Service Authorization Reference

Service Authorization Reference



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

Service Authorization Reference: Service Authorization Reference

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

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

This documentation is a draft for private preview for regions in the AWS European Sovereign Cloud. Documentation content will continue to evolve. Published: December 30, 2025.

Table of Contents

Reference 1
Actions, resources, and condition keys 1
Actions table 1
Resource types table 2
Condition keys table 3
AWS Account Management 6
Apache Kafka APIs for Amazon MSK clusters 13
AWS AppConfig 20
Amazon Application Recovery Controller - Zonal Shift 38
AWS Artifact 50
AWS Backup 55
AWS Batch 78
Amazon Bedrock 96
AWS Billing And Cost Management Data Exports 157
AWS Budget Service 163
AWS Certificate Manager 169
AWS CloudTrail 176
Amazon CloudWatch 196
Amazon CloudWatch Logs 211
Amazon CloudWatch Synthetics 236
AWS Cost Explorer Service 244
Amazon Data Lifecycle Manager 260
AWS DataSync 265
Amazon EC2 280
Amazon EC2 Auto Scaling 1273
Amazon EC2 Image Builder 1305
Amazon Elastic Block Store 1341
Amazon Elastic Container Registry 1346
Amazon Elastic File System 1359
Amazon Elastic Kubernetes Service 1370
AWS Elastic Load Balancing 1394
AWS Elastic Load Balancing V2 1413
Amazon Elastic MapReduce 1447
Amazon EventBridge 1466

Amazon EventBridge Scheduler 1485
Amazon FSx 1491
AWS Health APIs and Notifications 1516
AWS IAM Identity Center directory 1521
AWS Identity and Access Management (IAM) 1532
AWS Identity and Access Management Roles Anywhere 1573
AWS Identity Store 1580
AWS Key Management Service 1593
Amazon Kinesis Data Streams 1684
Amazon Kinesis Firehose 1697
AWS Lambda 1701
Amazon Managed Streaming for Apache Kafka 1724
AWS Marketplace Discovery 1743
AWS Marketplace Entitlement Service 1745
AWS Marketplace Metering Service 1747
Amazon OpenSearch Service 1750
AWS Organizations 1775
AWS Performance Insights 1794
AWS Price List 1800
AWS Private Certificate Authority 1803
Amazon RDS 1810
AWS Resource Access Manager (RAM) 1883
Amazon Resource Group Tagging API 1903
AWS Resource Groups 1907
Amazon Route 53 1914
Amazon S3 1930
Amazon SageMaker 2141
AWS Savings Plans 2307
AWS Secrets Manager 2312
AWS Security Hub 2351
AWS Security Token Service 2377
Amazon SES 2398
Amazon Simple Email Service - Mail Manager 2416
Amazon Simple Email Service v2 2435
Amazon Simple Workflow Service 2475
Amazon SQS 2493

AWS Step Functions ... 2499
AWS Storage Gateway ... 2510
AWS Support ... 2534
AWS Support Console ... 2541
AWS Transfer Family ... 2546
AWS User Notifications ... 2563
AWS User Notifications Contacts ... 2573
AWS WAF V2 ... 2578
AWS X-Ray ... 2599
Related resources ... 2610
Programmatic access to service reference information ... 2611
Glossary ... 2617
Additional field definitions ... 2617

Reference

The *Service Authorization Reference* provides a list of the actions, resources, and condition keys that are supported by each AWS service. You can specify actions, resources, and condition keys in AWS Identity and Access Management (IAM) policies to manage access to AWS resources.

Contents

- Actions, resources, and condition keys for AWS services
- Related resources

Actions, resources, and condition keys for AWS services

Each AWS service can define actions, resources, and condition context keys for use in IAM policies. This topic describes how the elements provided for each service are documented.

Each topic consists of tables that provide the list of available actions, resources, and condition keys.

The actions table

The **Actions** table lists all the actions that you can use in an IAM policy statement's `Action` element. Not all API operations that are defined by a service can be used as an action in an IAM policy. Some services include permission-only actions that don't directly correspond to an API operation. These actions are indicated with **[permission only]**. Use this list to determine which actions you can use in an IAM policy. For more information about the `Action`, `Resource`, or `Condition` elements, see IAM JSON policy elements reference. The **Actions** and **Description** table columns are self-descriptive.

- The **Access level** column describes how the action is classified (List, Read, Write, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Understanding access level summaries within policy summaries.
- The **Resource types** column indicates whether the action supports resource-level permissions. If the column is empty, then the action does not support resource-level permissions and you must specify all resources ("*") in your policy. If the column includes a resource type, then you can specify the resource ARN in the `Resource` element of your policy. For more information about that resource, refer to that row in the **Resource types** table. All actions and resources that are

included in one statement must be compatible with each other. If you specify a resource that is not valid for the action, any request to use that action fails, and the statement's `Effect` does not apply.

Required resources are indicated in the table with an asterisk (*). If you specify a resource-level permission ARN in a statement using this action, then it must be of this type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one but not the other.

- The **Condition keys** column includes keys that you can specify in a policy statement's `Condition` element. Condition keys might be supported with an action, or with an action and a specific resource. Pay close attention to whether the key is in the same row as a specific resource type. This table does not include global condition keys that are available for any action or under unrelated circumstances. For more information about global condition keys, see AWS global condition context keys.
- The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

  Dependent actions are not required in all scenarios. Refer to the individual service's documentation for more information about providing granular permissions to users.

The resource types table

The **Resource types** table lists all the resource types that you can specify as an ARN in the `Resource` policy element. Not every resource type can be specified with every action. Some resource types work with only certain actions. If you specify a resource type in a statement with an action that does not support that resource type, then the statement doesn't allow access. For more information about the `Resource` element, see IAM JSON policy elements: Resource.

- The **ARN** column specifies the Amazon Resource Name (ARN) format that you must use to reference resources of this type. The portions that are preceded by a $ must be replaced by the actual values for your scenario. For example, if you see `$user-name` in an ARN, you must replace that string with either the actual user's name or a policy variable that contains a user's name. For more information about ARNs, see IAM ARNs.

- The **Condition keys** column specifies condition context keys that you can include in an IAM policy statement only when both this resource and a supporting action from the table above are included in the statement.

The condition keys table

The **condition keys** table lists all of the condition context keys that you can use in an IAM policy statement's `Condition` element. Not every key can be specified with every action or resource. Certain keys only work with certain types of actions and resources. For more information about the `Condition` element, see IAM JSON policy elements: Condition.

