren öffentlichen SSH-Schlüssel auf die Instance zu übertragen. Dies startet eine serielle Konsolensitzung.

   Wenn für diese Instance bereits eine serielle Konsolensitzung gestartet wurde, schlägt der Befehl fehl, da Sie jeweils nur eine Sitzung geöffnet haben können. Es dauert 30 Sekunden, um eine Sitzung abzubrechen, nachdem Sie die Verbindung zur seriellen Konsole getrennt haben, um eine neue Sitzung zuzulassen.

```
aws ec2-instance-connect send-serial-console-ssh-public-key \
    --instance-id i-001234a4bf70dec41EXAMPLE \
    --serial-port 0 \
```

```
    --ssh-public-key file://my_key.pub \
    --region us-east-1
```

2. Stellen Sie mit Ihrem privaten Schlüssel eine Verbindung zur seriellen Konsole her

   Verwenden Sie den ssh-Befehl, um eine Verbindung mit der seriellen Konsole herzustellen, bevor der öffentliche Schlüssel aus dem seriellen Konsolendienst entfernt wird. Sie haben 60 Sekunden bevor er entfernt wird.

   Verwenden Sie den privaten Schlüssel, der dem öffentlichen Schlüssel entspricht.

   Das Benutzernamenformat, das die Instance-ID und den Port 0 umfasst, ist `instance-id.port0`. Im folgenden Beispiel lautet der Benutzername `i-001234a4bf70dec41EXAMPLE.port0`.

   Der Endpunkt des seriellen Konsolendienstes ist für jede Region unterschiedlich. In der EC2 Endpunkte und Fingerabdrücke der seriellen Konsole Tabelle finden Sie die Endpunkte der einzelnen Regionen. Im folgenden Beispiel befindet sich der serielle Konsolendienst in der Region us-east-1.

   ```
   ssh -i my_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-connect.us-east-1.aws
   ```

   Im folgenden Beispiel wird `timeout 3600` verwendet, um Ihre SSH-Sitzung nach 1 Stunde zu beenden. Während der Sitzung gestartete Prozesse können auch nach Beendigung der Sitzung auf Ihrer Instance weiter ausgeführt werden.

   ```
   timeout 3600 ssh -i my_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-connect.us-east-1.aws
   ```

3. (Optional) Überprüfen Sie den Fingerabdruck

   Wenn Sie zum ersten Mal eine Verbindung mit der seriellen Konsole herstellen, werden Sie aufgefordert, den Fingerabdruck zu überprüfen. Sie können den Fingerabdruck der seriellen Konsole mit dem Fingerabdruck vergleichen, der zur Überprüfung angezeigt wird. Wenn diese Fingerabdrücke nicht übereinstimmen, versucht möglicherweise jemand einen "" -Angriff. man-in-the-middle Wenn sie übereinstimmen, können Sie sich sicher mit der seriellen Konsole verbinden.

Der folgende Fingerabdruck gilt für den seriellen Konsolendienst in der Region us-east-1. Informationen zu den Fingerabdrücken für die einzelnen Regionen finden Sie unter EC2 Endpunkte und Fingerabdrücke der seriellen Konsole.

```
SHA256:dXwn5ma/xadVMeBZGEru5l2gx+yI5LDiJaLUcz0FMmw
```

Der Fingerabdruck wird nur angezeigt, wenn Sie zum ersten Mal eine Verbindung mit der seriellen Konsole herstellen.

4. Drücken Sie die Eingabetaste. Wenn eine Eingabeaufforderung zurückkehrt, sind Sie mit der seriellen Konsole verbunden.

   Wenn der Bildschirm schwarz bleibt, können Sie die folgenden Informationen verwenden, um Probleme bei der Verbindung mit der seriellen Konsole zu beheben:

   - Stellen Sie sicher, dass Sie den Zugriff auf die serielle Konsole konfiguriert haben. Weitere Informationen finden Sie unter Konfigurieren Sie den Zugriff auf die EC2 serielle Konsole.
   - (Nur Linux-Instanzen) Wird verwendet SysRq , um eine Verbindung zur seriellen Konsole herzustellen. SysRq erfordert nicht, dass Sie eine Verbindung über SSH herstellen. Weitere Informationen finden Sie unter (Linux-Instanzen) Verwenden Sie diese Option SysRq , um Fehler in Ihrer Instanz zu beheben.
   - (Nur Linux-Instances) Starten Sie getty neu. Wenn Sie SSH-Zugriff auf Ihre Instance haben, stellen Sie mithilfe von SSH eine Verbindung zu Ihrer Instance her und starten Sie Getty mit dem folgenden Befehl neu.

     ```
     [ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
     ```

   - Starten Sie Ihre Instance neu. Sie können Ihre Instance neu starten, indem Sie SysRq (nur Linux-Instances), die EC2 Konsole oder den AWS CLI verwenden. Weitere Informationen finden Sie unter (Linux-Instanzen) Verwenden Sie diese Option SysRq , um Fehler in Ihrer Instanz zu beheben (nur Linux-Instances) oder Eine Amazon-EC2-Instance neu starten.

5. (Nur Linux-Instances) Geben Sie an der `login`-Eingabeaufforderung den Benutzernamen des passwortbasierten Benutzers ein, den Sie zuvor eingerichtet haben, und drücken Sie dann die Eingabetaste.
6. (Nur Linux-Instances) Geben Sie an der `Password`-Eingabeaufforderung das Passwort ein und drücken Sie dann die Eingabetaste.

EC2 Endpunkte und Fingerabdrücke der seriellen Konsole

Im Folgenden sind die Service-Endpunkte und Fingerabdrücke für die serielle Konsole aufgeführt. EC2 Um programmgesteuert eine Verbindung zur seriellen Konsole einer Instanz herzustellen, verwenden Sie einen EC2 Serial Console-Endpunkt. Die Endpunkte und Fingerabdrücke der EC2 seriellen Konsole sind für jede Region einzigartig. AWS

Name der Region	Region	Endpoint	Fingerabdruck
USA Ost (Ohio)	us-east-2	serial-console.ec2-instance-connect.us-east-2.aws	SHA256: EhwPkTzRt TY7 TRSzz26 RM7m xbb0/HVV9J CZN0xw/ d/0
USA Ost (Nord-Virginia)	us-east-1	serial-console.ec2-instance-connect.us-east-1.aws	SHA256: VMe BZGEru5l2gx LDi xBB0/HVV9J CZN0xW/d/0 ----SEP -----: DXWN5mA/xAD +yl5 Ja 0 LUcz FMmw
USA West (Nordkalifornien)	us-west-1	serial-console.ec2-instance-connect.us-west-1.aws	SHA256: H3Y OHldlc MET8u7 QLSX3jm RTRAPFHVtqbyo LZBMUCqi
USA West (Oregon)	us-west-2	serial-console.ec2-instance-connect.us-west-2.aws	SHA256: O2Jx EMCIe23 TqKa BI6y GHainq ZcMwqNkDhh AVHa1 VUc
Afrika (Kapstadt)	af-south-1	ec2-serial-console.af-south-1.api.aws	SHA256: O5JL2 21ed00biiwi RMWWZ2f VePe JUqzj KIg XsczoHlz
Asien-Pazifik (Hongkong)	ap-east-1	ec2-serial-console.ap-east-1.api.aws	SHA256: lpiXxCho ZHpln o5JL2 XVi

Name der Region	Region	Endpoint	Fingerabdruck
			21ED00BIIWI ---- SEP -----: T0Q1 AKJBP7TKM2x C9b Ynifk JFsj
Asien-Pazifik (Hyderabad)	ap-south-2	ec2-serial-console.ap-south-2.api.aws	SHA256: WJg PBSw V4/Sun+ 15 OPITValoew AuYj DVW845 JEh DKRs
Asien-Pazifik (Jakarta)	ap-southeast-3	ec2-serial-console.ap-southeast-3.api.aws	SHA256: ZwgrCh V4/Sun+ XITq 15 YFqy3o8m ----sep----:5 +lfns32 l/4O0ZIFB X4BZGS Ik
Asien-Pazifik (Malaysia)	ap-southeast-5	ec2-serial-console.ap-southeast-5.api.aws	SHA256QXT HQMRcqRdI jmAGoAMBS ExeoRobYyRwec2-serial-console.ap-southeast-5.api.aws ----sep----:c T67 A yTjnEi
Asien-Pazifik (Melbourne)	ap-southeast-4	ec2-serial-console.ap-southeast-4.api.aws	SHA256:c hFgLvjn T67 TSSh A GG46wf ZJv ----SEP----:AVAQ27 5g Z0OV7H90P0 oET6 M

Name der Region	Region	Endpoint	Fingerabdruck
Asien-Pazifik (Mumbai)	ap-south-1	serial-console.ec2-instance-connect.ap-south-1.aws	SHA256:Avaq27 BLXc 5g HHEbli ARx TPi SM35 Z0ov7H90P 0 oeT6 M ----sep----:o Ymklq egh8ISO51 REZ BSU40
Asia Pacific (Osaka)	ap-northeast-3	ec2-serial-console.ap-northeast-3.api.aws	SHA256:o BKBn BuFnHr Ymklq EV3 egh8iso51REZ BSU40 ----sep---:AM0/Ji 9axSG G8tu/vvhfxe/3ucyJSQ
Asien-Pazifik (Seoul)	ap-northeast-2	serielle Konsole.ec2-instance-connect.ap-northeast-2.aws	SHA256:AM0/Ji NTztg9 PK49 WYMq 9axSG G8TU/VVHF XE/3UCYJSQ ZM2d ----SEP----:FOQWXN X+DZ++GU bx+FRC SRQRi
Asien-Pazifik (Singapur)	ap-southeast-1	serial-console.ec2-instance-connect.ap-southeast-1.aws	SHA256: Ein Lu1Gy/ L8 Zuac6L45C oY PLFNn7 CQDHx3qmw TUX7 LQg
Asien-Pazifik (Sydney)	ap-southeast-2	serial-console.ec2-instance-connect.ap-southeast-2.aws	SHA256: yFvMw UK9l EUQj QTRo XXzu VSe9 N+Cw9/W98 4Cf5Tgzo4

Name der Region	Region	Endpoint	Fingerabdruck
Asien-Pazifik (Thailand)	ap-southeast-7	ec2-serial-console.ap-southeast-7.api.aws	SHA256: R1q2lqsg7 2wmj DY KCAZi RYr vTwixWmvc VT31 XRg SdEf
Asien-Pazifik (Tokio)	ap-northeast-1	serial-console.ec2-instance-connect.ap-northeast-1.aws	SHA256: RQfs DCZTOf Qawew Em/ TRDV1t9 + HMr FQe CRl IOT5um4k
Kanada (Zentral)	ca-central-1	serial-console.ec2-instance-connect.ca-central-1.aws	SHA256: OZwmp Qawew YW738 FIOTHd UTy Em/ + ----SEP----:P2O2J mWKPO6 EV2Gcz YMMO7s4
Kanada West (Calgary)	ca-west-1	ec2-serial-console.ca-west-1.api.aws	SHA256:P2O2J mWKPO6 EV2GCZ ----SEP----:S3RC8L I2XHBHR3IEDJ 6Q JNx GAFLPGOLjx7 IxxXrGckk
China (Beijing)	cn-north-1	ec2-serial-console .cn-north-1.api.am azonwebservices.co m.cn	SHA256:S3 RC8LI2XHBHR3IEDJ 6Q ----sep----:2 g H7UU3+WA D28V/ LGGT+Y HVFy4 FUx ggMeqjvSlgngpg

Name der Region	Region	Endpoint	Fingerabdruck
China (Ningxia)	cn-northwest-1	appmesh.cn-northwest-1.api.amazonwebservices.com.cn	SHA256: 2 g NZki QOd H7UU3+WA YEBUh D28V/LGGT +Y ---------: TDGR Vf o4SZUA09 M VWI5r YOZGTogpwmi
Europa (Frankfurt)	eu-central-1	serial-console.ec2-instance-connect.eu-central-1.aws	SHA256:Tdgr yIcOd OlkXvOl Vf JJ3 O4SZUA09 M ----sep----:ACMFS/ 8AMZ1TOE+BBNR FY0K0DE2C
Europa (Irland)	eu-west-1	serial-console.ec2-instance-connect.eu-west-1.aws	SHA256:ACMFS/ GAWO4 qTrHj ZAw CW6 8AMZ1TOE+ BBNR FY0K0DE2C ----SEP----:H2AA HATHHTM6E ZS3BJ7UDGUXI2 E
Europa (London)	eu-west-2	serial-console.ec2-instance-connect.eu-west-2.aws	SHA256:H2AA CE/ AEG4Amm53I6lkD1 ZPvS/BCV TPW2 RnJg HAthHTM6E ZS3BJ7UDGUXI2 E ----sep----:a69rd5 3t 8
Europa (Milan)	eu-south-1	ec2-serial-console.eu-south-1.api.aws	SHA256:a69rd5 OVJnpg 3t BVrxn 8 ----sep----:LC0K Fy 0A7N99eCLB S7X7 0 XSX95cuu QK3

Name der Region	Region	Endpoint	Fingerabdruck
Europa (Paris)	eu-west-3	serial-console.ec2-instance-connect.eu-west-3.aws	SHA256:LC0K FVng Fy RPAr 0A7N99ECLB S7X7 0 ----SEP----:Q8LDNA F9PYMENE8BN Y3 / kxsw JUzfrlxe EWs
Europa (Spain)	eu-south-2	ec2-serial-console.eu-south-2.api.aws	SHA256:Q8 LDNAF9PYM ENE8BN Y3 /kxsw CW2 DFRlu669 QNxq FxEcs ----SEP----:GO R6f /4F4N7T45 ZUz ZcwoEc
Europa (Stockholm)	eu-north-1	serial-console.ec2-instance-connect.eu-north-1.aws	SHA256:Go GFFUVUDvoc R6f GSS3 /4F4N7T45 ----sep----:tk Di CU8GDL6W2ui32 X84 EPNp KFKLw
Europa (Zürich)	eu-central-2	ec2-serial-console.eu-central-2.api.aws	SHA256:tk BMf6 WdCw Di NUlz CU8GDL6W2 UI32 X84 ----sep---:8PPX2M 0 KFWM4/ IfRz 4Oa XFut QXWp6mk
Israel (Tel Aviv)	il-central-1	ec2-serial-console.il-central-1.api.aws	SHA256: + Nm JR6q8v6k NNPi8 QSFQ4dj5dim M1 Yu ZPTgwgs SNvt

Name der Region	Region	Endpoint	Fingerabdruck
Mexiko (Zentral)	mx-central-1	ec2-serial-console .mx-central-1.api.aws	SHA256: BCu VL13i QNk + 18EF4P2 FETB32GS0 CcVnt ZHUr BBAOxl
Naher Osten (Bahrain)	me-south-1	ec2-serial-console .me-south-1.api.aws	SHA256: LLKHu2 QnLdUq VL13i VArso + PJOMRJKCB z CDq 18EF4P2 FETB32GS0 ----SEP---:NPJ 2k K5xV C3k8
Naher Osten (VAE)	me-central-1	ec2-serial-console .me-central-1.api.aws	SHA256:NPJ dFwPeyyk 2k MPBYh K5xV XNe FSDKBv C3K8 ----SEP---:ZPB5DUKIBZ+L0 B4 I/Xz LE
Südamerika (São Paulo)	sa-east-1	serial-console.ec2-instance-connect.sa-east-1.aws	SHA256:ZP B5DUKIBZ+L0 B4 I/Xz LE ----sep----:RD2+/3 2OGNJEW1Y QZC +BOTBIH62OQ I VIem ENa APDq1d
AWS GovCloud (USA-Ost)	us-gov-east-1	serielle Konsole.ec2-Instanzenverbindung.us-gov-east-1.amazonaws.com	SHA256GWs oyLCIrtvu38YEEh-1.amazonaws.com ----SEP----:TIWE19 + F28 DHIkqn DcZnmtebv

Name der Region	Region	Endpoint	Fingerabdruck
AWS GovCloud (USA-West)	us-gov-west-1	serielle Konsole.ec2-Instanzenverbindung.us-gov-west-1.amazonaws.com	SHA256-1.amazonaws.com ----sep----:kf b +UTBD3BRF8 8n iW5DQ OFRWLa OZf OlPf GO2 YZLq XZi

Trennen Sie die Verbindung zur seriellen Konsole EC2

Wenn Sie nicht mehr mit der EC2 seriellen Konsole Ihrer Instance verbunden sein müssen, können Sie die Verbindung zu dieser trennen. Wenn Sie die Verbindung zur seriellen Konsole trennen, wird jede Shell-Sitzung, die auf der Instance ausgeführt wird, weiterhin ausgeführt. Wenn Sie die Shell-Sitzung beenden möchten, müssen Sie sie beenden, bevor Sie die Verbindung zur seriellen Konsole trennen.

Überlegungen

- Die Verbindung zur seriellen Konsole dauert normalerweise 1 Stunde, sofern Sie sie nicht beenden. Während der Systemwartung unterbricht Amazon jedoch EC2 die serielle Konsolensitzung.
- Es dauert 30 Sekunden, um eine Sitzung abzubrechen, nachdem Sie die Verbindung zur seriellen Konsole getrennt haben, um eine neue Sitzung zuzulassen.

Die Art und Weise, wie die Verbindung zur seriellen Konsole getrennt wird, hängt vom Client ab.

Browserbasierter Client

Um die Verbindung zur seriellen Konsole zu trennen, schließen Sie das Terminalfenster der seriellen Konsole im Browser.

Standard-OpenSSH-Client

Um die Verbindung zur seriellen Konsole zu trennen, verwenden Sie den folgenden Befehl, um die SSH-Verbindung zu schließen. Dieser Befehl muss unmittelbar nach einer neuen Zeile ausgeführt werden.

```
~.
```

Der Befehl, den Sie zum Schließen einer SSH-Verbindung verwenden, kann je nach verwendetem SSH-Client unterschiedlich sein.

Beheben Sie Probleme mit Ihrer EC2 Amazon-Instance mithilfe der EC2 seriellen Konsole

Mithilfe der EC2 seriellen Konsole können Sie Boot-, Netzwerkkonfigurations- und andere Probleme beheben, indem Sie eine Verbindung zur seriellen Schnittstelle Ihrer Instance herstellen.

Verwenden Sie die Anleitung für das Betriebssystem Ihrer Instance und für das Tool, das Sie auf Ihrer Instance konfiguriert haben.