- The **Type** column specifies the data type of the condition key. This data type determines which condition operators you can use to compare values in the request with the values in the policy statement. You must use an operator that is appropriate for the data type. If you use an incorrect operator, then the match always fails and the policy statement never applies.

  If the **Type** column specifies a "List of …" one of the simple types, then you can use multiple keys and values in your policies. Do this using condition set prefixes with your operators. Use the `ForAllValues` prefix to specify that **all** values in the request must match a value in the policy statement. Use the `ForAnyValue` prefix to specify that **at least one** value in the request matches one of the values in the policy statement.

Topics

- Actions, resources, and condition keys for AWS Account Management
- Actions, resources, and condition keys for Apache Kafka APIs for Amazon MSK clusters
- Actions, resources, and condition keys for AWS AppConfig
- Actions, resources, and condition keys for Amazon Application Recovery Controller - Zonal Shift
- Actions, resources, and condition keys for AWS Artifact
- Actions, resources, and condition keys for AWS Backup
- Actions, resources, and condition keys for AWS Batch
- Actions, resources, and condition keys for Amazon Bedrock
- Actions, resources, and condition keys for AWS Billing And Cost Management Data Exports
- Actions, resources, and condition keys for AWS Budget Service
- Actions, resources, and condition keys for AWS Certificate Manager

- Actions, resources, and condition keys for AWS CloudTrail
- Actions, resources, and condition keys for Amazon CloudWatch
- Actions, resources, and condition keys for Amazon CloudWatch Logs
- Actions, resources, and condition keys for Amazon CloudWatch Synthetics
- Actions, resources, and condition keys for AWS Cost Explorer Service
- Actions, resources, and condition keys for Amazon Data Lifecycle Manager
- Actions, resources, and condition keys for AWS DataSync
- Actions, resources, and condition keys for Amazon EC2
- Actions, resources, and condition keys for Amazon EC2 Auto Scaling
- Actions, resources, and condition keys for Amazon EC2 Image Builder
- Actions, resources, and condition keys for Amazon Elastic Block Store
- Actions, resources, and condition keys for Amazon Elastic Container Registry
- Actions, resources, and condition keys for Amazon Elastic File System
- Actions, resources, and condition keys for Amazon Elastic Kubernetes Service
- Actions, resources, and condition keys for AWS Elastic Load Balancing
- Actions, resources, and condition keys for AWS Elastic Load Balancing V2
- Actions, resources, and condition keys for Amazon Elastic MapReduce
- Actions, resources, and condition keys for Amazon EventBridge
- Actions, resources, and condition keys for Amazon EventBridge Scheduler
- Actions, resources, and condition keys for Amazon FSx
- Actions, resources, and condition keys for AWS Health APIs and Notifications
- Actions, resources, and condition keys for AWS IAM Identity Center directory
- Actions, resources, and condition keys for AWS Identity and Access Management (IAM)
- Actions, resources, and condition keys for AWS Identity and Access Management Roles Anywhere
- Actions, resources, and condition keys for AWS Identity Store
- Actions, resources, and condition keys for AWS Key Management Service
- Actions, resources, and condition keys for Amazon Kinesis Data Streams
- Actions, resources, and condition keys for Amazon Kinesis Firehose
- Actions, resources, and condition keys for AWS Lambda
- Actions, resources, and condition keys for Amazon Managed Streaming for Apache Kafka

- Actions, resources, and condition keys for AWS Marketplace Discovery
- Actions, resources, and condition keys for AWS Marketplace Entitlement Service
- Actions, resources, and condition keys for AWS Marketplace Metering Service
- Actions, resources, and condition keys for Amazon OpenSearch Service
- Actions, resources, and condition keys for AWS Organizations
- Actions, resources, and condition keys for AWS Performance Insights
- Actions, resources, and condition keys for AWS Price List
- Actions, resources, and condition keys for AWS Private Certificate Authority
- Actions, resources, and condition keys for Amazon RDS
- Actions, resources, and condition keys for AWS Resource Access Manager (RAM)
- Actions, resources, and condition keys for Amazon Resource Group Tagging API
- Actions, resources, and condition keys for AWS Resource Groups
- Actions, resources, and condition keys for Amazon Route 53
- Actions, resources, and condition keys for Amazon S3
- Actions, resources, and condition keys for Amazon SageMaker
- Actions, resources, and condition keys for AWS Savings Plans
- Actions, resources, and condition keys for AWS Secrets Manager
- Actions, resources, and condition keys for AWS Security Hub
- Actions, resources, and condition keys for AWS Security Token Service
- Actions, resources, and condition keys for Amazon SES
- Actions, resources, and condition keys for Amazon Simple Email Service - Mail Manager
- Actions, resources, and condition keys for Amazon Simple Email Service v2
- Actions, resources, and condition keys for Amazon Simple Workflow Service
- Actions, resources, and condition keys for Amazon SQS
- Actions, resources, and condition keys for AWS Step Functions
- Actions, resources, and condition keys for AWS Storage Gateway
- Actions, resources, and condition keys for AWS Support
- Actions, resources, and condition keys for AWS Support Console
- Actions, resources, and condition keys for AWS Transfer Family
- Actions, resources, and condition keys for AWS User Notifications

- Actions, resources, and condition keys for AWS User Notifications Contacts
- Actions, resources, and condition keys for AWS WAF V2
- Actions, resources, and condition keys for AWS X-Ray

Actions, resources, and condition keys for AWS Account Management

AWS Account Management (service prefix: `account`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Account Management
- Resource types defined by AWS Account Management
- Condition keys for AWS Account Management

Actions defined by AWS Account Management

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a

resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptPrimaryEmailUpdate	Grants permission to accept the process to update the primary email address of an account	Write	accountInOrganization		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				account:EmailTargetDomain	
CloseAccount [permission only]	Grants permission to close an account	Write	account		
DeleteAlternateContact	Grants permission to delete the alternate contacts for an account	Write	account		
			accountInOrganization		
				account:AlternateContactTypes	
DisableRegion	Grants permission to disable use of a Region	Write	account		
			accountInOrganization		
				account:TargetRegion	
EnableRegion	Grants permission to enable use of a Region	Write	account		
			accountInOrganization		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				account:TargetRegion	
GetAccountInformation	Grants permission to retrieve the account information for an account	Read	account		
			accountInOrganization		
GetAlternateContact	Grants permission to retrieve the alternate contacts for an account	Read	account		
			accountInOrganization		
				account:AlternateContactTypes	
GetContactInformation	Grants permission to retrieve the primary contact information for an account	Read	account		
			accountInOrganization		
GetGovCloudAccountInformation	Grants permission to retrieve the linked GovCloud account information for an account	Read	account		
			accountInOrganization		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPrimaryEmail	Grants permission to retrieve the primary email address of an account	Read	accountInOrganization		
GetRegionOptStatus	Grants permission to get the opt-in status of a Region	Read	account		
			accountInOrganization		
				account:TargetRegion	
ListRegions	Grants permission to list the available Regions	List	account		
			accountInOrganization		
PutAccountName	Grants permission to update the name for an account	Write	account		
			accountInOrganization		
PutAlternateContact	Grants permission to modify the alternate contacts for an account	Write	account		
			accountInOrganization		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				account:AlternateContactTypes	
PutContactInformation	Grants permission to update the primary contact information for an account	Write	account		
			accountInOrganization		
StartPrimaryEmailUpdate	Grants permission to start the process to update the primary email address of an account	Write	accountInOrganization		
				account:EmailTargetDomain	