Tools

- (Linux-Instances) GRUB verwenden, um Fehler in Ihrer Instance zu beheben
- (Linux-Instanzen) Verwenden Sie diese Option SysRq , um Fehler in Ihrer Instanz zu beheben
- (Windows-Instances) SAC zur Fehlerbehebung Ihrer Instance verwenden

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie die Voraussetzungen erfüllt haben, einschließlich der Konfiguration Ihres ausgewählten Tools zur Fehlerbehebung.

(Linux-Instances) GRUB verwenden, um Fehler in Ihrer Instance zu beheben

GNU GRUB (kurz für GNU GRand Unified Bootloader, allgemein als GRUB bezeichnet) ist der Standard-Bootloader für die meisten Linux-Betriebssysteme. Im GRUB-Menü können Sie auswählen, in welchen Kernel Sie booten möchten oder Menüeinträge ändern, um den Bootvorgang des Kernels zu ändern. Dies kann bei der Problembehandlung einer fehlerhaften Instance nützlich sein.

Das GRUB-Menü wird während des Startvorgangs angezeigt. Das Menü ist nicht über normales SSH zugänglich, aber Sie können es über die serielle Konsole aufrufen. EC2

Sie können in den Einzelbenutzermodus oder in den Notfallmodus starten. Der Einzelbenutzermodus bootet den Kernel auf ein niedrigeres Runlevel. Zum Beispiel könnte es das Dateisystem einhängen, aber das Netzwerk nicht aktivieren, was Ihnen die Möglichkeit gibt, die Wartung durchzuführen, die

zum Reparieren der Instance erforderlich ist. Der Notfallmodus ähnelt dem Einzelbenutzermodus, mit der Ausnahme, dass der Kernel auf dem niedrigsten möglichen Runlevel läuft.

So booten Sie in den Einzelbenutzermodus

1. Stellen Sie eine Verbindung mit der seriellen Konsole der Instance her.
2. Starten Sie die Instance mit dem folgenden Befehl neu.

   ```
   [ec2-user ~]$ sudo reboot
   ```

3. Wenn während des Neustarts das GRUB-Menü angezeigt wird, drücken Sie eine beliebige Taste, um den Bootvorgang zu beenden.
4. Verwenden Sie im GRUB-Menü die Pfeiltasten, um den zu bootenden Kernel auszuwählen, und drücken Sie e auf Ihrer Tastatur.
5. Verwenden Sie die Pfeiltasten, um den Cursor in der Zeile zu finden, die den Kernel enthält. Die Zeile beginnt mit `linux` oder `linux16`, abhängig von dem AMI, das zum Starten der Instance verwendet wurde. Für Ubuntu beginnen zwei Zeilen mit `linux`, die beide im nächsten Schritt geändert werden müssen.
6. Am Ende der Zeile fügen Sie das Wort `single` hinzu.

   Im Folgenden finden Sie ein Beispiel für Amazon Linux 2.

   ```
   linux /boot/vmlinuz-4.14.193-149.317.amzn2.aarch64 root=UUID=d33f9c9a-\
   dadd-4499-938d-ebbf42c3e499 ro  console=tty0 console=ttyS0,115200n8 net.ifname\
   s=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.she\
   ll=0 single
   ```

7. Drücken Sie Strg+X, um in den Einzelbenutzermodus zu starten.
8. Geben Sie an der `login`-Eingabeaufforderung den Benutzernamen des passwortbasierten Benutzers ein, den Sie vorher eingerichtet haben, und drücken Sie dann die Eingabetaste.
9. Geben Sie an der `Password`-Eingabeaufforderung das Passwort ein und drücken Sie dann die Eingabetaste.

In den Notfallmodus starten

Gehen Sie genauso vor wie im Einzelbenutzermodus, fügen Sie jedoch in Schritt 6 das Wort `emergency` anstelle von `single` hinzu.

(Linux-Instanzen) Verwenden Sie diese Option SysRq , um Fehler in Ihrer Instanz zu beheben

Der Schlüssel System Request (SysRq), der manchmal auch als SysRq „Magic“ bezeichnet wird, kann verwendet werden, um dem Kernel direkt außerhalb einer Shell einen Befehl zu senden, und der Kernel wird antworten, unabhängig davon, was der Kernel tut. Wenn die Instanz beispielsweise nicht mehr reagiert, können Sie den SysRq Schlüssel verwenden, um dem Kernel mitzuteilen, dass er abstürzen oder neu starten soll. Weitere Informationen finden Sie unter Magic SysRq Key in Wikipedia.

Sie können SysRq Befehle im browserbasierten EC2 Serial Console-Client oder in einem SSH-Client verwenden. Der Befehl zum Senden einer Unterbrechungsanfrage ist für jeden Client unterschiedlich.

Wählen Sie zur Verwendung SysRq je nach verwendetem Client eines der folgenden Verfahren aus.

Browser-based client

Zur Verwendung SysRq in der seriellen Konsole (browserbasierter Client)

1. Stellen Sie eine Verbindung mit der seriellen Konsole der Instance her.
2. Um eine Unterbrechungsanfrage zu senden, drücken Sie `CTRL+0` (Null). Wenn Ihre Tastatur dies unterstützt, können Sie auch eine Unterbrechungsanfrage mit der Pause- oder Break-Taste senden.

   ```
   [ec2-user ~]$ CTRL+0
   ```

3. Um einen SysRq Befehl auszuführen, drücken Sie die Taste auf Ihrer Tastatur, die dem gewünschten Befehl entspricht. Um beispielsweise eine Liste mit SysRq Befehlen anzuzeigen, drücken Sieh.

   ```
   [ec2-user ~]$ h
   ```

   Der h-Befehl gibt etwas Ähnliches wie das Folgende aus.

   ```
   [ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
   tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
   ```

```
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
buffer(z)
```

SSH client

Zur Verwendung SysRq in einem SSH-Client

1. Stellen Sie eine Verbindung mit der seriellen Konsole der Instance her.
2. Um eine Unterbrechungsanfrage zu senden, drücken Sie ~B (Tilde, gefolgt von Großbuchstaben B).

```
[ec2-user ~]$ ~B
```

3. Um einen SysRq Befehl auszuführen, drücken Sie die Taste auf Ihrer Tastatur, die dem gewünschten Befehl entspricht. Um beispielsweise eine Liste mit SysRq Befehlen anzuzeigen, drücken Sieh.

```
[ec2-user ~]$ h
```

Der h-Befehl gibt etwas Ähnliches wie das Folgende aus.

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
buffer(z)
```

> **Note**
>
> Der Befehl, den Sie zum Senden einer Unterbrechungsanfrage verwenden, kann je nach verwendetem SSH-Client unterschiedlich sein.

(Windows-Instances) SAC zur Fehlerbehebung Ihrer Instance verwenden

Die Special-Admin-Console(SAC)-Funktion von Windows bietet eine Möglichkeit zur Fehlerbehebung einer Windows-Instance. Wenn Sie eine Verbindung zur seriellen Konsole der Instance herstellen und SAC verwenden, können Sie den Startvorgang unterbrechen und Windows im abgesicherten Modus starten.

> **Note**
>
> Wenn Sie SAC auf einer Instance aktivieren, funktionieren die EC2 Dienste, die auf den Kennwortabruf angewiesen sind, nicht von der EC2 Amazon-Konsole aus. Die EC2 Startagenten von Windows auf Amazon (EC2Config, EC2 Launch v1 und EC2 Launch v2) benötigen die serielle Konsole, um verschiedene Aufgaben auszuführen. Diese Aufgaben werden nicht erfolgreich ausgeführt, wenn Sie SAC für eine Instance aktivieren. Weitere Informationen zu Windows on Amazon EC2 Launch Agents finden Sie unterthe section called “Konfigurieren Ihrer Windows-Instance”. Wenn Sie SAC aktivieren, können Sie es später deaktivieren. Weitere Informationen finden Sie unter Deaktivieren von SAC und vom Boot-Menü.

Aufgaben

- Verwenden von SAC
- Verwenden des Boot-Menüs
- Deaktivieren von SAC und vom Boot-Menü

Verwenden von SAC

So verwenden Sie SAC

1. Stellen Sie eine Verbindung mit der seriellen Konsole her.

   Wenn SAC auf der Instance aktiviert ist, zeigt die serielle Konsole die `SAC>`-Anfrage an.

```
Computer is booting, SAC started and initialized.

Use the "ch -?" command for information about using channels.
Use the "?" command for general help.


SAC>?
EVENT: The CMD command is now available.
SAC
```

2. Geben Sie zum Anzeigen der SAC-Befehle „?“ ein und drücken Sie dann die Eingabetaste.

   Erwartete Ausgabe

```
SAC>?
ch                      Channel management commands.  Use ch -? for more help.
cmd                     Create a Command Prompt channel.
d                       Dump the current kernel log.
f                       Toggle detailed or abbreviated tlist info.
? or help               Display this list.
i                       List all IP network numbers and their IP addresses.
i <#> <ip> <subnet> <gateway> Set IPv4 addr., subnet and gateway.
id                      Display the computer identification information.
k <pid>                 Kill the given process.
l <pid>                 Lower the priority of a process to the lowest possible.
lock                    Lock access to Command Prompt channels.
m <pid> <MB-allow>      Limit the memory usage of a process to <MB-allow>.
p                       Toggle paging the display.
r <pid>                 Raise the priority of a process by one.
s                       Display the current time and date (24 hour clock used).
s mm/dd/yyyy hh:mm      Set the current time and date (24 hour clock used).
t                       Tlist.
restart                 Restart the system immediately.
shutdown                Shutdown the system immediately.
crashdump               Crash the system. You must have crash dump enabled.
```

3. Um einen Eingabeaufforderungskanal (z. B. `cmd0001` oder `cmd0002`) zu erstellen, geben Sie cmd ein und drücken Sie dann die Eingabetaste.
4. Um den Eingabeaufforderungskanal anzuzeigen, drücken Sie ESC und drücken Sie dann auf TAB.

   Erwartete Ausgabe

```
Name:                 Cmd0001
Description:          Command
Type:                 VT-UTF8
Channel GUID:         ef9f20a0-1287-11eb-82b0-0e4ba51872e5
Application Type GUID: 63d02271-8aa4-11d5-bccf-00b0d014a2d0

Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.
```

5. Um Kanäle zu wechseln, drücken Sie ESC+Tab+Kanalnummer gleichzeitig. Um zum Beispiel zum `cmd0002`-Kanal (falls er erstellt wurde) zu wechseln, drücken Sie ESC+TAB+2.
6. Geben Sie die für den Eingabeaufforderungskanal erforderlichen Anmeldeinformationen ein.

```
Please enter login credentials.
Username: Administrator
Domain  : .
Password: *******
```

Die Eingabeaufforderung ist dieselbe voll funktionsfähige Command Shell, die Sie auf einem Desktop erhalten, mit der Ausnahme, dass sie das Lesen von bereits ausgegebenen Zeichen nicht zulässt.

```
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>diskpart

Microsoft DiskPart version 10.0.17763.1

Copyright (C) Microsoft Corporation.
On computer: EC2AMAZ-ASR4SAI

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           30 GB      0 B
  Disk 1    Online           46 GB    46 GB

DISKPART>
```

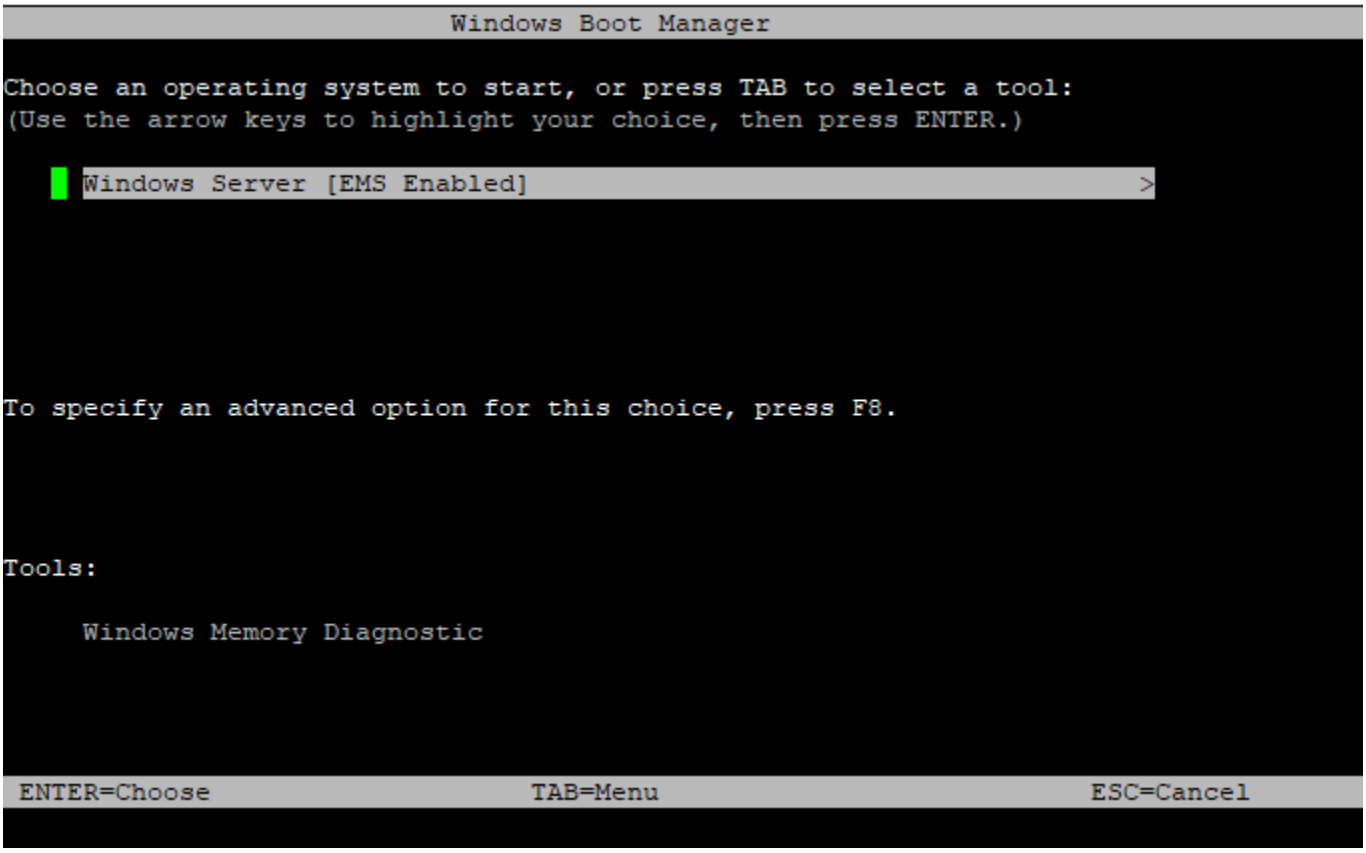
PowerShell kann auch von der Befehlszeile aus verwendet werden.

Beachten Sie, dass Sie möglicherweise die Einstellung Fortschritt auf den stillen Modus festlegen müssen.

```
PS C:\Windows\system32> $ProgressPreference="SilentlyContinue"
PS C:\Windows\system32> $computerInfo = Get-ComputerInfo
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Name
Intel(R) Xeon(R) Platinum 8124M CPU @ 3.00GHz
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Description
Intel64 Family 6 Model 85 Stepping 4
PS C:\Windows\system32>
```

Verwenden des Boot-Menüs

Wenn für die Instance das Boot-Menü aktiviert ist und nach der Verbindung über SSH neu gestartet wird, sollten Sie das Startmenü wie folgt sehen.



Befehle im Boot-Menü

EINGEBEN

Startet den ausgewählten Eintrag des Betriebssystems.

Tabulatortaste

Wechselt zum Tools-Menü.

ESC

Bricht die Instance ab und startet sie neu.

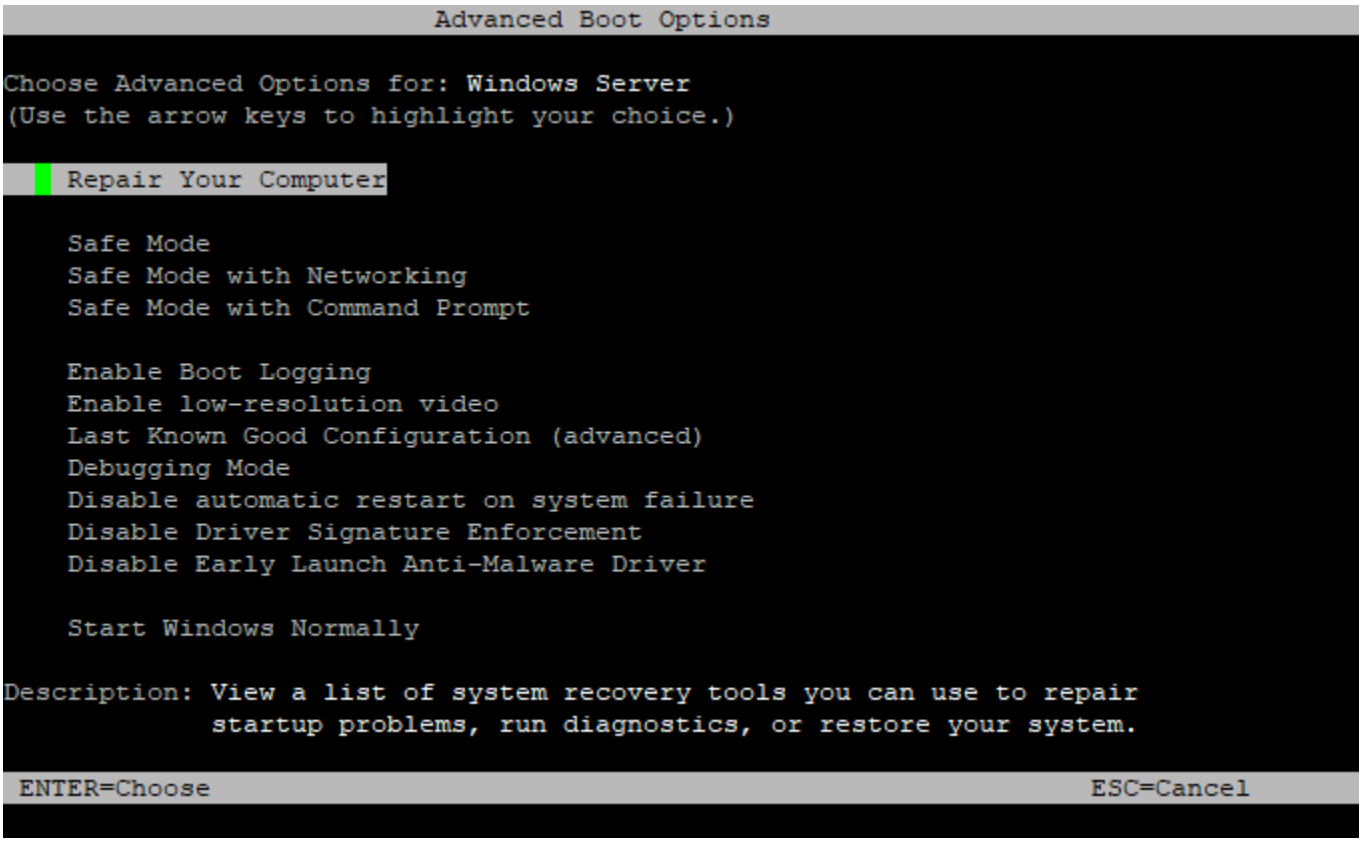
ESC, gefolgt von 8

Entspricht dem Drücken von F8. Zeigt erweiterte Optionen für das ausgewählte Element an.

ESC-Taste + linke Pfeiltaste

Geht zurück zum anfänglichen Boot-Menü.

Die ESC-Taste allein bringt Sie nicht zurück zum Hauptmenü, da Windows darauf wartet, zu sehen, ob eine Escapesequenz läuft.



Deaktivieren von SAC und vom Boot-Menü

Wenn Sie SAC und das Boot-Menü aktivieren, können Sie diese Funktionen später deaktivieren.

Verwenden Sie eine der folgenden Methoden, um SAC und das Boot-Menü einer Instance zu deaktivieren.

PowerShell

So deaktivieren Sie SAC und das Boot-Menü auf einer Windows-Instance

1. Connect zu Ihrer Instance her und führen Sie die folgenden Schritte von einer PowerShell Befehlszeile mit erhöhten Rechten aus.
2. Deaktivieren Sie zuerst das Boot-Menü, indem Sie den Wert in no ändern.