Resource types defined by AWS Account Management

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
account	`arn:${Partition}:account::${Account}:account`	

Resource types	ARN	Condition keys
accountInOrganization	`arn:${Partition}:account::${ManagementAccountId}:account/o-${OrganizationId}/${MemberAccountId}`	

Condition keys for AWS Account Management

AWS Account Management defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
account:AccountResourceOrgPaths	Filters access by the resource path for an account in an organization	ArrayOfString
account:AccountResourceOrgTags/${TagKey}	Filters access by resource tags for an account in an organization	String
account:AlternateContactTypes	Filters access by alternate contact types	ArrayOfString
account:EmailTargetDomain	Filters access by email domain of the target email address	String

Condition keys	Description	Type
account:TargetRegion	Filters access by a list of Regions. Enables or disables all the Regions specified here	String

Actions, resources, and condition keys for Apache Kafka APIs for Amazon MSK clusters

Apache Kafka APIs for Amazon MSK clusters (service prefix: `kafka-cluster`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Apache Kafka APIs for Amazon MSK clusters
- Resource types defined by Apache Kafka APIs for Amazon MSK clusters
- Condition keys for Apache Kafka APIs for Amazon MSK clusters

Actions defined by Apache Kafka APIs for Amazon MSK clusters

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AlterCluster	Grants permission to alter various aspects of the cluster, equivalent to Apache Kafka's ALTER CLUSTER ACL	Write	cluster*		kafka-cluster:Connect kafka-cluster:DescribeCluster
AlterClusterDynamicConfiguration	Grants permission to alter the dynamic configuration of a cluster, equivalent to Apache Kafka's ALTER_CONFIGS CLUSTER ACL	Write	cluster*		kafka-cluster:Connect kafka-cluster:DescribeClusterDynamicConfiguration
AlterGroup	Grants permission to join groups on a cluster, equivalent to Apache Kafka's READ GROUP ACL	Write	group*		kafka-cluster:Connect kafka-cluster:DescribeGroup
AlterTopic	Grants permission to alter topics on a cluster, equivalent to Apache Kafka's ALTER TOPIC ACL	Write	topic*		kafka-cluster:Connect

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					kafka-cluster:DescribeTopic
AlterTopicDynamicConfiguration	Grants permission to alter the dynamic configuration of topics on a cluster, equivalent to Apache Kafka's ALTER_CONFIGS TOPIC ACL	Write	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopicDynamicConfiguration
AlterTransactionalId	Grants permission to alter transactional IDs on a cluster, equivalent to Apache Kafka's WRITE TRANSACTIONAL_ID ACL	Write	transactional-id*		kafka-cluster:Connect kafka-cluster:DescribeTransactionalId kafka-cluster:WriteData
Connect	Grants permission to connect and authenticate to the cluster	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTopic	Grants permission to create topics on a cluster, equivalent to Apache Kafka's CREATE CLUSTER/TOPIC ACL	Write	topic*		kafka-cluster:Connect
DeleteGroup	Grants permission to delete groups on a cluster, equivalent to Apache Kafka's DELETE GROUP ACL	Write	group*		kafka-cluster:Connect kafka-cluster:DescribeGroup
DeleteTopic	Grants permission to delete topics on a cluster, equivalent to Apache Kafka's DELETE TOPIC ACL	Write	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic
DescribeCluster	Grants permission to describe various aspects of the cluster, equivalent to Apache Kafka's DESCRIBE CLUSTER ACL	List	cluster*		kafka-cluster:Connect
DescribeClusterDynamicConfiguration	Grants permission to describe the dynamic configuration of a cluster, equivalent to Apache Kafka's DESCRIBE_CONFIGS CLUSTER ACL	List	cluster*		kafka-cluster:Connect

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeGroup	Grants permission to describe groups on a cluster, equivalent to Apache Kafka's DESCRIBE GROUP ACL	List	group*		kafka-cluster:Connect
DescribeTopic	Grants permission to describe topics on a cluster, equivalent to Apache Kafka's DESCRIBE TOPIC ACL	List	topic*		kafka-cluster:Connect
DescribeTopicDynamicConfiguration	Grants permission to describe the dynamic configuration of topics on a cluster, equivalent to Apache Kafka's DESCRIBE_CONFIGS TOPIC ACL	List	topic*		kafka-cluster:Connect
DescribeTransactionalId	Grants permission to describe transactional IDs on a cluster, equivalent to Apache Kafka's DESCRIBE TRANSACTIONAL_ID ACL	List	transactional-id*		kafka-cluster:Connect
ReadData	Grants permission to read data from topics on a cluster, equivalent to Apache Kafka's READ TOPIC ACL	Read	topic*		kafka-cluster:AlterGroup kafka-cluster:Connect kafka-cluster:DescribeTopic

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
WriteData	Grants permission to write data to topics on a cluster, equivalent to Apache Kafka's WRITE TOPIC ACL	Write	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic
WriteDataIdempotently	Grants permission to write data idempotently on a cluster, equivalent to Apache Kafka's IDEMPOTENT_WRITE CLUSTER ACL	Write	cluster*		kafka-cluster:Connect kafka-cluster:WriteData

Resource types defined by Apache Kafka APIs for Amazon MSK clusters

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
cluster	`arn:${Partition}:kafka:${Region}:${Account}:cluster/${ClusterName}/${ClusterUuid}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
topic	arn:${Partition}:kafka:${Region}:${Account}:topic/${ClusterName}/${ClusterUuid}/${TopicName}	
group	arn:${Partition}:kafka:${Region}:${Account}:group/${ClusterName}/${ClusterUuid}/${GroupName}	
transactional-id	arn:${Partition}:kafka:${Region}:${Account}:transactional-id/${ClusterName}/${ClusterUuid}/${TransactionalId}	

Condition keys for Apache Kafka APIs for Amazon MSK clusters

Apache Kafka APIs for Amazon MSK clusters defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters actions based on tag key-value pairs attached to the resource. The resource tag context key will only apply to the cluster resource, not topics, groups and transactional IDs	String

Actions, resources, and condition keys for AWS AppConfig

AWS AppConfig (service prefix: `appconfig`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS AppConfig
- Resource types defined by AWS AppConfig
- Condition keys for AWS AppConfig

Actions defined by AWS AppConfig

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateApplication	Grants permission to create an application	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationProfile	Grants permission to create a configuration profile	Write	application*		
				aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
CreateDeploymentStrategy	Grants permission to create a deployment strategy	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	Grants permission to create an environment	Write	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateExtension	Grants permission to create an extension	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateExtensionAssociation	Grants permission to create an extension association	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateHostedConfigurationVersion	Grants permission to create a hosted configuration version	Write	application*		
			configurationprofile*		
DeleteApplication	Grants permission to delete an application	Write	application*		
DeleteConfigurationProfile	Grants permission to delete a configuration profile	Write	application*		
			configurationprofile*		
DeleteDeploymentStrategy	Grants permission to delete a deployment strategy	Write	deploymentstrategy*		
DeleteEnvironment	Grants permission to delete an environment	Write	application*		
			environment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteExtension	Grants permission to delete an extension	Write	extension*		
DeleteExtensionAssociation	Grants permission to delete an extension association	Write	extensionassociation*		
DeleteHostedConfigurationVersion	Grants permission to delete a hosted configuration version	Write	application*		
			configurationprofile*		
			hostedconfigurationversion*		
GetAccountSettings	Grants permission to view account-wide AppConfig settings	Read			
GetApplication	Grants permission to view details about an application	Read	application*		
				aws:ResourceTag/${TagKey}	
GetConfiguration	Grants permission to view details about a configuration	Read	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			configurationprofile*		
			environment*		
				aws:ResourceTag/${TagKey}	
GetConfigurationProfile	Grants permission to view details about a configuration profile	Read	application*		
			configurationprofile*		
				aws:ResourceTag/${TagKey}	
GetDeployment	Grants permission to view details about a deployment	Read	application*		
			deployment*		
			environment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetDeploymentStrategy	Grants permission to view details about a deployment strategy	Read	deploymentstrategy*		
				aws:ResourceTag/${TagKey}	
GetEnvironment	Grants permission to view details about an environment	Read	application*		
			environment*		
				aws:ResourceTag/${TagKey}	
GetExtension	Grants permission to view details about an extension	Read	extension*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetExtensionAssociation	Grants permission to view details about an extension association	Read	extensionassociation*		
				aws:ResourceTag/${TagKey}	
GetHostedConfigurationVersion	Grants permission to view details about a hosted configuration version	Read	application*		
			configurationprofile*		
			hostedconfigurationversion*		
GetLatestConfiguration	Grants permission to retrieve a deployed configuration	Read	configuration*		
				aws:ResourceTag/${TagKey}	
ListApplications	Grants permission to list the applications in your account	List			
ListConfigurationProfiles	Grants permission to list the configuration profiles for an application	List	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDeploymentStrategies	Grants permission to list the deployment strategies for your account	List			
ListDeployments	Grants permission to list the deployments for an environment	List	application*		
			environment*		
ListEnvironments	Grants permission to list the environments for an application	List	application*		
ListExtensionAssociations	Grants permission to list the extension associations in your account	List			
ListExtensions	Grants permission to list the extensions in your account	List			
ListHostedConfigurationVersions	Grants permission to list the hosted configuration versions for a configuration profile	List	application*		
			configurationprofile*		
ListTagsForResource	Grants permission to view a list of resource tags for a specified resource	Read	application		
			configurationprofile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			deployment		
			deploymentstrategy		
			environment		
			extension		
			extensionassociation		
				aws:ResourceTag/${TagKey}	
StartConfigurationSession	Grants permission to start a configuration session	Write	configuration*		
				aws:ResourceTag/${TagKey}	
StartDeployment	Grants permission to initiate a deployment	Write	application*		
			configurationprofile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			deploymentstrategy*		
			environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StopDeployment	Grants permission to stop a deployment	Write	application*		
			deployment*		
			environment*		
TagResource	Grants permission to tag an appconfig resource	Tagging	application		
			configuration		
			configurationprofile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			deployment		
			deploymentstrategy		
			environment		
			extension		
			extensionassociation		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag an appconfig resource	Tagging	application		
			configuration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			configurationprofile		
			deployment		
			deploymentstrategy		
			environment		
			extension		
			extensionassociation		
				aws:TagKeys	
UpdateAccountSettings	Grants permission to modify account-wide AppConfig settings	Write			
UpdateApplication	Grants permission to modify an application	Write	application*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateConfigurationProfile	Grants permission to modify a configuration profile	Write	application*		
			configurationprofile*		
				aws:ResourceTag/${TagKey}	
UpdateDeploymentStrategy	Grants permission to modify a deployment strategy	Write	deploymentstrategy*		
				aws:ResourceTag/${TagKey}	
UpdateEnvironment	Grants permission to modify an environment	Write	application*		
			environment*		
				aws:ResourceTag/${TagKey}	
UpdateExtension	Grants permission to modify an extension	Write	extension*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
UpdateExtensionAssociation	Grants permission to modify an extension association	Write	extensionassociation*		
				aws:ResourceTag/${TagKey}	
ValidateConfiguration	Grants permission to validate a configuration	Write	application*		
			configurationprofile*		

Resource types defined by AWS AppConfig

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
application	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}	aws:ResourceTag/${TagKey}
environment	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}	aws:ResourceTag/${TagKey}
configurationprofile	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/configurationprofile/${ConfigurationProfileId}	aws:ResourceTag/${TagKey}
deploymentstrategy	arn:${Partition}:appconfig:${Region}:${Account}:deploymentstrategy/${DeploymentStrategyId}	aws:ResourceTag/${TagKey}
deployment	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}/deployment/${DeploymentNumber}	aws:ResourceTag/${TagKey}
hostedconfigurationversion	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/configurationprofile/${ConfigurationProfileId}/hostedconfigurationversion/${VersionNumber}	
configuration	arn:${Partition}:appconfig:${Region}:${Account}:application/${ApplicationId}/environment/${EnvironmentId}/configuration/${ConfigurationProfileId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
extension	arn:${Partition}:appconfig:${Region}:${Account}:extension/${ExtensionId}/${ExtensionVersionNumber}	aws:ResourceTag/${TagKey}
extension association	arn:${Partition}:appconfig:${Region}:${Account}:extensionassociation/${ExtensionAssociationId}	aws:ResourceTag/${TagKey}