```
bcdedit /set '{bootmgr}' displaybootmenu no
```

3. Deaktivieren Sie dann SAC, indem Sie den Wert auf `off` setzen.

```
bcdedit /ems '{current}' off
```

4. Wenden Sie die aktualisierte Konfiguration an, indem Sie die Instance neu starten.

```
shutdown -r -t 0
```

Command prompt

So deaktivieren Sie SAC und das Boot-Menü auf einer Windows-Instance

1. Stellen Sie eine Verbindung mit Ihrer Instance her und führen Sie die folgenden Schritte an der Eingabeaufforderung aus.
2. Deaktivieren Sie zuerst das Boot-Menü, indem Sie den Wert in no ändern.

```
bcdedit /set {bootmgr} displaybootmenu no
```

3. Deaktivieren Sie dann SAC, indem Sie den Wert auf `off` setzen.

```
bcdedit /ems {current} off
```

4. Wenden Sie die aktualisierte Konfiguration an, indem Sie die Instance neu starten.

```
shutdown -r -t 0
```

Senden Sie einen Diagnose-Interrupt, um eine nicht erreichbare Amazon-Instance zu debuggen EC2

> **Warning**
>
> Diagnose-Interrupts sind für fortgeschrittene Benutzer vorgesehen. Eine falsche Verwendung kann sich negativ auf Ihre Instance auswirken. Das Senden eines Diagnose-Interrupts an eine Instance kann zum Absturz und Neustart einer Instance führen, was unter Umständen den Verlust von Daten zur Folge hat.

Sie können eine Diagnose-Unterbrechung an eine nicht erreichbare oder nicht reagierende Instance senden, um manuell eine Kernel-Panik für eine Linux-Instance oder einen Anhalte-Fehler (allgemein als Bluescreen-Fehler bezeichnet) für eine Windows-Instance auszulösen.

Linux-Instances

Linux-Betriebssysteme stürzen bei einer Kernel-Panik gewöhnlich ab und werden neu gestartet. Das spezifische Verhalten des Betriebssystems ist von seiner Konfiguration abhängig. Mit einer Kernel-Panik kann das Betriebssystem der Instance auch zum Ausführen von Aufgaben, z. B. Generieren einer Dump-Datei, veranlasst werden. Sie können dann mithilfe der Informationen in der Absturzabbilddatei eine Ursachenanalyse durchführen und die Instance debuggen. Die Absturzabbilddaten werden lokal von dem Betriebssystem auf der Instance selbst erstellt.

Windows-Instances

Im Allgemeinen stürzen Windows-Betriebssysteme ab und werden neu gestartet, wenn ein Abbruchfehler auftritt, das spezifische Verhalten hängt aber von seiner Konfiguration ab. Ein Abbruchfehler kann auch bewirken, dass das Betriebssystem Debugging-Informationen, wie z. B. ein Kernel-Speicherabbild, in einer Datei ausgibt. Sie können anhand dieser Informationen eine Ursachenanalyse durchführen, um die Instance zu debuggen. Die Speicherabbilddaten werden lokal von dem Betriebssystem auf der Instance selbst erstellt.

Bevor Sie ein Diagnose-Interrupt an Ihre Instance senden, empfehlen wir Ihnen, die Dokumentation für Ihr Betriebssystem zu konsultieren und anschließend die erforderlichen Konfigurationsänderungen vorzunehmen.

Inhalt

- Unterstützte Instance-Typen
- Voraussetzungen
- Senden eines Diagnose-Interrupts

Unterstützte Instance-Typen

Der Diagnose-Interrupt wird auf allen Nitro-basierten Instance-Typen unterstützt, mit Ausnahme derjenigen, die von Graviton-Prozessoren angetrieben werden. AWS Weitere Informationen finden Sie unter Instances, die auf dem AWS Nitro System und Graviton basieren.AWS

Voraussetzungen

Bevor Sie einen Diagnose-Interrupt verwenden, müssen Sie das Betriebssystem der Instance entsprechend konfigurieren. Dadurch wird sichergestellt, dass die Aktionen ausgeführt werden, die Sie benötigen, wenn eine Kernel-Panik (Linux-Instances) oder ein Stop-Fehler (Windows-Instances) auftritt.

Linux-Instances

Amazon Linux 2 oder Amazon Linux 2023 zum Generieren eines Absturzabbildes bei Auftreten einer Kernel-Panik konfigurieren

1. Verbinden Sie sich mit der Instance.
2. Installieren Sie kexec und kdump.

   ```
   [ec2-user ~]$ sudo yum install kexec-tools -y
   ```

3. Konfigurieren Sie den Kernel zum Reservieren einer angemessenen Menge an Arbeitsspeicher für den sekundären Kernel. Die Menge an Arbeitsspeicher ist von dem insgesamt verfügbaren Arbeitsspeicher Ihrer Instance abhängig. Öffnen Sie die Datei `/etc/default/grub` in Ihrem bevorzugten Texteditor, suchen Sie die Zeile, die mit `GRUB_CMDLINE_LINUX_DEFAULT` beginnt, und fügen Sie dann den Parameter `crashkernel` im folgenden Format hinzu: `crashkernel=`*`memory_to_reserve`*. Um beispielsweise `256MB` zu reservieren, ändern Sie die Datei `grub` wie folgt ab:

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="crashkernel=256M console=tty0 console=ttyS0,115200n8
    net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
    rd.shell=0"
   ```

```
GRUB_TIMEOUT=0
GRUB_DISABLE_RECOVERY="true"
```

4. Speichern Sie Ihre Änderungen und schließen Sie die Datei `grub`.
5. Erstellen Sie die GRUB2 Konfigurationsdatei neu.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

6. Bei Instances auf Intel- und AMD-Prozessoren sendet der Befehl `send-diagnostic-interrupt` einen unbekannten nicht maskierbaren Interrupt (NMI) an die Instance. Sie müssen den Kernel so konfigurieren, dass er bei Eingang des unbekannten NMI abstürzt. Öffnen Sie die Datei `/etc/sysctl.conf` mit Ihrem bevorzugten Texteditor und fügen Sie Folgendes hinzu.

```
kernel.unknown_nmi_panic=1
```

7. Starten Sie Ihre Instance neu und richten Sie wieder eine Verbindung zu ihr ein.
8. Vergewissern Sie sich, dass der Kernel mit dem richtigen `crashkernel`-Parameter gestartet wurde.

```
$ grep crashkernel /proc/cmdline
```

   Die folgende Beispielausgabe weist auf eine erfolgreiche Konfiguration hin.

```
BOOT_IMAGE=/boot/vmlinuz-4.14.128-112.105.amzn2.x86_64 root=UUID=a1e1011e-
e38f-408e-878b-fed395b47ad6 ro crashkernel=256M console=tty0 console=ttyS0,115200n8
 net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
 rd.shell=0
```

9. Überprüfen Sie, ob der kdump-Service ausgeführt wird.

```
[ec2-user ~]$ systemctl status kdump.service
```

   Die folgende Beispielausgabe zeigt das Ergebnis, wenn der Service kdump derzeit ausgeführt wird.

```
kdump.service - Crash recovery kernel arming
   Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor preset:
 enabled)
   Active: active (exited) since Fri 2019-05-24 23:29:13 UTC; 22s ago
  Process: 2503 ExecStart=/usr/bin/kdumpctl start (code=exited, status=0/SUCCESS)
```

```
Main PID: 2503 (code=exited, status=0/SUCCESS)
```

> **Note**
>
> Die Absturzabbilddatei wird standardmäßig in `/var/crash/` gespeichert. Um den Speicherort zu ändern, bearbeiten Sie die Datei `/etc/kdump.conf` mit Ihrem bevorzugten Texteditor.

So konfigurieren Sie SUSE Linux Enterprise, Ubuntu oder Red Hat Enterprise Linux

Bei Instances auf Intel- und AMD-Prozessoren sendet der Befehl `send-diagnostic-interrupt` einen unbekannten nicht maskierbaren Interrupt (NMI) an die Instance. Sie müssen den Kernel so konfigurieren, dass er bei Eingang des unbekannten NMI abstürzt, indem Sie die Konfigurationsdatei für Ihr Betriebssystem anpassen. Informationen darüber, wie Sie den Kernel so konfigurieren, dass er abstürzt, finden Sie in der Dokumentation für Ihr Betriebssystem:

- SUSE Linux Enterprise
- Ubuntu
- Red Hat Enterprise Linux (RHEL)

Windows-Instances

So konfigurieren Sie Windows zum Generieren eines Speicherabbilds bei Auftreten von Abbruchfehlern

1. Verbinden Sie sich mit der Instance.
2. Öffnen Sie die Systemsteuerung und wählen Sie System, Erweiterte Systemeinstellungen.
3. Wählen Sie im Dialogfeld Systemeigenschaften die Registerkarte Erweitert aus.
4. Wählen Sie im Bereich Startup und Wiederherstellen die Option Einstellungen....
5. Konfigurieren Sie die Einstellungen im Bereich Systemfehler ganz nach Bedarf und wählen Sie dann OK.

Weitere Informationen zum Konfigurieren von Windows-Abbruchfehlern finden Sie unter Overview of memory dump file options for Windows.

Senden eines Diagnose-Interrupts

Nachdem Sie die erforderlichen Konfigurationsänderungen vorgenommen haben, können Sie mithilfe der AWS CLI oder der EC2 Amazon-API einen Diagnose-Interrupt an Ihre Instance senden.

AWS CLI

So senden Sie einen Diagnose-Interrupt an Ihre Instance

Verwenden Sie den Befehl send-diagnostic-interrupt.

```
aws ec2 send-diagnostic-interrupt --instance-id i-1234567890abcdef0
```

PowerShell

So senden Sie einen Diagnose-Interrupt an Ihre Instance

Verwenden Sie das cmdlet Send-EC2DiagnosticInterrupt.

```
Send-EC2DiagnosticInterrupt -InstanceId i-1234567890abcdef0
```

Dokumentenverlauf für das EC2 Amazon-Benutzerhandbuch

In der folgenden Tabelle werden wichtige Ergänzungen des EC2 Amazon-Benutzerhandbuchs ab 2019 beschrieben. Außerdem aktualisieren wir den Leitfaden regelmäßig, um auf die Rückmeldungen einzugehen, die Sie uns schicken.

Änderung	Beschreibung	Datum
Reservierungen für unterbrechbare Kapazitäten	Reservierungen für unterbrechbare Kapazitäten helfen Ihnen dabei, ungenutzte Kapazität vorübergehend für andere Workloads innerhalb Ihres Kontos verfügbar zu machen.	21. November 2025
Instanztopologie für P6-B300-Instances	Sie können die Informationen zur Instance-Topologie für `p6-b300.48xlarge` -Instances abrufen.	18. November 2025
AMI-Abstammung	Sie können jetzt den Ursprung eines AMI verfolgen, indem Sie eine Liste aller seiner Vorfahren abrufen AMIs.	12. November 2025
Topologie der Kapazitätsreservierung	Sie können die DescribeCapacityReservationTopology API verwenden, um zu beschreiben, wo sich Ihre reservierten Kapazitäten im Verhältnis zueinander in der Netzwerkhierarchie befinden werden, bevor Sie Instances starten.	28. Oktober 2025

Optimieren Sie, CPUs um Lizenzeinsparungen zu erzielen	Sie können jetzt active konfigurieren CPUs , um Lizenzkosten für Windows- und SQL Server-Instanzen zu sparen, die in der Lizenz enthalten sind.	15. Oktober 2025
Neuer EC2 Kapazität smanager	Amazon EC2 hat EC2 Capacity Manager hinzugefü gt, mit dem Sie Ihre Kapazität snutzung für On-Demand-Instances, Spot-Instances und Kapazitätsreservierungen von einem einzigen Standort aus überwachen, analysieren und verwalten können.	15. Oktober 2025
AWSEC2CapacityMana gerServiceRolePolicy — neue verwaltete Richtlinie	Amazon EC2 hat die AWSEC2 CapacityManagerSer viceRolePolicy verwaltete Richtlinie hinzugefügt, damit Sie Kapazitätsressourcen verwalten und sich in Ihrem Namen mit AWS Organizat ions integrieren können.	15. Oktober 2025
`GPUPowerUtilization` - Metrik	Neue `GPUPowerU tilization` -Metrik für beschleunigte Computing-Instances.	13. Oktober 2025

EC2 IPv6 Unterstützung für Instance Connect Endpoints	EC2 Instance Connect Endpoint unterstützt jetzt IPv6 Konnektivität. Sie können EC2 Instance Connect-Endpunkte jetzt so konfigurieren, dass sie Dual-Stack unterstützen oder IPv6 nur Verbindungen zu Instances mit IPv6 Adressen herstellen.	2. Oktober 2025
AMIs Zulässig - neue Parameter	Allowed AMIs, eine Funktion, mit der Sie die Erkennung und Verwendung von AMIs innerhalb Ihres einschränken können AWS-Konto, unterstützt jetzt vier neue Parameter: AWS Marketplace Produktcodes, AMI-Namen, maximale Dauer seit AMI-Verfall und Höchstalter für. AMIs	25. September 2025
Detaillierte Leistungsstatistiken für Instance-Speicher-Volumes	Amazon EC2 bietet hochauflösende Leistungsstatistiken in Echtzeit für NVMe Instance-Speicher-Volumes, die an Nitro-basierte Instances angehängt sind.	16. September 2025
Aktualisierungen für Amazon EC2 Mac Dedicated Host	Amazon EC2 Mac Dedicated Hosts unterstützen die auto Wiederherstellung von Dedicated Hosts und die Host-Wartung auf Basis eines Neustarts.	28. August 2025

AMI-Kopien für Local Zones	Sie können jetzt Amazon EBS-gestützt AMIs in und aus Local Zones kopieren.	28. August 2025
Amazon EC2 ImageRefe rencesAccessPolicy — neue verwaltete Richtlinie	Amazon EC2 hat die von Amazon EC2 ImageRefe rencesAccessPolicy verwaltet e Richtlinie hinzugefügt, um die Erlaubnis zum Scannen aller von der EC2 DescribeI mageReferences API unterstüt zten Ressourcentypen zu gewähren.	26. August 2025
AMI-Nutzungsberichte	Wenn Sie Ihre Amazon Machine Images (AMIs) mit anderen teilen AWS-Konte n— sei es mit bestimmten Organisationen AWS-Konten, Organisationseinheiten (OUs) oder öffentlich — können Sie anhand von AMI-Nutzu ngsberichten sehen, wie diese verwendet AMIs werden. Die Berichte geben Aufschluss darüber, AWS-Konten welche Instances oder Startvorlagen Ihre AMIs EC2 In-Instances oder Startvorlagen verwenden und wie viele Instances oder Startvorlagen auf jedes AMI verweisen.	26. August 2025

AMI-Referenzen	Sie können Ihre AWS Ressourcen identifizieren, die auf bestimmte Amazon Machine Images (AMIs) verweisen, unabhängig davon, ob sie öffentlich oder privat AMIs sind oder wem sie gehören. Durch diese Transparenz können Sie sicherstellen, dass Ihre Ressourcen die neuesten konformen Daten verwenden AMIs.	26. August 2025
EC2 Instance Connect-Endpunkt ändern	Sie können jetzt einen vorhandenen EC2 Instance Connect-Endpunkt mithilfe des AWS CLI oder eines SDK ändern.	14. August 2025
Verbesserungen bei der Freigabe von Kapazitätsreservierung	Sie können jetzt Kapazitätsreservierungen freigeben, die Sie in Cluster-Placement-Gruppen erstellen.	12. August 2025

Aktualisierte verwaltete Richtlinie für EC2 Instance Connect Endpoint	Um die Änderung vorhanden er EC2 Instance Connect-E ndpunkte zu unterstützen, hat Amazon die `Ec2Instan ceConnectEndpoint` Richtlinie EC2 aktualisiert, um Berechtigungen zum Zuweisen und Aufheben der Zuweisung von IPv6 Adressen und zum Ändern von Sicherheitsgruppen auf Netzwerkschnittstellen, die von EC2 Instance Connect Endpoint erstellt wurden, hinzuzufügen. Amazon hat diese Richtlinie EC2 auch aktualisiert, um den `Null` Condition Operator durch den `StringLike` Condition Operator zu ersetzen.	31. Juli 2025
Instance-Topologie – zusätzlic he Unterstützung für Regionen	Die DescribeInstanceTopology API ist jetzt im asiatisch-pazifischen Raum (Melbourne) verfügbar.	31. Juli 2025
Erzwungene Beendigung	Sie können jetzt das Beenden einer Instance erzwingen.	31. Juli 2025
Instance-Topologie – zusätzlic he Unterstützung für Regionen	Die DescribeInstanceTopology API ist jetzt in AWS GovCloud (US-West) verfügbar.	24. Juli 2025

Das Herunterfahren des Betriebssystems beim Beenden der Instance überspringen	Sie können das ordnungsgemäße Herunterfahren des Betriebssystems beim Beenden einer Instance umgehen.	23. Juli 2025
Das Herunterfahren des Betriebssystems beim Anhalten der Instance überspringen	Sie können das ordnungsgemäße Herunterfahren des Betriebssystems beim Anhalten einer Instance umgehen.	23. Juli 2025
P6-B200-Kapazitätsblöcke in us-east-1	P6-B200-Kapazitätsblöcke sind jetzt in USA Ost (Nord-Virginia) verfügbar – `us-east-1` .	23. Juli 2025
Die verwaltete Richtlinie für die verknüpfte Rolle mit dem EC2 Fast Launch Service wurde aktualisiert	Um zu verhindern, dass Ressourcen verwaist sind, hat Amazon diese Richtlinie EC2 aktualisiert und nun die Erlaubnis hinzugefügt, Volumes, Volumenattribute und Netzwerkschnittstellen zu beschreiben und Volumes und Netzwerkschnittstellen zu löschen, die von EC2 Fast Launch erstellt wurden.	17. Juli 2025
EC2 Serielle Konsole — zusätzliche Unterstützung für Regionen	EC2 Serial Console ist jetzt auch in Asien-Pazifik (Thailand) und Mexiko (Zentral) verfügbar.	15. Juli 2025

EC2 Instance Connect — zusätzliche Unterstützung für Regionen	EC2 Instance Connect ist jetzt auch im asiatisch-pazifischen Raum (Thailand) und Mexiko (Zentral) verfügbar.	15. Juli 2025
Hardware-Paket-Zeitstempel	Sie können Hardware-Paket-Zeitstempel auf Ihrer EC2 Instance aktivieren, um jedem eingehenden Netzwerkpaket einen 64-Bit-Zeitstempel mit einer Genauigkeit von Nanosekunden hinzuzufügen.	23. Juni 2025
Snapshots während der AMI-Abmeldung löschen	Wenn Sie ein AMI abmelden, können Sie gleichzeitig automatisch die zugehörigen Snapshots löschen.	28. Mai 2025
Vom Benutzer initiierte Neustart-Migration	Wenn Ihre Instance eine Benachrichtigung über ein EC2 geplantes Neustart-Ereignis erhält, ist diese standardmäßig für die Instance-Migration aktiviert, wenn Sie die Instance vor dem Ereignis neu starten.	20. Mai 2025
SIP-Konfiguration für Amazon EC2 Mac-Instances	Sie können Systemintegritätsschutz-Einstellungen (SIP) für x86-Mac-Instances und Apple-Halbleiter-Mac-Instances konfigurieren.	20. Mai 2025

Delegierung des Root-Volume-Besitzes	Sie können jetzt die Delegierung des Besitzes von Root-Volumes für das Amazon-EBS-Root-Volume automatisieren, wenn Sie das Betriebssystem auf Apple-Halbleiter-Mac-Instances aktualisieren.	20. Mai 2025
Instance-Topologie für P6-B200-Instances	Sie können die Informationen zur Instance-Topologie für `p6-b200.48xlarge` -Instances abrufen.	15. Mai 2025
Die verwalteten Richtlinien für die verknüpfte Rolle mit dem EC2 Fast Launch Service wurden aktualisiert	Die Richtlinie für verknüpfte Rollen mit dem EC2 Fast Launch-Service wurde aktualisiert und bietet nun Zugriff auf die Erstellung und Verwaltung von EventBridge Amazon-Veranstaltungsregeln sowie andere Aktionen zur Verbesserung des EC2 Fast Launch-Erlebnisses . Weitere Informationen zu den Berechtigungen, die von der serviceverknüpften Rolle gewährt werden, finden Sie unter Berechtigungen gewährt von `EC2FastLaunchServiceRolePolicy` .	14. Mai 2025

Die verwalteten Richtlinien für die EC2 Fast Launch-Richtlinie für vollen Zugriff wurden aktualisiert	Die EC2 Schnellstart-Vollzugriffsrichtlinie wurde aktualisiert und bietet nun die Möglichkeit, Vorgänge zum Erstellen und Ändern von Startvorlagen, zum Erstellen von Netzwerk- und Sicherheitsgruppenressourcen, zum Autorisieren von Zugriffsregeln und zum Löschen von Ressourcen, die von EC2 Fast Launch erstellt wurden. Mit der Richtlinie können außerdem Stacks beschrieben und erstellt sowie CloudFormation Stacks gelöscht werden, die EC2 von Fast Launch erstellt wurden.	14. Mai 2025
Vereinfachtes Onboarding für Fast Launch EC2	EC2 Fast Launch wurde aktualisiert, um den Onboarding-Prozess zu vereinfachen.	14. Mai 2025
AWS Config Integration mit Allowed AMIs	Verwenden Sie die ec2-instance-launched-with-allowed AWS Config -ami-Regel, um zu überprüfen, ob laufende oder gestoppte Instances gestartet wurden AMIs , die Ihren Zulassungskriterien entsprechen. AMIs	11. März 2025

Von AWSEC2CapacityReservationFleetRolePolicy verwaltete Richtlinie aktualisiert	Amazon `AWSEC2CapacityReservationFleetRolePolicy` hat die verwaltete Richtlinie EC2 aktualisiert, sodass der `ArnLike` Bedingungsoperator anstelle des `StringLike` Bedingungsoperators verwendet wird.	03. März 2025
Zeitbasierte AMI-Kopien	Sie können jetzt eine Abschlussdauer für EBS-gestützte AMI-Kopiervorgänge anfordern, um sicherzustellen, dass AMI-Kopien innerhalb eines bestimmten Zeitrahmens abgeschlossen werden.	25. Februar 2025
AmazonEC2ReadOnlyAccess-Richtlinie aktualisiert	Amazon EC2 hat den `GetSecurityGroupsForVpc` Vorgang zur bestehenden EC2 ReadOnlyAccess Amazon-Richtlinie hinzugefügt.	27. Dezember 2024
Verwaltete Instances	Sie können jetzt von Amazon EC2 verwaltete Instances in der EC2 Konsole anzeigen.	01. Dezember 2024

Deklarative Richtlinien	Sie können jetzt deklarative Richtlinien verwenden, um Einstellungen auf Kontoebene für mehrere Regionen und Konten gleichzeitig anzuwenden. Deklarative Richtlinien werden für die Konfiguration der Einstellungen für EC2 seriellen Konsolenzugriff AMIs, Zulässig, IMDS-Standardeinstellungen und Blockierung des öffentlichen Zugriffs für VPCs AMIs, und Snapshots unterstützt. Weitere Informationen finden Sie unter Deklarative Richtlinien im AWS Organizations -Benutzerhandbuch sowie in der spezifischen Dokumentation zu den einzelnen unterstützten Features.	01. Dezember 2024
Erlaubt AMIs	Sie können jetzt die Erkennung und Verwendung von AMIs in Amazon steuern, EC2 indem Sie Kriterien angeben, die erfüllt AMIs werden müssen.	01. Dezember 2024
Sofortige Kapazitätsblöcke	Sie können jetzt Kapazitätsblöcke für ML reservieren, die bereits nach 30 Minuten beginnen können.	21. November 2024

Zuküftige Kapazitätsreservierungen	Sie können jetzt Kapazitätsreservierungen für einen zukünftigen Termin beantragen.	21. November 2024
Kapazitätsblock erweitern	Sie können jetzt die Dauer vorhandener Kapazitätsblöcke verlängern.	21. November 2024
Kapazitätsblöcke für 6 Monate	Sie können Kapazitätsblöcke jetzt für bis zu 6 Monate (182 Tage) für ML reservieren.	21. November 2024
Gespeicherte Filtersätze	Sie können jetzt benutzerdefinierte Filtergruppen erstellen und diese wiederverwenden, um Ihre EC2 Ressourcen effizient anzuzeigen.	20. November 2024
Leistungsschutz	Wenn Sie die attributbasierte Instance-Typauswahl für Ihre EC2 Flotte oder Spot-Flotte verwenden, können Sie jetzt den Performance-Schutz aktivieren, um sicherzustellen, dass die ausgewählten Instance-Typen einer bestimmten Performance-Baseline ähnlich sind oder diese übertreffen.	20. November 2024
Nur Kapazitätsreservierungen	Sie können auch festlegen, dass Instances nur in einer Kapazitätsreservierung oder Kapazitätsreservierungs-Ressourcengruppe laufen.	20. November 2024

Quell-AMI identifizieren	Sie können nun das Quell-AMI identifizieren, das zum Erstellen eines AMI verwendet wurde.	13. November 2024
Kapazität aufteilen	Erfahren Sie, wie Sie Kapazität aus einer bestehenden Kapazitätsreservierung abspalten um eine neue Kapazitätsreservierung zu erstellen.	30. Oktober 2024
Kapazität verschieben	Sie können jetzt Kapazität von einer Kapazitätsreservierung in eine andere verschieben.	30. Oktober 2024
Tutorials für Anfänger	Zwei neue Tutorials für Anfänger: Starten Sie meine allererste EC2 Instance und starten Sie eine EC2 Test-Instance und stellen Sie eine Verbindung zu ihr her.	21. Oktober 2024
Unterstützung für Windows Server 2025	Fügen Sie Unterstützung für Windows Server 2025 hinzu.	16. Oktober 2024
EC2 Globale Ansicht	EC2 Mit Global View können Sie jetzt Kapazitätsreservierungen und Kapazitätsblöcke in Ihrem Konto in allen Regionen einsehen.	16. Oktober 2024

Wartung des Hosts für die Live-Migration	Amazon EC2 Dedicated Hosts unterstützen jetzt die Wartung von Live-Migrations-Hosts, bei der unterstützte Instances automatisch von einem beeinträchtigten Dedicated Host auf einen Ersatz-Dedicated Host migriert werden, ohne sie zu stoppen und neu zu starten.	15. Oktober 2024
Abrechnungszuordnung für freigegebene Kapazitätsreservierungen	Sie können jetzt die Abrechnung aller verfügbaren Kapazitäten einer gemeinsamen Kapazitätsreservierung einem Kundenkonto zuweisen, das derselben AWS Organisation angehört.	14. Oktober 2024
PTP-Hardware-Uhr – zusätzliche Unterstützung für Regionen	Die PTP-Hardware-Uhr ist jetzt auch in USA Ost (Ohio) und Asien-Pazifik (Malaysia) verfügbar.	23. September 2024
EC2 Instance Connect unterstützt IPv6	Sie können jetzt EC2 Instance Connect verwenden, um eine Verbindung zur öffentlichen IPv6 Adresse Ihrer Instance herzustellen.	23. September 2024
EC2 Instance Connect-Präfixlisten	Sie können jetzt eine verwaltete Präfixliste für IPv4 oder IPv6 Adressen auswählen, wenn Sie Regeln in Ihren Sicherheitsgruppen erstellen, um SSH-Verkehr vom EC2 Instance Connect-Dienst zuzulassen.	23. September 2024

Neue Funktionen für On-Demand-Kapazitätsreservierungen	Sie können jetzt Ihre Kapazitätsreservierung aufteilen, Kapazität zwischen Kapazitätsreservierungen verschieben und das Instance-Berechtigungsattribut Ihrer Kapazitätsreservierung ändern.	14. August 2024
Ruhezustand unterstützt für C6g, C6gn, C6gd, C7g, C7gd, M6g, M6gd, M7g, M7gd, R6g, and R6gd	Ihre neu gestarteten Instances auf den Instance-Typen C6g, C6gn, C6gd, C7g, C7gd, M6g, M6gd, M7g, M7gd, R6g, and R6gd in den Ruhezustand versetzen.	30. Juli 2024
Hibernation-Unterstützung, die AMIs Graviton-Instanztypen unterstützt	Versetzen Sie Ihre neu gestarteten Instances, die über ein Amazon Linux- oder Ubuntu-AMI gestartet wurden, das Graviton-Instance-Typen unterstützt, in den Ruhezustand.	30. Juli 2024
Zusätzliche Instance-Typen werden für Credential Guard unterstützt	Sie können Credential Guard jetzt für C7i-, C7-flex, M7i-, M7i-flex-, R7i-, R7i-flex- und T3-Instances aktivieren.	26. Juni 2024
EC2 Instanztyp-Finder — zusätzliche Parameter	Der EC2 Instance-Typ-Finder bietet jetzt zusätzliche Parameter, mit denen Sie detailliertere Anforderungen für Ihren Workload angeben können.	5. Juni 2024

Neue verwaltete Richtlinie für EC2 Fast Launch	Die EC2FastLaunchFullAccess Richtlinie zur Ausführung von API-Aktionen im Zusammenhang mit der EC2 Schnellstartfunktion von einer Instanz aus wurde hinzugefügt.	14. Mai 2024
AMI-Abmeldeschutz	Sie können den Abmeldeschutz für ein AMI aktivieren, um ein versehentliches oder böswilliges Löschen zu verhindern.	23. April 2024
PTP-Hardware-Uhr – Unterstützung für Instance-Typen	Die PTP-Hardware-Uhr ist jetzt für die folgenden Instance-Typen verfügbar: M7a, M7g, M7i, R7a und R7i	22. April 2024
Überlegungen zur Nitro-Leistung für verbesserte Netzwerke wurden hinzugefügt	Diese Seite konzentriert sich auf Überlegungen zum Netzwerk, um Ihnen bei der Leistungsoptimierung Ihrer Nitro-basierten EC2 Amazon-Instances zu helfen.	4. April 2024
Neue verwaltete Richtlinie für VSS-basierte EBS-Snapshots	In Amazon EC2 VSS steht eine neue IAM-verwaltete Richtlinie zur Verfügung, die Sie zu Ihrer Instance-Profilrolle hinzufügen können, um sicherzustellen, dass Ihre Berechtigungen erhalten bleiben up-to-date und die bewährten Methoden eingehalten werden.	28. März 2024

PTP-Hardware-Uhr – USA Ost (Nord-Virginia)	Die PTP-Hardware-Uhr ist jetzt in der Region USA Ost (Nord-Virginia) verfügbar.	26. März 2024
IMDSv2 Als Standard für das Konto festlegen	Sie können für alle neuen EC2 Instanzstarts in Ihrem Konto festlegen, dass der Instanz-Metadatendienst Version 2 (IMDSv2) standardmäßig verwendet wird.	25. März 2024
Kennzeichnen Sie ein neues Linux, das aus einem Snapshot AMIs erstellt wurde	Wenn Sie ein Linux-AMI aus einem Snapshot erstellen, können Sie das neue AMI mit Tags vesehen.	7. März 2024
Kennzeichnen Sie beim AMIs Kopieren neue Dateien und Schnappschüsse	Wenn Sie ein AMI erstellen , können Sie das AMI und die Snapshots mit denselben Tags markieren oder sie mit verschiedenen Tags markieren .	7. März 2024
Entfernen Sie die AWS Management Pack-Seiten	Das AWS Management Pack wurde hauptsächlich mit Windows Server 2012 und früheren Versionen verwendet . Diese älteren Betriebss ystemplattformversionen werden nicht mehr unterstützt. Informationen zur Verwaltun g und Problembehebung Ihrer Serverflotte, die vor Ort AWS und lokal ausgeführt werden, finden Sie unter AWS Systems Manager Fleet Manager.	12. Februar 2024

EC2 Instance Connect ist auf macOS vorinstalliert AMIs	EC2 Instance Connect ist jetzt auf macOS Sonoma 14.2.1 oder höher, macOS Ventura 13.6.3 oder höher und macOS Monterey 12.7.2 oder höher vorinstalliert. AMIs	26. Januar 2024
EC2 Instance Connect-Unterstützung für CentOS, macOS und RHEL	Sie können EC2 Instance Connect jetzt auf unterstützten CentOS, macOS und AMIs RHEL installieren.	6. Dezember 2023
Unterstützt Ruhezustand für C7a, C7i, R7a, R7i und R7iz	Versetzen Sie Ihre neu gestarteten Instances, die auf C7a, C7i, R7a, R7i und R7iz-Instance-Typen ausgeführt werden, in den Ruhezustand.	1. Dezember 2023
Auswahl des Amazon EC2 Q-Instanztyps	Die Auswahl des Amazon EC2 Q-Instance-Typs berücksichtigt Ihren Anwendungsfall, Ihren Workload-Typ und die Präferenz des CPU-Herstellers sowie die Art und Weise, wie Sie Preis und Leistung priorisieren. Anschließend werden diese Daten verwendet, um Anleitungen und Vorschläge für EC2 Amazon-Instance-Typen bereitzustellen, die für Ihre neuen Workloads am besten geeignet sind.	28. November 2023
EC2 Kostenloses Kontingent	Sie können Ihre Nutzung des EC2 kostenlosen Kontingents im EC2 Dashboard verfolgen.	26. November 2023

Console-to-Code	Console-to-Code kann Ihnen bei den ersten Schritten mit Ihrem Automatisierungsco de helfen. Console-to-Codezeichnet Ihre Konsolena ktionen auf und verwendet dann generative KI, um Code in Ihrem bevorzugten Infrastruktur-as-Code-Forma t vorzuschlagen. Sie können den Code als Ausgangsp unkt verwenden und ihn so anpassen, dass er für Ihren speziellen Anwendungsfall produktionsbereit ist.	26. November 2023
Konfigurierbare Timeouts für die Nachverfolgung von Leerlaufverbindungen	Im Leerlauf befindliche Sicherheitsgruppenverbindun gen können zur Erschöpfung der Kapazität der Verbindun gsnachverfolgung führen und zur Folge haben, dass Verbindungen nicht nachverfo lgt und Pakete verworfen werden. Jetzt können Sie das Timeout für die Nachverfo lgung von Sicherheitsgruppen verbindungen auf einer Elastic-Network-Schnittstelle in Sekunden festlegen.	17. November 2023

PTP-Hardware-Uhr	Unterstützte Instances verfügen jetzt über eine Precision Time Protocol (PTP)-Hardware-Uhr. Die PTP-Hardware-Uhr unterstützt entweder NTP oder eine direkte PTP-Verbindung.	16. November 2023
Ändern Sie den Instance-Typ der Instance, die für den Ruhezustand aktiviert ist	Sie können jetzt den Instance-Typ einer Instance mit Ruhezustands-Unterstützung ändern, wenn sie sich im Zustand `stopped` befindet.	16. November 2023
Instance-Topologie	Sie können die DescribeInstanceTopology API verwenden, um den Standort Ihrer Instances zu ermitteln, und diese Informationen dann verwenden, um HPC- und ML-Jobs zu optimieren, indem Sie sie auf Instances ausführen, die physisch näher beieinander liegen.	13. November 2023
EC2 Gemeinsame AMI-Unterstützung für Fast Launch	Sie können jetzt EC2 Fast Launch auf einem AMI aktivieren, das mit Ihnen geteilt wurde. Wenn Sie EC2 Fast Launch auf einem gemeinsam genutzten AMI aktivieren, werden die vorab bereitgestellten Snapshots für einen schnelleren Start in Ihrem Konto erstellt.	6. November 2023