Condition keys for AWS AppConfig

AWS AppConfig defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for a specified tag	String
aws:ResourceTag/${TagKey}	Filters access by a tag key-value pair assigned to the AWS resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Application Recovery Controller - Zonal Shift

Amazon Application Recovery Controller - Zonal Shift (service prefix: `arc-zonal-shift`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Application Recovery Controller - Zonal Shift
- Resource types defined by Amazon Application Recovery Controller - Zonal Shift
- Condition keys for Amazon Application Recovery Controller - Zonal Shift

Actions defined by Amazon Application Recovery Controller - Zonal Shift

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit

resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelPracticeRun	Grants permission to cancel an active practice run	Write	ALB*		
			NLB*		
				arc-zonal-shift:ResourceIdentifier	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CancelZonalShift	Grants permission to cancel an active zonal shift	Write	ALB*		
			NLB*		
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePracticeRunConfiguration	Grants permission to create a practice run configuration	Write	ALB*		cloudwatch:DescribeAlarms iam:CreateServiceLinkedRole
			NLB*		
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeletePracticeRunConfiguration	Grants permission to delete a practice run configuration	Write	ALB*		
			NLB*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetAutoshiftObserverNotificationStatus	Grants permission to get autoshift observer notification status	Read			
GetManagedResource	Grants permission to get information about a managed resource	Read	ALB* NLB*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ListAutoshifts	Grants permission to list active and completed autoshifts	List			
ListManagedResources	Grants permission to list managed resources	List			
ListZonalShifts	Grants permission to list zonal shifts	List			
StartPracticeRun	Grants permission to start a practice run	Write	ALB* NLB*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
StartZonalShift	Grants permission to start a zonal shift	Write	ALB*		
			NLB*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateAutoshiftObserverNotificationStatus	Grants permission to update autoshift observer notification status	Write			
UpdatePracticeRunConfiguration	Grants permission to update a practice run configuration	Write	ALB*		cloudwatch:DescribeAlarms iam:CreateServiceLinkedRole
			NLB*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateZonalAutoshiftConfiguration	Grants permission to update a zonal autoshift status	Write	ALB*		iam:CreateServiceLinkedRole
			NLB*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
UpdateZonalShift	Grants permission to update an existing zonal shift	Write	ALB*		
			NLB*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Resource types defined by Amazon Application Recovery Controller - Zonal Shift

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
ALB	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}`	arc-zonal-shift:ResourceIdentifier

Resource types	ARN	Condition keys
		aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
NLB	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/net/${LoadBalancerName}/${LoadBalancerId}	arc-zonal-shift:ResourceIdentifier aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Condition keys for Amazon Application Recovery Controller - Zonal Shift

Amazon Application Recovery Controller - Zonal Shift defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
arc-zonal-shift:ResourceIdentifier	Filters access by the resource identifier of the managed resource	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the managed resource	String
elasticloadbalancing:ResourceTag/${TagKey}	Filters access by the tags associated with the managed resource	String

Actions, resources, and condition keys for AWS Artifact

AWS Artifact (service prefix: `artifact`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Artifact
- Resource types defined by AWS Artifact
- Condition keys for AWS Artifact

Actions defined by AWS Artifact

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptAgreement	Grants permission to accept an AWS agreement that has not yet been accepted by the customer account	Write	agreement*		
AcceptNdaForAgreement	Grants permission to accept the terms of an NDA Document for a given agreement resource	Write	agreement*		
GetAccountSettings	Grants permission to get the account settings for Artifact	Read			
GetAgreement	Grants permission to get an AWS agreement that has not yet been accepted by the customer account	Read	agreement*		
GetCustomerAgreement	Grants permission to get an AWS agreement that has been accepted by the customer account	Read	customer-agreement*		
GetNdaForAgreement	Grants permission to retrieve the NDA Document for a given agreement resource	Read	agreement*		
GetReport	Grants permission to download a report	Read	report*		
GetReportMetadata	Grants permission to download metadata associated with a report	Read	report*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTermForReport	Grants permission to download a term associated with a report	Read	report*		
ListAgreements	Grants permission to list AWS agreements	List			
ListCustomerAgreements	Grants permission to list customer-agreement resources that have been accepted by the customer account	List			
ListReportVersions	Grants permission to list report versions in your account	List			
ListReports	Grants permission to list reports in your account	List			
PutAccountSettings	Grants permission to put account settings for Artifact	Write			
TerminateAgreement	Grants permission to terminate a customer agreement that was previously accepted by the customer account	Write	customer-agreement*		

Resource types defined by AWS Artifact

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types

that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
customer-agreement	`arn:${Partition}:artifact::${Account}:customer-agreement/*`	
agreement	`arn:${Partition}:artifact:::agreement/*`	
report	`arn:${Partition}:artifact:${Region}::report/${ReportId}:${Version}`	artifact:ReportCategory artifact:ReportSeries

Condition keys for AWS Artifact

AWS Artifact defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
artifact:ReportCategory	Filters access by which category reports are associated with	String
artifact:ReportSeries	Filters access by which series reports are associated with	String

Actions, resources, and condition keys for AWS Backup

AWS Backup (service prefix: `backup`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Backup
- Resource types defined by AWS Backup
- Condition keys for AWS Backup