Kapazitätsblöcke für ML	Sie können GPU-Instances jetzt für einen späteren Zeitpunkt reservieren, um Ihre kurzfristigen Machine-L earning-Workloads (ML) zu unterstützen.	31. Oktober 2023
Spot-Instance-Ruhezustand	Sie können Ihre Spot Instances jetzt in den Ruhezustand versetzen und dabei das gleiche Ruhezusta ndserlebnis und die gleichen Instance-Familien nutzen, die derzeit für On-Demand-Instances verfügbar sind.	24. Oktober 2023
Standardeinstellungen für die Sperrung des öffentlichen Zugriffs für AMIs	Den öffentlichen Zugriff blockieren für AMIs ist jetzt standardmäßig für alle neuen Konten und für bestehend e Konten ohne öffentliche Konten aktiviert AMIs.	20. Oktober 2023
Amazon EC2 Global View	Amazon EC2 Global View unterstützt zusätzliche Ressourcentypen und anpassbare Anzeigeoptionen.	18. Oktober 2023
Unterstützung des Ruhezusta nds für Ubuntu 22.04.2 LTS (Jammy Jellyfish)	Versetzen Sie Ihre neu gestarteten Instances, die vom AMI mit Ubuntu 22.04.2 LTS (Jammy Jellyfish) gestartet wurden, in den Ruhezustand.	16. Oktober 2023

Deaktivieren eines AMIs	Sie können ein AMI deaktivieren, um zu verhindern, dass es für Instance-Starts verwendet wird.	12. Oktober 2023
Verknüpfte EBS-Statusprüfungen	Sie können die verknüpften EBS-Statusprüfungen verwenden, um zu überwachen, ob die mit einer Instance verknüpften Amazon EBS-Volumes erreichbar sind.	11. Oktober 2023
Hibernation-Unterstützung für Red Hat Enterprise Linux 9	Versetzen Sie Ihre neu gestarteten Instances, die von Red Hat Enterprise Linux 9 AMI gestartet wurden, in den Ruhezustand.	02. Oktober 2023
Hibernation-Unterstützung für Microsoft Windows Server 2022	Versetzen Sie Ihre neu gestarteten Instances, die von Microsoft Windows Server 2022 AMI gestartet wurden, in den Ruhezustand.	2. Oktober 2023
Hibernation-Unterstützung für 023 AL2	Versetzen Sie Ihre neu gestarteten Instances, die über das 023 AMI gestartet wurden, in den Ruhezustand. AL2	02. Oktober 2023

Initiieren der Unterbrechung von Spot-Instances in einer Spot-Flotte	Sie können in der EC2 Amazon-Konsole eine Spot-Flotte auswählen und eine Unterbrechung der Spot-Instances in der Flotte einleiten, sodass Sie testen können, wie die Anwendungen auf Ihren Spot-Instances mit Unterbrechungen umgehen.	21. September 2023
Sperren Sie den öffentlichen Zugriff auf AMIs	Sie können die Option „Öffentlichen Zugriff sperren“ AMIs auf Kontoebene aktivieren, um alle Versuche zu blockieren, Ihre Daten AMIs öffentlich zugänglich zu machen.	12. September 2023
Unterstützung des Ruhezustands für M7i und M7i-flex	Versetzen Sie neu gestartete Instances, die auf Instances vom Typ M7i und M7i-flex ausgeführt werden, in den Ruhezustand.	22. August 2023
EC2-Classic ist veraltet	Bei EC2 -Classic wurden EC2 Instanzen in einem einzigen, flachen Netzwerk ausgeführt, das mit anderen Kunden geteilt wurde. Amazon VPC ersetzt EC2 -Classic. Mit Amazon VPC werden Ihre Instances in einer Virtual Private Cloud (VPC) ausgeführt, die logisch von Ihrem AWS -Konto isoliert ist.	08. August 2023

Dedicated Hosts	Sie können Dedicated Hosts bestimmten Hardware-Assets auf einem Outpost zuweisen.	20. Juni 2023
EC2 Instance Connect-Endpunkt	Sie können jetzt über SSH oder RDP eine Verbindung zu einer Instanz herstellen, ohne dass die Instanz eine öffentliche IPv4 Adresse haben muss.	13. Juni 2023
IMDS-Paket-Analysator	Sie können jetzt den IMDS Packet Analyzer verwenden, um die Quellen von IMDSv1 Aufrufen auf Ihren Instances zu identifizieren. EC2	01. Juni 2023
EC2 Bare-Metal-Instanzen der seriellen Konsole	Die EC2 serielle Konsole unterstützt jetzt Konnektivität zur seriellen Schnittstelle ausgewählter Bare-Metal-Instances.	11. April 2023
Quotas für Startvorlagen	Sie können jetzt Ihre Kontingente für Startvorlagen und Startvorlagenversionen in der Service-Quotas-Konsole und mithilfe der Service-Quotas-CLI anzeigen.	03. April 2023
Benachrichtigungen zur Auslastung der Kapazitätsreservierung	AWS Health sendet jetzt Benachrichtigungen, wenn die Kapazitätsauslastung für Kapazitätsreservierungen in Ihrem Konto unter 20 Prozent fällt.	03. April 2023

Kapazitätsreservierungs-Gruppen	Sie können jetzt Kapazität sreservierungen, die für Sie freigegeben sind, zu Kapazität sreservierungsgruppen hinzufügen, die Sie besitzen.	30. März 2023
Modifizieren von Instance-Metadatenoptionen	Sie können jetzt die EC2 Amazon-Konsole verwenden, um die Optionen für Instance-Metadaten zu ändern.	20. März 2023
Direkte Updates für das macOS-Betriebssystem	Sie können jetzt Apple macOS-Betriebssystem-Updates auf M1-Mac-Instances direkt durchführen.	14. März 2023
UEFI Preferred	Sie können jetzt ein einziges AMI erstellen, das sowohl den Unified Extensible Firmware Interface (UEFI) als auch den Legacy BIOS-Startmodus unterstützt.	03. März 2023
Modifizieren Sie ein AMI für IMDSv2	Ändern Sie Ihr vorhandenes AMI so, dass Instances, die über das AMI gestartet werden, IMDSv2 standardmäßig Folgendes benötigen.	28. Februar 2023
Auf Windows-Virtualisierung basierende Sicherheit – Credential Guard	Sie können Credential Guard, eine virtualisierungsbasierte Sicherheitsfunktion (VBS), auf unterstützten Amazon-Instances aktivieren. EC2	31. Januar 2023

Neue verwaltete Richtlinie für EC2 Instance Connect Endpoint	Die `Ec2InstanceConnectEndpoint` Richtlinie, die der AWSServiceRoleForEC2InstanceConnectserviceverknüpften Rolle beigefügt ist, wurde hinzugefügt, damit Amazon EC2 Aktionen in Ihrem Namen durchführen kann, wenn Sie einen EC2 Instance Connect-Endpunkt erstellen.	24. Januar 2023
AMI-Alias in Startvorlagen	Sie können in Ihren Startvorlagen einen AWS Systems Manager Parameter anstelle der AMI-ID angeben, um zu vermeiden, dass Sie die Vorlagen jedes Mal aktualisieren müssen, wenn sich die AMI-ID ändert.	19. Januar 2023
Ruhezustand-Unterstützung für C6i, I3en und M6i	Versetzen Sie Ihre neu gestarteten Instances, die auf C6i-, I3en- und M6i-Instance-Typen ausgeführt werden, in den Ruhezustand.	19. Dezember 2022
Torn-Write-Prävention	Verbessern Sie die Leistung Ihrer I/O-intensiven relationalen Datenbank-Workloads und reduzieren Sie die Latenz, ohne die Datenstabilität zu beeinträchtigen, indem Sie das Blockspeicherfeature Torn-Write-Prävention verwenden.	29. November 2022

ENA Express	Erhöhen Sie mit ENA Express den Durchsatz und minimieren Sie die Latenz am Ende des Netzwerkverkehrs zwischen EC2 Instances.	28. November 2022
Kopieren von AMI-Tags	Wenn Sie ein AMI kopieren, können Sie gleichzeitig Ihre benutzerdefinierten AMI-Tags kopieren.	18. November 2022
AMI-Größe für Speichern und Wiederherstellen	Die Größe eines AMI (vor der Komprimierung), das in und von einem Amazon-S3-Bucket gespeichert und wiederher gestellt werden kann, kann jetzt bis zu 5 000 GB betragen.	16. November 2022
priceCapacityOptimized-Zuweisungsstrategie für Spot Instances	Eine Spot-Flotte, die die `priceCapacityOptimized` -Zuweisungsstrategie verwendet, berücksichtigt sowohl den Preis als auch die Kapazität, um die Pools mit Spot Instances auszuwählen, bei denen die Wahrscheinlichkeit einer Unterbrechung am geringsten ist und die den niedrigstmöglichen Preis haben.	10. November 2022

price-capacity-optimized-Zuweisungsstrategie für Spot Instances	Eine EC2 Flotte, die die `price-capacity-optimized` Zuweisungsstrategie verwendet, berücksichtigt sowohl den Preis als auch die Kapazität, um die Spot-Instance-Pools auszuwählen, bei denen die Wahrscheinlichkeit einer Unterbrechung am geringsten ist und die den niedrigstmöglichen Preis haben.	10. November 2022
Aufheben der Freigabe eines AMI für Ihr Konto	Wenn ein AMI mit Ihrem geteilt wurde AWS-Konto und Sie nicht mehr möchten, dass es mit Ihrem Konto geteilt wird, können Sie Ihr Konto aus den Startberechtigungen des AMI entfernen.	04. November 2022
Übertragen von Elastic-IP-Adressen	Sie können jetzt Elastic IP-Adressen von einer AWS-Konto zur anderen übertragen.	31. Oktober 2022
Ersetzen von Stamm-Volume	Sie können das Stamm-Amazon-EBS-Volume für eine ausgeführte Instance durch ein AMI ersetzen.	27. Oktober 2022
Automatisches Verbinden einer Instance mit der Datenbank	Verwenden Sie die automatische Verbindungsfunktion, um schnell eine oder mehrere EC2 Instances mit einer RDS-Datenbank zu verbinden, um den Datenverkehr zwischen ihnen zu ermöglichen.	10. Oktober 2022

AMI-Kontingente	Für das Erstellen und Teilen gelten jetzt Kontingente AMIs.	10. Oktober 2022
AMI konfigurieren für IMDSv2	Konfigurieren Sie Ihr AMI so, dass Instances, die über das AMI gestartet werden, IMDSv2 standardmäßig Folgendes benötigen.	3. Oktober 2022
Initiieren einer Spot-Instance-Unterbrechung	Sie können in der EC2 Amazon-Konsole eine Spot-Instance auswählen und eine Unterbrechung einleiten, sodass Sie testen können, wie die Anwendungen auf Ihren Spot-Instances mit Unterbrechungen umgehen.	26. September 2022
Verifizierter AMI-Anbieter	In der EC2 Amazon-Konsole werden öffentliche AMIs Inhalte, die Amazon oder einem verifizierten Amazon-Partner gehören, als Verifizierter Anbieter gekennzeichnet.	22. Juli 2022
Platzierungsgruppen auf AWS Outposts	Host-Spread-Strategie für Platzierungsgruppen auf einem Outpost hinzugefügt.	30. Juni 2022
Dedizierte Hosts auf AWS Outposts	Sie können Dedicated Hosts auf AWS Outposts zuweisen.	31. Mai 2022
Beendungsschutz der Instances	Wenn Sie verhindern möchten, dass Ihre Instance versehentlich gestoppt wird, können Sie den Stopp-Schutz für die Instance aktivieren.	24. Mai 2022

UEFI Secure Boot	UEFI Secure Boot baut auf dem langjährigen Secure Boot-Prozess von Amazon auf EC2 und bietet zusätzliche Funktionen, mit defense-in-depth denen Kunden Software vor Bedrohungen schützen können, die auch nach Neustarts bestehen bleiben.	10. Mai 2022
NitroTPM	Das Nitro Trusted Platform Module (NitroTPM) ist ein virtuelles Gerät, das vom AWS Nitro-System bereitgestellt wird und der TPM 2.0-Spezifikation entspricht.	10. Mai 2022
AMI-Status-Änderungsereignisse	Amazon generiert EC2 jetzt ein Ereignis, wenn ein AMI den Status ändert. Sie können Amazon verwenden EventBridge , um diese Ereignisse zu erkennen und darauf zu reagieren.	9. Mai 2022
Beschreiben öffentlicher Schlüssel	Sie können den öffentlichen Schlüssel und das Erstellungsdatum eines EC2 Amazon-Schlüsselpaars abfragen.	28. April 2022
Erstellen von Schlüsselpaaren	Sie können das Schlüsselformat (PEM oder PPK) angeben, wenn Sie ein neues Schlüsselpaar erstellen.	28. April 2022

FSx Amazon-Dateisysteme beim Start einhängen	Mit dem neuen Instance-Startassistenten können Sie beim Start ein neues oder vorhandenes Amazon FSx FSx for NetApp ONTAP- oder Amazon for OpenZFS-Dateisystem mounten.	12. April 2022
Neuer Launch Instance Wizard	Ein neues und verbesser tes Starterlebnis in der EC2 Amazon-Konsole, das eine schnellere und einfachere Möglichkeit bietet, eine EC2 Instance zu starten.	5. April 2022
Öffentlich automatisch als veraltet kennzeichnen AMIs	Standardmäßig AMIs ist das Verfallsdatum aller öffentlic hen Dateien auf zwei Jahre ab dem Datum der AMI-Erstellung festgelegt.	31. März 2022
Kategorie der Instanz-M etadaten: Autoscaling/ target-li fecycle-state	Wenn Sie Amazon EC2 Auto Scaling Scaling-Gruppen verwenden, können Sie über die Instance-Metadaten auf den Ziellebenszyklusstatus einer Instance zugreifen.	24. März 2022
Zeitpunkt des letzten AMI-Start s	`lastLaunchedTime` gibt an, wann Ihr AMI zuletzt zum Starten einer Instance verwendet wurde.	28. Februar 2022
ED25519 keys	ED25519 Schlüssel werden jetzt für EC2 Instance Connect und EC2 Serial Console unterstützt.	20. Januar 2022

Weitere RHEL-Plattformen für Kapazitätsreservierungen	Weitere Red Hat Enterprise Linux-Plattformen für Kapazitätsreservierungen on demand.	11. Januar 2022
Konfigurieren Sie Windows AMIs für einen schnelleren Start	Konfigurieren Sie Windows so AMIs , dass Instanzen mithilfe vorab bereitgestellter Snapshots bis zu 65% schneller gestartet werden.	10. Januar 2022
Instance-Tags in Instance-Metadaten	Sie können über die Instance-Metadaten auf die Tags einer Instance zugreifen.	6. Januar 2022
Kapazitätsreservierungen in Cluster-Placement-Gruppen	Sie können Kapazitätsreservierungen in Cluster-Placement-Gruppen erstellen.	6. Januar 2022
Spot-Flotte launch-before-terminate	Die Spot-Flotte kann die Spot-Instances beenden, die eine Neuausgleichsbenachrichtigung erhalten, nachdem neue Ersatz-Spot-Instances gestartet wurden.	4. November 2021
EC2 Flotte launch-before-terminate	EC2 Fleet kann die Spot-Instances, die nach dem Start neuer Ersatz-Spot-Instances eine Benachrichtigung über die Neuverteilung erhalten, beenden.	4. November 2021
Vergleichen von Zeitstempeln	Sie können den tatsächlichen Zeitpunkt eines Ereignisses ermitteln, indem Sie den Zeitstempel Ihrer Amazon EC2 Linux-Instance mit ClockBound vergleichen.	2. November 2021

AMIs Mit Organisationen teilen und OUs	Sie können es jetzt AMIs mit den folgenden AWS Ressourcen teilen: Organisationen und Organisationseinheiten (OUs).	29. Oktober 2021
Spot-Platzierungsbewertung	Holen Sie sich eine Empfehlung für eine AWS Region oder Availability Zone auf der Grundlage Ihrer Spot-Kapazitätsanforderungen.	27. Oktober 2021
Attributbasierte Instance-Typauswahl für Spot-Flotte	Geben Sie die Attribute an, die eine Instance haben muss, und Amazon EC2 identifiziert alle Instance-Typen mit diesen Attributen.	27. Oktober 2021
Attributbasierte Auswahl des Instance-Typs für Fleet EC2	Geben Sie die Attribute an, die eine Instance haben muss, und Amazon EC2 identifiziert alle Instance-Typen mit diesen Attributen.	27. Oktober 2021
On-Demand-Kapazitätsreservierungsflotte	Sie können eine Kapazitätsreservierungsflotte verwenden, um eine Gruppe oder Flotte von Kapazitätsreservierungen zu starten.	5. Oktober 2021
Unterstützung des Ruhezustands für Ubuntu 20.04 LTS (Focal)	Versetzen Sie Ihre neu gestarteten Instances, die vom AMI mit Ubuntu 20.04 LTS (Focal) gestartet wurden, in den Ruhezustand.	4. Oktober 2021

EC2 Flotten- und gezielte Kapazitätsreservierungen auf Abruf	EC2 Fleet kann On-Demand -Instances für `targeted` Kapazitätsreservierungen starten.	22. September 2021
T3-Instances auf Dedicated Hosts	Support für T3-Instances auf Amazon EC2 Dedicated Host.	14. September 2021
Ruhezustand-Support für RHEL, Fedora und CentOS	Versetzen Sie Ihre neu gestarteten Instances, die über RHEL, Fedora und CentOS gestartet wurden, in den Ruhezustand. AMIs	9. September 2021
Amazon EC2 Global View	Mit Amazon EC2 Global View können Sie Subnetze VPCs, Instances, Sicherhei tsgruppen und Volumes in mehreren AWS Regionen in einer einzigen Konsole anzeigen.	1. September 2021
Ruhezustand-Unterstützung für C5d, M5d und R5d	Versetzen Sie Ihre neu gestarteten Instances, die auf C5d-, M5d- und R5d-Instance-Typen ausgeführt werden, in den Ruhezustand.	19. August 2021
EC2 Amazon-Schlüsselpaare	Amazon unterstützt EC2 jetzt ED25519 Schlüssel auf Linux- und Mac-Instances.	17. August 2021
Präfixe für Netzwerkschnittste llen	Sie können Ihren Netzwerks chnittstellen entweder automatisch IPv4 oder manuell einen privaten Bereich oder einen IPv6 CIDR-Bereich zuweisen.	22. Juli 2021