Actions defined by AWS Backup

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateBackupVaultMpaApprovalTeam	Grants permission to associate an MPA approval team with a backup vault	Write	backupVault*		
				backup:MpaApprovalTeamArn	
CancelLegalHold	Grants permission to cancel a legal hold	Write	legalHold*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CopyFromBackupVault [permission only]	Grants permission to copy from a backup vault	Write	recoveryPoint*		
				backup:CopyTargets backup:CopyTargetOrgPaths	
CopyIntoBackupVault [permission only]	Grants permission to copy into a backup vault	Write	backupVault*		
				aws:RequestTag/${TagKey}	
CreateBackupAccessPoint [permission only]	Grants permission to create a new access point for backup instant access	Write	recoveryPoint*		
CreateBackupPlan	Grants permission to create a new backup plan	Write	backupPlan*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBackupSelection	Grants permission to create a new resource assignment in a backup plan	Write	backupPlan*		iam:PassRole
CreateBackupVault	Grants permission to create a new backup vault	Write	backupVault*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFramework	Grants permission to create a new framework	Write	framework*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLegalHold	Grants permission to create a new legal hold	Write	legalHold*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLogicallyAirGappedBackupVault	Grants permission to create a new logically air-gapped backup vault, a logical container where backups are stored	Write	backupVault*		
				aws:RequestTag/${TagKey} aws:TagKeys backup:MinRetentionDays backup:MaxRetentionDays	
CreateReportPlan	Grants permission to create a new report plan	Write	reportPlan*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys backup:FrameworkArns	
CreateRestoreAccessBackupVault	Grants permission to create a restore access backup vault	Write	backupVault*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRestoreTestingPlan	Grants permission to create a new restore testing plan	Write	restoreTestingPlan*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRestoreTestingSelection	Grants permission to create a new resource assignment in a restore testing plan	Write	restoreTestingPlan*		iam:PassRole
CreateTieringConfiguration	Grants permission to create a new tiering configuration	Write	tieringConfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBackupAccessPoint [permission only]	Grants permission to delete the access point	Write			
DeleteBackupPlan	Grants permission to delete a backup plan	Write	backupPlan*		
DeleteBackupSelection	Grants permission to delete a resource assignment from a backup plan	Write	backupPlan*		
DeleteBackupVault	Grants permission to delete a backup vault	Write	backupVault*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBackupVaultAccessPolicy	Grants permission to delete backup vault access policy	Permissions management	backupVault*		
DeleteBackupVaultLockConfiguration	Grants permission to remove the lock configuration from a backup vault	Write	backupVault*		
DeleteBackupVaultNotifications	Grants permission to remove the notifications from a backup vault	Write	backupVault*		
DeleteBackupVaultSharingPolicy [permission only]	Grants permission to delete backup vault sharing policy	Permissions management	backupVault*		
DeleteFramework	Grants permission to delete a framework	Write	framework*		
DeleteRecoveryPoint	Grants permission to delete a recovery point from a backup vault	Write	recoveryPoint*		
DeleteReportPlan	Grants permission to delete a report plan	Write	reportPlan*		
DeleteRestoreTestingPlan	Grants permission to delete a restore testing plan	Write	restoreTestingPlan*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRestoreTestingSelection	Grants permission to delete a resource assignment from a restore testing plan	Write	restoreTestingPlan*		
DeleteTieringConfiguration	Grants permission to delete a tiering configuration	Write	tieringConfiguration*		
DescribeBackupAccessPoint [permission only]	Grants permission to return information about the specified access point	Read			
DescribeBackupJob	Grants permission to describe a backup job	Read			
DescribeBackupVault	Grants permission to describe a new backup vault with the specified name	Read	backupVault*		
DescribeCopyJob	Grants permission to describe a copy job	Read			
DescribeFramework	Grants permission to describe a framework with the specified name	Read	framework*		
DescribeGlobalSettings	Grants permission to describe global settings	Read			
DescribeProtectedResource	Grants permission to describe a protected resource	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeRecoveryPoint	Grants permission to describe a recovery point	Read	recoveryPoint*		
DescribeRegionSettings	Grants permission to describe region settings	Read			
DescribeReportJob	Grants permission to describe a report job	Read			
DescribeReportPlan	Grants permission to describe a report plan with the specified name	Read	reportPlan*		
DescribeRestoreJob	Grants permission to describe a restore job	Read			
DescribeScanJob	Grants permission to describe a scan job	Read			
DisassociateBackupVaultMpaApprovalTeam	Grants permission to disassociate an MPA approval team from a backup vault	Write	backupVault*		
DisassociateRecoveryPoint	Grants permission to disassociate a recovery point from a backup vault	Write	recoveryPoint*		
DisassociateRecoveryPointFromParent	Grants permission to disassociate a recovery point from its parent	Write	recoveryPoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExportBackupPlanTemplate	Grants permission to export a backup plan as a JSON	Read			
GetBackupPlan	Grants permission to get a backup plan	Read	backupPlan*		
GetBackupPlanFromJSON	Grants permission to transform a JSON to a backup plan	Read			
GetBackupPlanFromTemplate	Grants permission to transform a template to a backup plan	Read			
GetBackupSelection	Grants permission to get a backup plan resource assignment	Read	backupPlan*		
GetBackupVaultAccessPolicy	Grants permission to get backup vault access policy	Read	backupVault*		
GetBackupVaultNotifications	Grants permission to get backup vault notifications	Read	backupVault*		
GetBackupVaultSharingPolicy [permission only]	Grants permission to get backup vault sharing policy	Read	backupVault*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLegalHold	Grants permission to get a legal hold	Read	legalHold*		
GetRecoveryPointIndexDetails	Grants permission to get indexing details for a recovery point	Read	recoveryPoint*		
GetRecoveryPointRestoreMetadata	Grants permission to get recovery point restore metadata	Read	recoveryPoint*		
GetRestoreJobMetadata	Grants permission to get the restore metadata associated with a restore job	Read			
GetRestoreTestingInferredMetadata	Grants permission to get inferred metadata generated by restore testing	Read			
GetRestoreTestingPlan	Grants permission to get a restore testing plan	Read	restoreTestingPlan*		
GetRestoreTestingSelection	Grants permission to get a restore testing plan resource assignment	Read	restoreTestingPlan*		
GetSupportedResourceTypes	Grants permission to get supported resource types	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTieringConfiguration	Grants permission to describe a tiering configuration	Read	tieringConfiguration*		
ListBackupJobSummaries	Grants permission to list backup job summaries	List			
ListBackupJobs	Grants permission to list backup jobs	List			
ListBackupPlanTemplates	Grants permission to list backup plan templates provided by AWS Backup	List			
ListBackupPlanVersions	Grants permission to list backup plan versions	List	backupPlan*		
ListBackupPlans	Grants permission to list backup plans	List			
ListBackupSelections	Grants permission to list resource assignments for a specific backup plan	List	backupPlan*		
ListBackupVaults	Grants permission to list backup vaults	List			
ListCopyJobSummaries	Grants permission to list copy job summaries	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCopyJobs	Grants permission to list copy jobs	List			
ListFrameworks	Grants permission to list frameworks	List			
ListIndexedRecoveryPoints	Grants permission to get list indexed recovery points	List			
ListIndexedRecoveryPointsForSearch [permission only]	Grants permission to list indexed recovery points to search	Permissions management			
ListLegalHolds	Grants permission to list legal holds	List			
ListProtectedResources	Grants permission to list protected resources by AWS Backup	List			
ListProtectedResourcesByBackupVault	Grants permission to list protected resources inside a backup vault	List	backupVault*		
ListRecoveryPointsByBackupVault	Grants permission to list recovery points inside a backup vault	List	backupVault*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRecoveryPointsByLegalHold	Grants permission to list recovery points by legal hold	List	legalHold*		
ListRecoveryPointsByResource	Grants permission to list recovery points for a resource	List			
ListReportJobs	Grants permission to list report jobs	List			
ListReportPlans	Grants permission to list report plans	List			
ListRestoreAccessBackupVaults	Grants permission to list a restore access backup vaults associated with a backup vault	List	backupVault*		
ListRestoreJobSummaries	Grants permission to list restore job summaries	List			
ListRestoreJobs	Grants permission to list restore jobs	List			
ListRestoreJobsByProtectedResource	Grants permission to list restore jobs for a protected resource	List			
ListRestoreTestingPlans	Grants permission to list restore testing plans	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRestoreTestingSelections	Grants permission to list resource assignments for a specific restore testing plan	List	restoreTestingPlan*		
ListScanJobSummaries	Grants permission to list scan job summaries	List			
ListScanJobs	Grants permission to list scan jobs	List			
ListTags	Grants permission to list tags for a resource	Read	backupPlan		
			backupVault		
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		
			tieringConfiguration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTieringConfigurations	Grants permission to list tiering configurations	List			
PutBackupVaultAccessPolicy	Grants permission to add an access policy to the backup vault	Permissions management	backupVault*		
PutBackupVaultLockConfiguration	Grants permission to add a lock configuration to the backup vault	Write	backupVault*		
				backup:ChangeableForDays backup:MinRetentionDays backup:MaxRetentionDays	
PutBackupVaultNotifications	Grants permission to add an SNS topic to the backup vault	Write	backupVault*		
PutBackupVaultSharingPolicy [permission only]	Grants permission to add a sharing policy to the backup vault	Permissions management	backupVault*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutRestoreValidationResult	Grants permission to put a restore validation result	Write			
RevokeRestoreAccessBackupVault	Grants permission to revoke a restore access backup vault	Write	backupVault*		
SearchRecoveryPoint [permission only]	Grants permission to search a recovery point	Permissions management	recoveryPoint*		
StartBackupJob	Grants permission to start a new backup job	Write	backupVault*		iam:PassRole
StartCopyJob	Grants permission to copy a backup from a source backup vault to a destination backup vault	Write	recoveryPoint*		iam:PassRole
StartReportJob	Grants permission to start a new report job	Write	reportPlan*		
StartRestoreJob	Grants permission to start a new restore job	Write	recoveryPoint*		iam:PassRole
StartScanJob	Grants permission to start a new scan job	Write	recoveryPoint*		iam:PassRole
StopBackupJob	Grants permission to stop a backup job	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag a resource	Tagging	backupPlan		
			backupVault		
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		
			tieringConfiguration		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	backupPlan		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			backupVault		
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		
			tieringConfiguration		
				aws:TagKeys	
UpdateBackupPlan	Grants permission to update a backup plan	Write	backupPlan*		iam:PassRole
UpdateFramework	Grants permission to update a framework	Write	framework*		
UpdateGlobalSettings	Grants permission to update the current global settings for the AWS Account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRecoveryPointIndexSettings	Grants permission to update recovery point index settings	Write	recoveryPoint*		
				backup:Index	
UpdateRecoveryPointLifecycle	Grants permission to update the lifecycle of the recovery point	Write	recoveryPoint*		
UpdateRegionSettings	Grants permission to update the current service opt-in settings for the Region	Write			
UpdateReportPlan	Grants permission to update a report plan	Write	reportPlan*		
				backup:FrameworkArns	
UpdateRestoreTestingPlan	Grants permission to update a restore testing plan	Write	restoreTestingPlan*		
UpdateRestoreTestingSelection	Grants permission to update a resource assignment in a restore testing plan	Write	restoreTestingPlan*		iam:PassRole
UpdateTieringConfiguration	Grants permission to update a tiering configuration	Write	tieringConfiguration*		