Ereignisfenster	Sie können benutzerdefinierte, wöchentlich wiederkehrende Ereignisfenster für geplante Ereignisse definieren, mit denen Ihre EC2 Amazon-Instances neu gestartet, gestoppt oder beendet werden.	15. Juli 2021
Ressourcen IDs - und Tagging-Unterstützung für Sicherheitsgruppenregeln	Sie können auf Sicherheitsgruppenregeln nach Ressourcen-ID verweisen. Sie können Ihren Sicherheitsgruppenregeln auch Tags hinzufügen.	7. Juli 2021
AMI als veraltet kennzeichnen	Sie können jetzt angeben, wann ein AMI veraltet ist.	11. Juni 2021
Sekundengenaue Abrechnung für Windows	Amazon EC2 berechnet die Nutzung auf Windows- und SQL-Server-Basis sekundengenau mit einer Mindestgebühr von einer Minute.	10. Juni 2021
Kapazitätsreservierungen am AWS Outposts	Sie können jetzt Kapazitätsreservierungen auf AWS Outposts nutzen.	24. Mai 2021
Freigabe einer Kapazitätsreservierung	Sie können jetzt in Local Zones und Wavelength Zones erstellte Kapazitätsreservierungen freigeben.	24. Mai 2021

Root-Volume-Ersatz	Sie können jetzt die Aufgaben Stammvolumenersatz verwenden, um das EBS-Stammvolumen für laufende Instances zu ersetzen.	22. April 2021
Speichern und Wiederherstellen eines AMI mit S3	Speichern Sie EBS-gestützt AMIs in S3 und stellen Sie sie aus S3 wieder her, um das partitionsübergreifende Kopieren von zu ermöglichen. AMIs	6. April 2021
EC2 Serielle Konsole	Beheben Sie Probleme mit dem Start und der Netzwerkkonnektivität, indem Sie eine Verbindung zum seriellen Port einer Instance herstellen.	30. März 2021
Startmodi	Amazon unterstützt EC2 jetzt UEFI-Boot auf ausgewählten AMD- und Intel-basierten Instances EC2 .	22. März 2021
Erstellen eines Reverse-DNS-Datensatzes	Sie können jetzt DNS-Rückwärtssuche für Ihre Elastic IP-Adressen einrichten.	3. Februar 2021
Tag AMIs und Schnappschüsse bei der AMI-Erstellung	Wenn Sie ein AMI erstellen, können Sie das AMI und die Snapshots mit denselben Tags (Markierungen) markieren oder sie mit verschiedenen Tags (Markierungen) markieren.	4. Dezember 2020

Verwenden Sie Amazon EventBridge , um Spot-Flottenereignisse zu überwachen	Erstellen Sie EventBridge Regeln, die als Reaktion auf Statusänderungen und Fehler von Spot Fleet programmatische Aktionen auslösen.	20. November 2020
Verwenden Sie Amazon EventBridge , um EC2 Flottenereignisse zu überwachen	Erstellen Sie EventBridge Regeln, die programmatische Aktionen als Reaktion auf Änderungen und Fehler im EC2 Flottenstatus auslösen.	20. November 2020
Löschen von instant-Flotten	Löschen Sie eine EC2 Flotte des Typs „Flotte“ `instant` und beenden Sie alle Instances in der Flotte in einem einzigen API-Aufruf.	18. November 2020
Ruhezustand-Unterstützung für T3 und T3a	Versetzen Ihre neu gestarteten Instances, die auf T3- und T3a-Instance-Typen ausgeführt werden, in den Ruhezustand.	17. November 2020
Amazon EFS Quick Create	Sie können ein Amazon-EFS-Dateisystem beim Start mit Amazon EFS Quick Create erstellen und in eine Instance einbinden.	9. November 2020
Instance-Metadatenkategorie: events/recommendations/rebalance	Der ungefähre Zeitpunkt in UTC, zu dem die Benachrichtigung über die Empfehlung zur Neugewichtung der EC2 Instance für die Instance ausgegeben wird.	4. November 2020

EC2 Empfehlung zur Neugewichtung der Instance	Ein Signal, das Sie benachrichtigt, wenn eine Spot-Instance ein erhöhtes Unterbrechungsrisiko hat.	4. November 2020
Kapazitätsreservierungen in Wavelength-Zonen	Kapazitätsreservierungen kann nun erstellt und in den Wavelength Zones verwendet werden.	4. November 2020
Kapazitätsausgleich	Konfigurieren Sie Spot Fleet oder EC2 Fleet so, dass eine Ersatz-Spot-Instance gestartet wird, wenn Amazon eine EC2 Empfehlung zur Neuverteilung ausgibt.	4. November 2020
Ruhezustand-Unterstützung für I3, M5ad und R5ad	Versetzen Sie Ihre neu gestarteten Instances, die auf I3-, M5ad- und R5ad-Instance-Typen ausgeführt werden, in den Ruhezustand.	21. Oktober 2020
vCPU-Limits für Spot-Instances	Spot-Instance-Limits werden jetzt anhand der Anzahl von v verwaltetCPUs , die Ihre laufenden Spot-Instances entweder verwenden oder bis zur Erfüllung offener Anfragen verwenden werden.	1. Oktober 2020
Kapazitätsreservierungen in Local Zones	Kapazitätsreservierungen kann nun in Local Zones erstellt und verwendet werden.	30. September 2020

Ruhezustand-Unterstützung für M5a und R5a	Versetzen Sie Ihre neu gestarteten Instances, die auf M5a- und R5a-Instance-Typen ausgeführt werden, in den Ruhezustand.	28. August 2020
Instance-Metadaten bieten Informationen zu Speicherort und Platzierung	Neue Instance-Metadaten felder unter der Kategorie `placement` : Region, Placement-Gruppennname, Partitionsnummer, Host-ID und Availability Zone-ID.	24. August 2020
Kapazitätsreservierungs-Gruppen	Sie können AWS Resource Groups verwenden, um logische Sammlungen von Kapazitätsreservierungen zu erstellen und dann Zielinstanzen in diesen Gruppen zu starten.	29. Juli 2020
EC2Starten Sie v2	Sie können EC2 Launch v2 verwenden, um Aufgaben während des Starts einer Instanz auszuführen, wenn eine Instanz gestoppt und später gestartet wird, wenn eine Instanz neu gestartet wird, und bei Bedarf. EC2Launch v2 unterstützt alle Versionen von Windows Server und ersetzt EC2 Launch und EC2 Config.	30. Juni 2020

Bringen Sie Ihre eigenen IPv6 Adressen mit	Sie können Ihren IPv6 Adressbereich ganz oder teilweise aus Ihrem lokalen Netzwerk auf Ihr AWS Konto übertragen.	21. Mai 2020
Starten von Instances mithilfe eines Systems-Manager-Parameters	Sie können einen AWS Systems Manager Parameter anstelle eines AMI angeben, wenn Sie eine Instance starten.	5. Mai 2020
Anpassen geplanter Ereignisbenachrichtigungen	Sie können geplante Ereignisbenachrichtigungen so anpassen, dass Tags (Markierungen) in die E-Mail-Benachrichtigung aufgenommen werden.	4. Mai 2020
Windows Server auf Dedicated Hosts	Sie können den von Amazon AMIs bereitgestellten Windows Server verwenden, um die neuesten Versionen von Windows Server auf Dedicated Hosts auszuführen.	7. April 2020
Stoppen und Starten einer Spot-Instance	Stoppen Sie Ihre von Amazon EBS unterstützten Spot-Instances und starten Sie sie nach Belieben, anstatt sich auf das Stop-Unterbrechungsverhalten zu verlassen.	13. Januar 2020

Ressourcen-Markierung	Sie können Internet-Gateways nur für ausgehend en Datenverkehr, lokale Gateways, Routing-Tabellen für lokale Gateways, virtuelle Schnittstellen von lokalen Gateways, virtuelle Schnittst ellengruppen von lokalen Gateways, VPC-Zuordnungen von Routing-Tabellen für lokale Gateways mit Tags (Markierungen) versehen.	10. Januar 2020
Verbinden mit Instance über Session Manager	Sie können eine Session Manager-Sitzung mit einer Instance von der EC2 Amazon-Konsole aus starten.	18. Dezember 2019
Dedicated Hosts und Hostressourcengruppen	Dedicated Hosts kann nun mit Hostressourcengruppen verwendet werden.	02. Dezember 2019
Dedicated-Host-Freigabe	Sie können Ihre Dedicated Hosts jetzt für mehrere AWS Konten gemeinsam nutzen.	02. Dezember 2019
Standardmäßige Guthaben-Spezifikation auf Kontoebene	Sie können die Standard-Kreditspezifikation pro Instance-Familie mit Burstable -Performance auf Kontoebene pro AWS Region festlegen.	25. November 2019
Erkennung von Instance-Typen	Sie können einen Instance-Typ finden, der Ihren Anforderungen entspricht.	22. November 2019

Dedicated Hosts	Sie können nun einen Dedicated Host konfigurieren, um mehrere Instance-Typen in einer Instance-Familie zu unterstützen.	21. November 2019
Instance Metadata Service Version 2	Sie können Instance-Metadatenservice Version 2 verwenden. Es handelt sich um eine sitzungsorientierte Methode zum Anfordern von Instance-Metadaten.	19. November 2019
Elastic Fabric Adapter	Elastic Fabric-Adapter können jetzt auch mit Intel MPI 2019 Update 6 verwendet werden.	15. November 2019
Ruhezustand-Unterstützung für On-Demand-Windows-Instances	Sie können On-Demand-Windows-Instances in den Ruhezustand versetzen.	14. Oktober 2019
In die Warteschlange gestellte Käufe von Reserved Instances	Sie können den Kauf einer Reserved Instance bis zu drei Jahre im Voraus in die Warteschlange einstellen.	4. Oktober 2019
Diagnose-Interrupt	Sie können einen Diagnose-Interrupt an eine unerreich bare oder nicht reagierende Instance senden, um eine Kernel-Panik auszulösen.	14. August 2019
Kapazitätsoptimierte Zuweisungsstrategie	Mit EC2 Fleet oder Spot Fleet können Sie Spot-Instances aus Spot-Pools mit optimaler Kapazität für die Anzahl der gestarteten Instances starten.	12. August 2019

On-Demand-Kapazitätsreservierungs-Freigabe	Sie können Ihre Kapazitätsreservierungen jetzt für mehrere AWS Konten gemeinsam nutzen.	29. Juli 2019
Elastic Fabric Adapter	EFA unterstützt jetzt Open MPI 3.1.4 und Intel MPI 2019 Update 4.	26. Juli 2019
EC2 Instanzverbindung	EC2 Instance Connect ist eine einfache und sichere Methode, um mithilfe von Secure Shell (SSH) eine Verbindung zu Ihren Instances herzustellen.	27. Juni 2019
Host-Wiederherstellung	Starten Sie Ihre Instance bei einem unerwarteten Hardware-Ausfall auf einem Dedicated Host auf einem neuen Host neu.	5. Juni 2019
Anwendungskonsistente VSS-Snapshots	Erstellen Sie mit Run Command anwendungskonsistente Snapshots aller Amazon EBS-Volumes, die an Ihre Windows-Instances angehängt sind. AWS Systems Manager	13. Mai 2019
Assistent zum Ändern der Plattform von Windows auf Linux für Microsoft SQL Server-Datenbanken	Verschieben Sie vorhandene Microsoft SQL Server-Workloads von einem Windows- zu einem Linux-Betriebssystem. Der aktualisierte Link verweist auf das Microsoft SQL Server on EC2 Amazon-Benutzerhandbuch.	8. Mai 2019

Automatisiertes Windows-Upgrade	Führen Sie automatisierte Upgrades von EC2 Windows-Instances durch mit AWS Systems Manager.	6. Mai 2019
Elastic Fabric Adapter	Sie können einen Elastic Fabric Adapter an Ihre Instances anfügen, um High Performance Computing (HPC)-Anwendungen zu beschleunigen.	29. April 2019

Informationen zu den Instance-Typ-Releases für Amazon EC2 finden Sie unter Dokumentverlauf im Amazon EC2 Instance Types Guide.

Verlauf für 2018 und früher

In der folgenden Tabelle werden wichtige Ergänzungen des EC2 Amazon-Benutzerhandbuchs im Jahr 2018 und in früheren Jahren beschrieben.

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Partitions-Placement-Gruppen	15.11.2016	Partitions-Placement-Gruppen verteilen Instances über logische Partitionen. Sie gewährleisten dabei, dass Instances in einer Partition keine zugrunde liegende Hardware mit Instances in anderen Partitionen teilen. Weitere Informationen finden Sie unter Partitions-Placement-Gruppen.	20. Dezember 2018
Versetzen Sie Linux-Instances in den Ruhezustand EC2	15.11.2016	Sie können eine Linux-Instance nur dann in den Ruhezustand versetzen, wenn sie für den Ruhezustsand aktiviert ist und die Vorausset	28. November 2018

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
		zungen für den Ruhezustand erfüllt. Weitere Informationen finden Sie unter Versetzen Sie Ihre Amazon-Instance in den Ruhezustand EC2 .	
Amazon Elastic Inference Accelerators	15.11.2016	Sie können Ihren Instances einen Amazon EI-Accelerator hinzufügen, um GPU-gesteuerte Beschleunigung zu nutzen und dadurch die Kosten für die Ausführung von Deep Learning-Inferenz zu senken.	28. November 2018
Spot-Konsole empfiehlt eine Flotte von Instances	15.11.2016	Die Spot-Konsole empfiehlt eine Flotte von Instances, die auf den bewährten Methoden von Spot (Instance-Diversifizierung) basieren, um die Hardware-Mindestanforderungen (VCPUs, Arbeitsspeicher und Speicher) für Ihre Anwendungsanforderungen zu erfüllen. Weitere Informationen finden Sie unter Erstellen einer Spot-Flotte.	20. November 2018
Neuer EC2 Flottenanfragetyp: instant	15.11.2016	EC2 Fleet unterstützt jetzt einen neuen Anforderungstyp`instant`, mit dem Sie synchron Kapazität für verschiedene Instance-Typen und Kaufmodelle bereitstellen können. Die `instant`-Anforderung gibt die gestarteten Instances in der API-Antwort zurück und führt keine weiteren Aktionen durch, sodass Sie steuern können, ob und wann Instances gestartet werden. Weitere Informationen finden Sie unter EC2-Flotten- und Spot-Flotten-Anforderungstypen.	14. November 2018

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Informationen zu Spot-Einsparungen	15.11.2016	Sie können die Einsparungen anzeigen, die durch die Verwendung von Spot-Instances für eine einzelne Spot-Flotte oder für alle Spot-Instances erzielt wurden. Weitere Informationen finden Sie unter Einsparungen durch den Spot-Instances-Einkauf.	5. November 2018
Konsolenunterstützung zur Optimierung der CPU-Optionen	15.11.2016	Wenn Sie eine Instance starten, können Sie die CPU-Optionen mithilfe der EC2 Amazon-Konsole an bestimmte Workloads oder Geschäftsanforderungen anpassen. Weitere Informationen finden Sie unter CPU-Optionen für EC2 Amazon-Instances.	31. Oktober 2018
Konsolenunterstützung zum Erstellen einer Startvorlage anhand einer Instance	15.11.2016	Sie können mithilfe der EC2 Amazon-Konsole eine Startvorlage erstellen, indem Sie eine Instance als Grundlage für eine neue Startvorlage verwenden. Weitere Informationen finden Sie unter Erstellen Sie eine EC2 Amazon-Startvorlage.	30. Oktober 2018
On-Demand Capacity Reservations	15.11.2016	Sie können Kapazität für Ihre EC2 Amazon-Instances in einer bestimmten Availability Zone für einen beliebigen Zeitraum reservieren. Auf diese Weise können Sie Kapazitätsreservierungen unabhängig von den Abrechnungsrabatten der Reserved Instances (RI) anlegen und verwalten. Weitere Informationen finden Sie unter Reservieren Sie Rechenkapazität mit Kapazitätsreservierungen EC2 auf Abruf.	25. Oktober 2018

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Eigene IP-Adressen mitbringen (BYOIP)	15.11.2016	Sie können Ihren öffentlichen IPv4 Adressbereich ganz oder teilweise aus Ihrem lokalen Netzwerk auf Ihr AWS Konto übertragen. Nachdem Sie den Adressbereich auf übertragen haben AWS, wird er in Ihrem Konto als Adresspool angezeigt. Sie können eine elastische IP-Adresse aus Ihrem Adresspool erstellen und diese mit Ihren AWS -Ressourcen verwenden. Weitere Informationen finden Sie unter Bringen Sie Ihre eigenen IP-Adressen (BYOIP) zu Amazon EC2.	23. Oktober 2018
Dedicated Host-Tags (Markierungen) beim Erstellen und Konsolenunterstützung	15.11.2016	Sie können Ihre Dedicated Hosts bei der Erstellung taggen und Sie können Ihre Dedicated Host-Tags über die EC2 Amazon-Konsole verwalten. Weitere Informationen finden Sie unter Weisen Sie Ihrem Konto einen Amazon EC2 Dedicated Host zu.	08. Oktober 2018
Konsolenunterstützung für geplante Skalierungsaktionen für Spot-Flotten	15.11.2016	Erhöhen oder Verringern der aktuellen Kapazität der Flotte auf Grundlage von Datum und Zeit. Weitere Informationen finden Sie unter Geplante Skalierung: Spot-Flotte nach einem Zeitplan skalieren.	20. September 2018

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Allokationsstrategien für EC2 Flotten	15.11.2016	Sie können angeben, ob die On-Demand-Kapazität nach Preis (niedrigster Preis an erster Stelle) oder nach Priorität (höchste Priorität an erster Stelle) erfüllt wird. Sie können die Anzahl der Spot-Pools angeben, über die Ihre Spot-Zielkapazität zugewiesen werden soll. Weitere Informationen finden Sie unter Verwenden Sie Zuweisungsstrategien, um festzustellen, wie die EC2-Flotte oder Spot-Flotte die Spot- und On-Demand-Kapazitäten ausfüllt.	26. Juli 2018
Zuweisungsstrategien für Spot-Flotten	15.11.2016	Sie können angeben, ob die On-Demand-Kapazität nach Preis (niedrigster Preis an erster Stelle) oder nach Priorität (höchste Priorität an erster Stelle) erfüllt wird. Sie können die Anzahl der Spot-Pools angeben, über die Ihre Spot-Zielkapazität zugewiesen werden soll. Weitere Informationen finden Sie unter Verwenden Sie Zuweisungsstrategien, um festzustellen, wie die EC2-Flotte oder Spot-Flotte die Spot- und On-Demand-Kapazitäten ausfüllt.	26. Juli 2018
Automatisieren des Snapshot-Lebenszyklus	15.11.2016	Sie können mit Amazon Data Lifecycle Manager das Erstellen und Löschen von Snapshots für Ihre EBS-Volumes automatisieren. Weitere Informationen hierzu finden Sie unter Amazon Data Lifecycle Manager.	12. Juli 2018

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
CPU-Optionen für Startvorlagen	15.11.2016	Wenn Sie unter Verwendung der Befehlszeilen-Tools eine Vorlage starten, können Sie die CPU-Optionen für bestimmte Workloads oder Geschäftsanforderungen optimieren. Weitere Informationen finden Sie unter Erstellen Sie eine EC2 Amazon-Startvorlage.	11. Juli 2018
Dedicated Hosts markieren	15.11.2016	Sie können Ihre Dedicated Hosts markieren.	3. Juli 2018
Abrufen der neuesten Konsolenausgabe	15.11.2016	Sie können die neueste Konsolenausgabe für einige Instance-Typen abrufen, wenn Sie den get-console-output AWS CLI Befehl verwenden .	9. Mai 2018
CPU-Optionen optimieren	15.11.2016	Wenn Sie eine Instance starten, können Sie die CPU-Optionen für bestimmte Workloads oder Geschäftsanforderungen optimieren. Weitere Informationen finden Sie unter CPU-Optionen für EC2 Amazon-Instances.	8. Mai 2018
EC2 Flotte	15.11.2016	Sie können EC2 Fleet verwenden, um eine Gruppe von Instances für verschiedene EC2 Instance-Typen und Availability Zones sowie für die Kaufmodelle On-Demand-Instance , Reserved Instance und Spot-Instance zu starten. Weitere Informationen finden Sie unter EC2 Flotte und Spot-Flotte.	2. Mai 2018

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
On-Demand-Instances in Spot-Flotten	15.11.2016	Sie können eine Anforderung nach On-Demand-Kapazität in Ihre Spot-Flotten-Anforderung aufnehmen, um sicherzustellen, dass Sie immer über Instance-Kapazität verfügen. Weitere Informationen finden Sie unter EC2 Flotte und Spot-Flotte.	2. Mai 2018
EBS-Snapshots bei der Erstellung mit Tags (Markierungen) versehen	15.11.2016	Sie können Snapshots während der Erstellung mit Tags (Markierungen) versehen.	2. April 2018
Placement-Gruppen ändern	15.11.2016	Sie können eine Instance in oder aus einer Platzierungsgruppe verschieben oder deren Platzierungsgruppe ändern. Weitere Informationen finden Sie unter Platzierung für eine EC2-Instance ändern.	1. März 2018
Längere Ressource IDs	15.11.2016	Sie können das längere ID-Format für weitere Ressourcentypen aktivieren.	9. Februar 2018
Verbesserungen der Netzwerkleistung	15.11.2016	Instances außerhalb einer Cluster Placement-Gruppe können jetzt von einer erhöhten Bandbreite profitieren, wenn sie Netzwerkverkehr zwischen anderen Instances oder Amazon S3 senden oder empfangen.	24. Januar 2018
Elastic IP-Adressen markieren	15.11.2016	Sie können Ihre Elastic IP-Adressen markieren.	21. Dezember 2017

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Amazon Time Sync Service	15.11.2016	Sie können den Amazon Time Sync Service verwenden, um zuverlässige Zeiteinstellungen für Ihre Instance zu gewährleisten. Weitere Informationen finden Sie unter Präzise Uhr- und Zeitsynchronisierung auf Ihrer EC2-Instance.	29. November 2017
T2 Unlimited	15.11.2016	T2 Unlimited-Instances können die Leistung so lange, wie nötig, über die Baseline hinaus steigern. Weitere Informationen finden Sie unter Burstable Performance Instances.	29. November 2017
Startvorlagen	15.11.2016	Eine Startvorlage kann alle oder einige der Parameter zum Starten einer Instance enthalten. Auf diese Weise müssen Sie sie nicht jedes Mal angeben, wenn Sie eine Instance starten. Weitere Informationen finden Sie unter Instance-Startparameter in EC2 Amazon-Startvorlagen speichern.	29. November 2017
Spread Placement	15.11.2016	Spread Placement-Gruppen werden für Anwendungen mit einer geringen Anzahl kritischer Instances empfohlen, die getrennt voneinander gehalten werden sollten. Weitere Informationen finden Sie unter Spread Placement-Gruppen.	29. November 2017
Spot-Instance-Ruhezustand	15.11.2016	Der Spot-Service kann Spot-Instances im Falle einer Unterbrechung in den Ruhezustand versetzen.	28. November 2017

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Spot-Flotten-Zielverfolgung	15.11.2016	Sie können Skalierungsrichtlinien für die Zielverfolgung für Ihre Spot-Flotte einrichten. Weitere Informationen finden Sie unter Skalierung der Zielverfolgung: Skalieren der Spot-Flotte, indem auf einen Wert für eine bestimmte Metrik abgezielt wird.	17. November 2017
Spot Fleet lässt sich in ELB integrieren	15.11.2016	Sie können einen oder mehrere Load Balancer an eine Spot-Flotte anfügen.	10. November 2017
Zusammenführen und Teilen von Convertible Reserved Instances	15.11.2016	Sie können zwei oder mehrere Convertible Reserved Instances durch eine neue Convertible Reserved Instance ersetzen (bzw. in einer neuen zusammenführen). Außerdem können Sie eine Convertible Reserved Instance durch diesen Prozess in kleinere Reservierungen aufteilen. Weitere Informationen finden Sie unter Austauschen von Convertible Reserved Instances.	6. November 2017
Ändern der VPC-Tenancy	15.11.2016	Das Attribut für die Instance-Tenancy einer VPC kann von `dedicated` in `default` geändert werden. Weitere Informationen finden Sie unter Ändern der Instance-Tenancy einer VPC.	16. Oktober 2017
Sekundengenaue Abrechnung	15.11.2016	Amazon EC2 berechnet die Linux-basierte Nutzung sekundengenau mit einer Mindestgebühr von einer Minute.	2. Oktober 2017

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Stopp bei Unterbrechungen	15.11.2016	Sie können angeben, ob Amazon Spot-Instances stoppen oder beenden EC2 soll, wenn sie unterbrochen werden. Weitere Informationen finden Sie unter Verhalten von Spot-Instance-Unterbrechungen.	18. September 2017
Markieren von NAT-Gateways	15.11.2016	Sie können Ihren NAT-Gateway markieren. Weitere Informationen finden Sie unter Markieren Ihrer -Ressourcen mit Tags (Markierungen).	7. September 2017
Beschreibungen der Sicherheitsgruppenregel	15.11.2016	Sie können Ihren Sicherheitsgruppenregeln Beschreibungen hinzufügen.	31. August 2017
Elastic Graphics	15.11.2016	Fügen Sie Ihren Instances Elastic Graphics-Accelerators hinzu, um die Grafikleistung Ihrer Anwendungen zu verbessern.	29. August 2017
Wiederherstellen von Elastic IP-Adressen	15.11.2016	Wenn Sie eine Elastic IP-Adresse für die Verwendung in einer VPC freigeben, können Sie sie möglicherweise wiederherstellen.	11. August 2017
Markieren von Spot-Flotten-Instances	15.11.2016	Sie können Ihre Spot-Flotte so konfigurieren, dass die gestarteten Instances automatisch markiert werden.	24. Juli 2017

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Zuordnung von Tags (Markierungen) zu Ressourcen während der Erstellung	15.11.2016	Sie können Instances und Volumes zum Zeitpunkt der Erstellung Tags (Markierungen) zuordnen. Weitere Informationen finden Sie unter Markieren Ihrer -Ressourcen mit Tags (Markierungen). Darüber hinaus können Sie Tag (Markierung)-basierte Berechtigungen auf Ressourcenebene dazu verwenden, die Tags (Markierungen) zu kontrollieren, die angewendet werden. Weitere Informationen finden Sie unter Erteilen Sie die Erlaubnis, EC2 Amazon-Ressourcen während der Erstellung zu taggen.	28. März 2017
Durchführen von Modifikationen bei angefügten EBS-Volumes	15.11.2016	Da die meisten EBS-Volumes an die meisten EC2 Instances angeschlossen sind, können Sie Volume-Größe, Typ und IOPS ändern, ohne das Volume zu trennen oder die Instance anzuhalten.	13. Februar 2017
Hinzufügen einer IAM-Rolle	15.11.2016	Sie können eine IAM-Rolle zu einer bestehenden Instance hinzufügen, sie von der Instance trennen oder sie ersetzen. Weitere Informationen finden Sie unter IAM-Rollen für Amazon EC2.	9. Februar 2017
Dedicated Spot Instances	15.11.2016	Sie können Spot-Instances auf Single-Tenant-Hardware in einer Virtual Private Cloud (VPC) ausführen. Weitere Informationen finden Sie unter Auf Einzel-Tenant-Hardware starten.	19. Januar 2017

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
IPv6 Unterstützung	15.11.2016	Sie können Ihrer VPC und Ihren Subnetzen einen IPv6 CIDR zuordnen und Instances in Ihrer VPC IPv6 Adressen zuweisen. Weitere Informationen finden Sie unter IP-Adressierung von Amazon EC2-Instances.	1. Dezember 2016
Automatische Skalierung für Spot-Flotten		Sie können jetzt Skalierungsrichtlinien für Ihre Spot-Flotte einrichten. Weitere Informationen finden Sie unter Automatische Skalierung für Spot-Flotten verstehen.	1. September 2016
Elastic Network Adapter (ENA)	01.04.2016	Sie können ENA jetzt für Enhanced Networking verwenden. Weitere Informationen finden Sie unter Erweitertes Netzwerk in Amazon-EC2-Instances.	28. Juni 2016
Verbesserte Unterstützung für längeres Anzeigen und Ändern IDs	01.04.2016	Sie können jetzt längere ID-Einstellungen für andere IAM-Benutzer, IAM-Rollen oder den Stammbenutzer anzeigen und ändern.	23. Juni 2016
Verschlüsselte Amazon EBS-Snapshots zwischen Konten kopieren AWS	01.04.2016	Sie können jetzt verschlüsselte EBS-Snapshots zwischen Konten kopieren. AWS	21. Juni 2016
Aufnehmen eines Screenshots einer Instance-Konsole	01.10.2015	Sie können jetzt zusätzliche Informationen erhalten, wenn Sie ein Debugging bei Instances vornehmen, die nicht erreichbar sind. Weitere Informationen finden Sie unter Aufnehmen eines Screenshots einer nicht erreichbaren Instance.	24. Mai 2016

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Zwei neue EBS-Volume-Typen	01.10.2015	Sie können jetzt Throughput Optimized HDD(st1)- und Cold HDD(sc1)-Volumes erstellen.	19. April 2016
Neue NetworkPacketsIn und NetworkPacketsOut Metriken für Amazon hinzugefügt EC2		Neue NetworkPacketsIn und NetworkPacketsOut Metriken für Amazon hinzugefügt EC2. Weitere Informationen finden Sie unter Instance-Metriken.	23. März 2016
CloudWatch Metriken für Spot Fleet		Sie können jetzt CloudWatch Metriken für Ihre Spot-Flotte abrufen. Weitere Informationen finden Sie unter Überwachen Sie Ihre EC2 Flotte oder Spot-Flotte mit CloudWatch.	21. März 2016
Geplante Instances	01.10.2015	Geplante Reserved Instances (geplante Instances) ermöglichen Ihnen, Kapazitätsreservierungen, die täglich, wöchentlich oder monatlich wiederkehren, mit Angabe von Startzeit und Dauer zu kaufen.	13. Januar 2016
Längere Ressource IDs	01.10.2015	Wir führen schrittweise eine längere Länge IDs für einige Amazon EC2 - und Amazon EBS-Ressourcentypen ein. Während des Übergangszeitraums können Sie das längere ID-Format für unterstützte Ressourcentypen aktivieren.	13. Januar 2016
ClassicLink DNS-Unterstützung	01.10.2015	Sie können die ClassicLink DNS-Unterstützung für Ihre VPC aktivieren, sodass DNS-Hostnamen, die zwischen verknüpften EC2 -Classic-Instances und Instances in der VPC adressiert werden, in private IP-Adressen und nicht in öffentliche IP-Adressen aufgelöst werden.	11. Januar 2016

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Dedicated Hosts	01.10.2015	Ein Amazon EC2 Dedicated Host ist ein physischer Server mit Instance-Kapazität, die für Ihre Nutzung reserviert ist. Weitere Informationen finden Sie unter EC2 Dedizierte Amazon-Hosts.	23. November 2015
Spot-Instance-Dauer	01.10.2015	Sie können jetzt eine Dauer für Ihre Spot-Instances festlegen. Spot-Blocks werden nicht unterstützt (Januar 2023).	6. Oktober 2015
Anforderung zur Änderung einer Spot-Flotte	01.10.2015	Sie können jetzt die Zielkapazität Ihrer Spot-Flotten-Anforderung ändern. Weitere Informationen finden Sie unter Ändern einer Spot-Flotten-Anforderung.	29. September 2015
Diversifizierte Zuordnungsstrategie für Spot-Flotten	15.04.2015	Sie können jetzt Spot-Instances in mehreren Spot-Pools mithilfe einer einzigen Spot-Flotten-Anforderung zuordnen. Weitere Informationen finden Sie unter Verwenden Sie Zuweisungsstrategien, um festzustellen, wie die EC2-Flotte oder Spot-Flotte die Spot- und On-Demand-Kapazitäten ausfüllt.	15. September 2015
Instance-Gewichtung für Spot-Flotten	15.04.2015	Sie können jetzt Kapazitätseinheiten definieren, die jeder Instance-Typ zur Leistung Ihrer Anwendung beiträgt, und Ihren Gebotspreis für Spot-Instances jeden Spot-Pool entsprechend anpassen. Weitere Informationen finden Sie unter Instance-Gewichtung verwenden, um die Kosten und die Leistung Ihrer EC2-Flotte oder Spot-Flotte zu verwalten.	31. August 2015

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Neue Neustart-Alarmaktion und neue IAM-Rolle für die Verwendung mit Alarmaktionen		Neustart-Alarmaktion und neue IAM-Rolle für die Verwendung mit Alarmaktionen hinzugefügt. Weitere Informationen finden Sie unter Erstellen von Alarmen, mit denen eine Instance angehalten, beendet, neu gestartet oder wiederhergestellt wird.	23. Juli 2015
Spot Fleets	15.04.2015	Sie können eine Sammlung oder Flotte von Spot-Instances verwalten, anstatt getrennte Spot-Instance-Anforderungen verwalten zu müssen. Weitere Informationen finden Sie unter EC2 Flotte und Spot-Flotte.	18. Mai 2015
Migrieren Sie Elastic IP-Adressen zu EC2 -Classic	15.04.2015	Sie können eine Elastic IP-Adresse, die Sie für die Verwendung in EC2 -Classic zugewiesen haben, zur Verwendung in einer VPC migrieren .	15. Mai 2015
Import VMs mit mehreren Festplatten als AMIs	01.03.2015	Der VM-Importvorgang unterstützt jetzt den Import VMs mit mehreren Festplatten als AMIs. Weitere Informationen finden Sie unter Importieren einer VM als Image mithilfe von VM Import/Export im Import/Export VM-Benutzerhandbuch.	23. April 2015
Systems Manager		Systems Manager ermöglicht es Ihnen, Ihre EC2 Instanzen zu konfigurieren und zu verwalten.	17. Februar 2015
Systems Manager for Microsoft SCVMM 1.5		Sie können jetzt Systems Manager for Microsoft SCVMM verwenden, um eine Instance zu starten und eine VM von SCVMM nach Amazon zu importieren. EC2	21. Januar 2015

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Automatische Wiederherstellung für Instanzen EC2		Sie können einen CloudWatch Amazon-Alarm erstellen, der eine EC2 Amazon-Instance überwacht und die Instance automatisch wiederherstellt, wenn sie aufgrund eines zugrunde liegenden Hardwarefehlers oder eines Problems, das eine Reparatur erfordert AWS , beeinträchtigt wird. Eine wiederhergestellte Instance ist mit der ursprünglichen Instance identisch. Dies schließt auch die Instance-ID, IP-Adressen und alle Instance-Metadaten mit ein. Weitere Informationen finden Sie unter Automatische Instance-Wiederherstellung.	12. Januar 2015
ClassicLink	01.10.2014	ClassicLink ermöglicht es Ihnen, Ihre EC2 -Classic-Instance mit einer VPC in Ihrem Konto zu verknüpfen. Sie können VPC-Sicherheitsgruppen mit der EC2 -Classic-Instance verknüpfen und so die Kommunikation zwischen Ihrer EC2 -Classic-Instance und Instances in Ihrer VPC über private IP-Adressen ermöglichen.	07. Januar 2015

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Benachrichtigungen über Spot-Instance-Unterbrechungen		Am besten können Sie Ihre Anwendung vor einer Spot-Instance-Unterbrechung schützen, indem Sie sie so konzipieren, dass sie fehlertolerant ist. Darüber hinaus können Sie Benachrichtigungen zur Kündigung von Spot-Instances nutzen, die eine zweiminütige Warnung enthalten, bevor Amazon Ihre Spot-Instance kündigen EC2 muss. Weitere Informationen finden Sie unter Spot-Instance-Unterbrechungsbenachrichtigungen.	5. Januar 2015
Systems Manager for Microsoft SCVMM		Systems Manager for Microsoft SCVMM bietet eine einfache easy-to-use Oberfläche für die Verwaltung von AWS Ressourcen, wie z. B. EC2 Instanzen, von Microsoft SCVMM aus.	29. Oktober 2014
`DescribeVolumes` Paginierungsunterstützung	01.09.2014	Der API-Aufruf `DescribeVolumes` unterstützt jetzt die Paginierung von Ergebnissen mit den Parametern `MaxResults` und `NextToken`. Weitere Informationen finden Sie DescribeVolumesin der Amazon EC2 API-Referenz.	23. Oktober 2014