Resource types defined by AWS Backup

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
backupVault	`arn:${Partition}:backup:${Region}:${Account}:backup-vault:${BackupVaultName}`	aws:ResourceTag/${TagKey}
backupPlan	`arn:${Partition}:backup:${Region}:${Account}:backup-plan:${BackupPlanId}`	aws:ResourceTag/${TagKey}
recoveryPoint	`arn:${Partition}:${Vendor}:${Region}:*:${ResourceType}:${RecoveryPointId}`	aws:ResourceTag/${TagKey}
framework	`arn:${Partition}:backup:${Region}:${Account}:framework:${FrameworkName}-${FrameworkId}`	aws:ResourceTag/${TagKey}
reportPlan	`arn:${Partition}:backup:${Region}:${Account}:report-plan:${ReportPlanName}-${ReportPlanId}`	aws:ResourceTag/${TagKey}
legalHold	`arn:${Partition}:backup:${Region}:${Account}:legal-hold:${LegalHoldId}`	aws:ResourceTag/${TagKey}
restoreTestingPlan	`arn:${Partition}:backup:${Region}:${Account}:restore-testing-plan:${RestoreTestingPlanName}-${RestoreTestingPlanId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
tieringConfiguration	`arn:${Partition}:backup:${Region}:${Account}:tiering-configuration:${TieringConfigurationName}-${TieringConfigurationId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Backup

AWS Backup defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tags in the request	ArrayOfString
backup:ChangeableForDays	Filters access by the value of the ChangeableForDays parameter	Numeric
backup:CopyTargetOrgPaths	Filters access by the organization unit	ArrayOfString

Condition keys	Description	Type
backup:CopyTargets	Filters access by the ARN of a backup vault	ArrayOfARN
backup:FrameworkArns	Filters access by the Framework ARNs	ArrayOfARN
backup:Index	Filters access by the value of Index parameter	String
backup:MaxRetentionDays	Filters access by the value of the MaxRetentionDays parameter	Numeric
backup:MinRetentionDays	Filters access by the value of the MinRetentionDays parameter	Numeric
backup:MpaApprovalTeamArn	Filters access by the MPA Approval Team ARN of a backup vault	ARN

Actions, resources, and condition keys for AWS Batch

AWS Batch (service prefix: `batch`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Batch
- Resource types defined by AWS Batch
- Condition keys for AWS Batch