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Unterstützung für Amazon CloudWatch Logs hinzugefügt		Sie können Amazon CloudWatch Logs verwenden, um Ihre System-, Anwendungs- und benutzerdefinierten Protokolldateien von Ihren Instances oder anderen Quellen aus zu überwachen, zu speichern und darauf zuzugreifen. Anschließend können Sie die zugehörigen Protokolldaten mithilfe der CloudWatch Amazon-Konsole, der CloudWatch Logs-Befehle in der AWS CLI oder des CloudWatch Logs-SDK aus CloudWatch Logs abrufen.	10. Juli 2014
Neue Seite mit EC2 Service-Limits		Verwenden Sie die Seite EC2 Service Limits in der EC2 Amazon-Konsole, um die aktuellen Limits für Ressourcen, die von Amazon EC2 und Amazon VPC bereitgestellt werden, für jede Region einzusehen.	19. Juni 2014
Amazon EBS-Allzweck-SSD-Volumes	01.05.2014	Allzweck-SSD-Volumes bieten kostengünstigen Speicher, der für ein breites Spektrum an Workloads gedacht ist. Diese Volumes bieten Latenzen im einstelligen Millisekundenbereich, die Möglichkeit, für längere Zeiträume auf 3 000 IOPS zu beschleunigen und eine Basisleistung von 3 IOPS/GiB. Universelle SSD-Volumes verfügen über Größen von 1 GiB bis 1 TiB.	16. Juni 2014
AWS Management Pack		AWS Das Management Pack unterstützt jetzt System Center Operations Manager 2012 R2.	22. Mai 2014

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Amazon EBS encryption	01.05.2014	Amazon EBS-Verschlüsselung bietet nahtlose Verschlüsselung von EBS-Daten-Volumes und Snapshots, wodurch die Notwendigkeit entfällt, eine sichere Infrastruktur zur Schlüsselverwaltung aufzubauen und zu unterhalten. Die EBS-Verschlüsselung gewährleistet die Sicherheit gespeicherter Daten, indem Ihre Daten mithilfe von Von AWS verwaltete Schlüssel verschlüsselt werden. Die Verschlüsselung erfolgt auf den Servern, die EC2 Instanzen hosten, und sorgt für die Verschlüsselung von Daten, die zwischen EC2 Instanzen und EBS-Speicher übertragen werden.	21. Mai 2014
EC2 Amazon-Nutzungsberichte		EC2 Amazon-Nutzungsberichte sind eine Reihe von Berichten, die Kosten- und Nutzungsdaten Ihrer Nutzung von enthalten EC2.	28. Januar 2014
Importieren virtueller Maschinen mit Linux-Betriebssystem	15.10.2013	Der VM Import-Prozess unterstützt jetzt den Import von Linux-Instances. Weitere Informationen finden Sie im Import/Export VM-Benutzerhandbuch.	16. Dezember 2013
Berechtigungen auf Ressourcenebene für RunInstances	15.10.2013	Sie können jetzt Richtlinien erstellen AWS Identity and Access Management , um die Berechtigungen auf Ressourcenebene für die EC2 RunInstances Amazon-API-Aktion zu kontrollieren. Weitere Informationen und Beispielrichtlinien finden Sie unter Identitäts- und Zugriffsmanagement für Amazon EC2.	20. November 2013

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Starten einer Instance von AWS Marketplace		Sie können jetzt eine Instance AWS Marketplace mithilfe des EC2 Amazon-Startassistenten starten. Weitere Informationen finden Sie unter Starten einer Amazon-EC2-Instance von einem AWS Marketplace-AMI.	11. November 2013
Neuer Launch Wizard		Es gibt einen neuen und neu gestalteten EC2 Startassistenten. Weitere Informationen finden Sie unter EC2-Instance mit dem Launch Instance Wizard in der Konsole starten.	10. Oktober 2013
Instance-Typen von Reserved Instances ändern	01.10.2013	Sie können jetzt den Instance-Typ von Linux-Reserved Instances innerhalb derselben Familie ändern (z. B. M1, M2, M3, C1). Weitere Informationen finden Sie unter Ändern von Reserved Instances.	09. Oktober 2013
Ändern von Amazon EC2 Reserved Instances	15.08.2013	Sie können jetzt Reserved Instances in einer Region ändern. Weitere Informationen finden Sie unter Ändern von Reserved Instances.	11. September 2013
Zuweisen einer öffentlichen IP-Adresse	15.07.2013	Sie können jetzt eine öffentliche IP-Adresse zuweisen, wenn Sie eine Instance in einer VPC starten. Weitere Informationen finden Sie unter Eine öffentliche IPv4-Adresse beim Start zuweisen.	20. August 2013
Gewähren von Berechtigungen auf Ressourcenebene	15.06.2013	Amazon EC2 unterstützt neue Amazon-Ressourcennamen (ARNs) und Bedingungsschlüssel. Weitere Informationen finden Sie unter Identitätsbasierte Richtlinien für Amazon EC2.	8. Juli 2013

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Inkrementelle Snapshot-Kopien	01.02.2013	Sie können jetzt inkrementelle Snapshot-Kopien erstellen.	11. Juni 2013
AWS Management Pack		Das AWS Management Pack verknüpft EC2 Amazon-Instances und die darin ausgeführten Windows- oder Linux-Betriebssysteme. Das AWS Management Pack ist eine Erweiterung für Microsoft System Center Operations Manager.	8. Mai 2013
Neue Tags-Seite		In der EC2 Amazon-Konsole gibt es eine neue Tags-Seite. Weitere Informationen finden Sie unter Kennzeichnen Sie Ihre EC2 Amazon-Ressourcen.	04. April 2013
Kopieren eines AMI von einer Region in eine andere	01.02.2013	Sie können ein AMI von einer Region in eine andere kopieren, sodass Sie schnell und einfach konsistente Instances in mehr als einer AWS Region starten können. Weitere Informationen finden Sie unter Ein EC2 Amazon-AMI kopieren.	11. März 2013
Starten von Instances in einer Standard-VPC	01.02.2013	Ihr AWS Konto ist in der Lage, Instances entweder in EC2 -Classic oder einer VPC oder nur in einer VPC auf einer Basis zu starten. region-by-region Falls Sie Instances nur in der VPC starten können, erstellen wir eine standardmäßige VPC für Sie. Wir starten Ihre Instance dann in Ihrer standardmäßigen VPC, sofern Sie keine nicht standardmäßige VPC erstellt und beim Start der Instance angegeben haben.	11. März 2013

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
EBS-Snapshot-Kopie	01.12.2012	Sie können Snapshot-Kopien verwenden, um Datensicherungen zu erstellen, neue Amazon EBS-Volumes zu erstellen oder Amazon Machine Images (AMIs) zu erstellen.	17. Dezember 2012
Aktualisierte EBS-Metriken und Statusprüfungen für Provisioned IOPS SSD-Volumes	01.10.2012	EBS-Metriken wurden aktualisiert, um zwei neue Metriken für Provisioned IOPS SSD-Volumes aufzunehmen. Außerdem wurden neue Statusprüfungen für Provisioned IOPS SSD-Volumes hinzugefügt.	20. November 2012
Status von Spot-Instance-Anforderungen	01.10.2012	Mit der Spot-Instance-Statusabfrage lässt sich der Status Ihrer Spot-Anforderungen leicht ermitteln.	14. Oktober 2012
Amazon EC2 Reserved Instance Marketplace	15.08.2012	Der Reserved Instance Marketplace bringt Verkäufer mit Amazon EC2 Reserved Instances, die sie nicht mehr benötigen, mit Käufern zusammen, die zusätzliche Kapazität erwerben möchten. Reserved Instances, die über den Reserved Instance Marketplace gekauft und verkauft werden, funktionieren so wie andere Reserved Instances, mit der Ausnahme, dass sie möglicherweise nicht mehr die volle Standardlaufzeit bieten und zu anderen Preisen verkauft werden können.	11. September 2012
Provisioned IOPS SSD für Amazon EBS	20.07.2012	Provisioned IOPS SSD-Volumes liefern eine kalkulierbare, hohe Leistung für I/O-intensive Workloads, z. B. Datenbankanwendungen, für die konsistente und schnelle Reaktionszeiten erforderlich sind.	31. Juli 2012

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
IAM-Rollen auf Amazon-Instances EC2	01.06.2012	IAM-Rollen für Amazon EC2 bieten: • AWS Zugriffsschlüssel für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden. • Automatische Rotation der AWS Zugriffsschlüssel auf der EC2 Amazon-Instance. • Granulare Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden und Anfragen an Ihre AWS Services stellen.	11. Juni 2012

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Spot-Instance-Features, die es einfacher machen, erste Schritte zu unternehmen und das Störungspotenzial zu bewältigen.		Sie können Ihre Spot-Instances jetzt wie folgt verwalten: • Definieren Sie unter Verwendung der Auto Scaling Startkonfigurationen ein Gebot für Spot-Instances. Erstellen Sie einen Zeitplan für die Definition des Gebots, das Sie für Spot-Instances abgeben möchten. Weitere Informationen finden Sie unter Spot-Instances anfordern im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch. • Erhalten von Benachrichtigungen, wenn Instances gestartet oder beendet werden. • Verwenden Sie CloudFormation Vorlagen, um Spot-Instances in einem Stapel mit AWS Ressourcen zu starten.	7. Juni 2012
EC2 Instanzexport und Zeitstempel für Statuschecks für Amazon EC2	01.05.2012	Unterstützung für den Export von Windows Server-Instances hinzugefügt, in die Sie ursprünglich importiert EC2 haben. Unterstützung für Zeitstempel für Instance- und Systemstatus wurde hinzugefügt, um das Datum und den Zeitpunkt anzuzeigen, zu dem eine Statusprüfung fehlgeschlagen ist.	25. Mai 2012

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
EC2 Instance-Export und Zeitstempel bei Instance- und Systemstatusprüfungen für Amazon VPC	01.05.2012	Unterstützung für den EC2 Instanzexport nach Citrix Xen, Microsoft Hyper-V und VMware vSphere hinzugefügt. Unterstützung für Zeitstempel in Instance- und Systemstatusprüfungen wurde hinzugefügt.	25. Mai 2012
AWS Marketplace AMIs	01.04.2012	Unterstützung für hinzugefügt. AWS Marketplace AMIs	19. April 2012
Preisstufen für Reserved Instances	15.12.2011	Ein neuer Abschnitt wurde hinzugefügt, in dem behandelt wird, wie die Rabatte genutzt werden können, die in die Preisstufen für Reserved Instances integriert sind.	5. März 2012
Elastische Netzwerkschnittstellen (ENIs) für EC2 Instanzen in Amazon Virtual Private Cloud	01.12.2011	Ein neuer Abschnitt über elastische Netzwerkschnittstellen (ENIs) für EC2 Instances in einer VPC wurde hinzugefügt. Weitere Informationen finden Sie unter Elastic-Network-Schnittstelle.	21. Dezember 2011
Neue Angebotstypen für Amazon EC2 Reserved Instances	01.11.2011	Sie können aus einer Vielzahl von Reserved Instance-Angeboten auswählen, die auf Ihre projizierte Nutzung der Instance abgestimmt sind.	01. Dezember 2011

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
EC2 Amazon-Instanzstatus	01.11.2011	Sie können zusätzliche Informationen zum Status Ihrer Instances einsehen, einschließlich der von Ihnen geplanten geplanten Ereignisse AWS , die sich auf Ihre Instances auswirken könnten. Zu diesen Betriebsaktivitäten gehören Instance-Neustarts, die zur Anwendung von Software-Updates oder Sicherheits-Patches erforderlich sind oder Instance-Aussonderungen, die im Falle von Hardware-Problemen erforderlich sind. Weitere Informationen finden Sie unter Überwachen Sie den Status Ihrer EC2 Amazon-Instances.	16. November 2011
Spot Instances in Amazon VPC	15.07.2011	Es wurden Informationen über die Unterstützung für Spot-Instances in Amazon VPC hinzugefügt. Mit diesem Update können die Benutzer Spot-Instances in einer Virtual Private Cloud (VPC) starten. Durch Starten von Spot-Instances in einer VPC kommen die Verwender von Spot-Instances in den Genuss der Vorteile von Amazon VPC.	11. Oktober 2011
Vereinfachter VM Import-Prozess für Benutzer von CLI-Tools	15.07.2011	Der VM-Importvorgang wird durch die erweiterte Funktionalität von `ImportInstance` und vereinfacht`ImportVolume` , das nun den Upload der Bilder EC2 nach Amazon durchführt, nachdem die Importaufgabe erstellt wurde. Außerdem können die Benutzer mit der Einführung von `ResumeImport` einen unvollständigen Upload an dem Punkt neu starten, an dem die Aufgabe gestoppt wurde.	15. September 2011

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Unterstützung für den Import in das VHD-Dateiformat		VM Import kann jetzt Image-Dateien virtueller Maschinen im VHD-Format importieren. Das VHD-Dateiformat ist mit den Citrix Xen- und Microsoft Hyper-V-Virtualisierungsplattformen kompatibel. Mit dieser Version unterstützt VM Import jetzt die Bildformate RAW, VHD und VMDK (VMware ESX-kompatibel). Weitere Informationen finden Sie im VM-Benutzerhandbuch. Import/Export	24. August 2011
Update auf den Amazon EC2 VM Import Connector für VMware vCenter		Es wurden Informationen zur 1.1-Version des Amazon EC2 VM Import Connector für die virtuelle VMware vCenter-Appliance (Connector) hinzugefügt. Diese Aktualisierung beinhaltet Proxy-Unterstützung für den Internetzugriff, bessere Fehlerbehandlung, verbesserte Genauigkeit des Aufgaben-Fortschrittsbalkens und verschiedene Fehlerbehebungen.	27. Juni 2011
Preisänderungen bei Spot-Instances in bestimmten Availability Zones	15.05.2011	Es wurden Informationen über das Preise-Feature für Spot-Instances in bestimmten Availability Zones hinzugefügt. In dieser Veröffentlichung haben wir im Rahmen der Informationen, die zurückgegeben werden, wenn Sie Spot-Instance-Anforderungen und den Spot-Preisverlauf abfragen, neue Preisoptionen für Availability Zones hinzugefügt. Diese zusätzlichen Informationen machen es einfacher, den Preis für das Starten einer Spot-Instance in einer bestimmten Availability Zone zu ermitteln.	26. Mai 2011

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
AWS Identity and Access Management		Es wurden Informationen zu AWS Identity and Access Management (IAM) hinzugefügt, mit denen Benutzer angeben können, welche EC2 Amazon-Aktionen ein Benutzer mit EC2 Amazon-Ressourcen im Allgemeinen verwenden kann. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für Amazon EC2.	26. April 2011
Dedicated Instances		Dedicated Instances werden innerhalb Ihrer Amazon Virtual Private Cloud (Amazon VPC) gestartet. Dabei handelt es sich um Instances, die physisch auf Host-Hardware-Ebene isoliert sind. Mit Dedicated Instances können Sie die Vorteile von Amazon VPC und der AWS Cloud nutzen. Zu den Vorteilen gehört die flexible Bereitstellung auf Abruf. Sie zahlen nur für das, was Sie tatsächlich nutzen, während Sie Ihre EC2 Amazon-Compute-Instances auf Hardwareebene isolieren. Weitere Informationen finden Sie unter Amazon-EC2-Dedicated-Instances.	27. März 2011
Updates für Reserved Instances in der Management Console AWS		Aktualisierungen der AWS Management Console erleichtern es Benutzern, ihre Reserved Instances einzusehen und zusätzliche Reserved Instances, einschließlich Dedicated Reserved Instances, zu erwerben.	27. März 2011

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
Metadaten-Informationen	01.01.2011	Es wurden Informationen über Metadaten hinzugefügt, um Änderungen für Version 2011-01-01 zu berücksichtigen. Weitere Informationen erhalten Sie unter Verwenden Sie Instanz-Metadaten, um Ihre EC2 Instanz zu verwalten und Instance-Metadatenkategorien.	11. März 2011
Amazon EC2 VM Import Connector für VMware vCenter		Es wurden Informationen zum Amazon EC2 VM Import Connector für die virtuelle VMware vCenter-Appliance (Connector) hinzugefügt. Der Connector ist ein Plug-in für VMware vCenter, das in den VMware vSphere Client integriert ist und eine grafische Benutzeroberfläche bietet, mit der Sie Ihre VMware virtuellen Maschinen in Amazon importieren können. EC2	3. März 2011
Erzwungene Volume-Trennung		Sie können jetzt den verwenden AWS-Managementkonsole , um die Trennung eines Amazon EBS-Volumes von einer Instance zu erzwingen.	23. Februar 2011
Beendigungsschutz für Instances		Sie können jetzt die AWS Management Console verwenden, um zu verhindern, dass eine Instance beendet wird. Weitere Informationen finden Sie unter Beendigungsschutz für Instances ändern.	23. Februar 2011

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
VM Import	15.11.2010	Es wurden Informationen zum VM Import hinzugefügt, mit dem Sie eine virtuelle Maschine oder ein Volume in Amazon importieren können EC2. Weitere Informationen finden Sie im Import/Export VM-Benutzerhandbuch.	15. Dezember 2010
Grundlegende Überwachung für Instances	31.08.2010	Es wurden Informationen zur grundlegenden Überwachung von EC2 Instanzen hinzugefügt.	12. Dezember 2010
Filter und Tags (Markierungen)	31.08.2010	Es wurden Informationen über das Auflisten, Filtern und Markieren von Ressourcen hinzugefügt. Weitere Informationen erhalten Sie unter Finden Sie Ihre EC2 Amazon-Ressourcen und Kennzeichnen Sie Ihre EC2 Amazon-Ressourcen.	19. September 2010
Idempotenter Instance-Start	31.08.2010	Es wurden Informationen über das Sicherstellen von Idempotenz beim Ausführen von Instances hinzugefügt.	19. September 2010
AWS Identity and Access Management für Amazon EC2		Amazon EC2 ist jetzt in AWS Identity and Access Management (IAM) integriert. Weitere Informationen finden Sie unter Identitäts- und Zugriffsmanagement für Amazon EC2.	2. September 2010
IP-Adressenangabe in Amazon VPC	15.06.2010	Amazon VPC-Benutzer können jetzt die IP-Adresse angeben, um eine Instance zuzuweisen, die in einer VPC gestartet wurde.	12. Juli 2010

Feature	API-Version	Beschreibung	Datum der Veröffentlichung
CloudWatch Amazon-Überwachung für Amazon EBS-Volumes		Die CloudWatch Amazon-Überwachung ist jetzt automatisch für Amazon EBS-Volumes verfügbar.	14. Juni 2010
Reserved Instances mit Windows		Amazon unterstützt EC2 jetzt Reserved Instances mit Windows.	22. Februar 2010

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.