Actions defined by AWS Batch

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelJob	Grants permission to cancel a job in an AWS Batch job queue in your account	Write	job*		
CreateComputeEnvironment	Grants permission to create an AWS Batch compute environment in your account	Write	compute-environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConsumableResource	Grants permission to create an AWS Batch consumable resource in your account	Write	consumable-resource*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateJobQueue	Grants permission to create an AWS Batch job queue in your account	Write	job-queue*		
			compute-environment		
			scheduling-policy		
			service-environment		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchedulingPolicy	Grants permission to create an AWS Batch scheduling policy in your account	Write	scheduling-policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateServiceEnvironment	Grants permission to create an AWS Batch service environment in your account	Write	service-environment*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComputeEnvironment	Grants permission to delete an AWS Batch compute environment in your account	Write	compute-environment*		
DeleteConsumableResource	Grants permission to delete an AWS Batch consumable resource in your account	Write	consumable-resource*		
DeleteJobQueue	Grants permission to delete an AWS Batch job queue in your account	Write	job-queue*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSchedulingPolicy	Grants permission to delete an AWS Batch scheduling policy in your account	Write	scheduling-policy*		
DeleteServiceEnvironment	Grants permission to delete an AWS Batch service environment in your account	Write	service-environment*		
DeregisterJobDefinition	Grants permission to deregister an AWS Batch job definition in your account	Write	job-definition-revision*		
DescribeComputeEnvironments	Grants permission to describe one or more AWS Batch compute environments in your account	Read			
DescribeConsumableResource	Grants permission to describe one or more AWS Batch consumable resource in your account	Read	consumable-resource*		
DescribeJobDefinitions	Grants permission to describe one or more AWS Batch job definitions in your account	Read			
DescribeJobQueues	Grants permission to describe one or more AWS Batch job queues in your account	Read			
DescribeJobs	Grants permission to describe a list of AWS Batch jobs in your account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSchedulingPolicies	Grants permission to describe one or more AWS Batch scheduling policies in your account	Read			
DescribeServiceEnvironments	Grants permission to describe one or more AWS Batch service environments in your account	Read			
DescribeServiceJob	Grants permission to describe a AWS Batch service job in your account	Read			
GetJobQueueSnapshot	Grants permission to get a snapshot of an AWS Batch job queue in your account	Read	job-queue*		
ListConsumableResources	Grants permission to list AWS Batch consumable resources in your account	List			
ListJobs	Grants permission to list jobs for a specified AWS Batch job queue in your account	List			
ListJobsByConsumableResource	Grants permission to list AWS Batch jobs that require a specific consumable resource in your account	List	consumable-resource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSchedulingPolicies	Grants permission to list AWS Batch scheduling policies in your account	Read			
ListServiceJobs	Grants permission to list service jobs for a specified AWS Batch job queue in your account	List			
ListTagsForResource	Grants permission to list tags for an AWS Batch resource in your account	Read	compute-environment		
			consumable-resource		
			job		
			job-definition-revision		
			job-queue		
			scheduling-policy		
			service-environment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			service-job		
RegisterJobDefinition	Grants permission to register an AWS Batch job definition in your account	Write	job-definition*	aws:ResourceTag/${TagKey}	
			consumable-resource		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				batch:User batch:Privileged batch:Image batch:LogDriver batch:AWSLogsGroup batch:AWSLogsRegion batch:AWSLogsStreamPrefix batch:AWSLogsCreateGroup batch:EKSServiceAccountName batch:EKSImage	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				batch:EKSRunAsUser batch:EKSRunAsGroup batch:EKSPrivileged batch:EKSNamespace aws:RequestTag/${TagKey} aws:TagKeys	
SubmitJob	Grants permission to submit an AWS Batch job from a job definition in your account	Write	job* job-queue*	batch:ShareIdentifier batch:EKSImage batch:EKSNamespace	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			consumable-resource		
			job-definition		
			job-definition-revision		
				aws:RequestTag/${TagKey} aws:TagKeys	
SubmitServiceJob	Grants permission to submit an AWS Batch service job	Write	job-queue*		
			service-job*	batch:ShareIdentifier	
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag an AWS Batch resource in your account	Tagging	compute-environment		
			consumable-resource		
			job		
			job-definition-revision		
			job-queue		
			scheduling-policy		
			service-environment		
			service-job		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateJob	Grants permission to terminate a job in an AWS Batch job queue in your account	Write	job*		
TerminateServiceJob	Grants permission to terminate a service job in an AWS Batch job queue in your account	Write	service-job*		
UntagResource	Grants permission to untag an AWS Batch resource in your account	Tagging	compute-environment		
			consumable-resource		
			job		
			job-definition-revision		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			job-queue		
			scheduling-policy		
			service-environment		
			service-job		
				aws:TagKeys	
UpdateComputeEnvironment	Grants permission to update an AWS Batch compute environment in your account	Write	compute-environment*		
UpdateConsumableResource	Grants permission to update an AWS Batch consumable resource in your account	Write	consumable-resource*		
UpdateJobQueue	Grants permission to update an AWS Batch job queue in your account	Write	job-queue*		
			compute-environment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			scheduling-policy		
UpdateSchedulingPolicy	Grants permission to update an AWS Batch scheduling policy in your account	Write	scheduling-policy*		
UpdateServiceEnvironment	Grants permission to update an AWS Batch service environment in your account	Write	service-environment*		

Resource types defined by AWS Batch

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
compute-environment	`arn:${Partition}:batch:${Region}:${Account}:compute-environment/${ComputeEnvironmentName}`	aws:ResourceTag/${TagKey}
job-queue	`arn:${Partition}:batch:${Region}:${Account}:job-queue/${JobQueueName}`	aws:ResourceTag/${TagKey}
job-definition	`arn:${Partition}:batch:${Region}:${Account}:job-definition/${JobDefinitionName}`	

Resource types	ARN	Condition keys
job-definition-revision	arn:${Partition}:batch:${Region}:${Account}:job-definition/${JobDefinitionName}:${Revision}	aws:ResourceTag/${TagKey}
job	arn:${Partition}:batch:${Region}:${Account}:job/${JobId}	aws:ResourceTag/${TagKey}
scheduling-policy	arn:${Partition}:batch:${Region}:${Account}:scheduling-policy/${SchedulingPolicyName}	aws:ResourceTag/${TagKey}
service-environment	arn:${Partition}:batch:${Region}:${Account}:service-environment/${ServiceEnvironmentName}	aws:ResourceTag/${TagKey}
service-job	arn:${Partition}:batch:${Region}:${Account}:service-job/${JobId}	aws:ResourceTag/${TagKey}
consumable-resource	arn:${Partition}:batch:${Region}:${Account}:consumable-resource/${ConsumableResourceName}	aws:ResourceTag/${TagKey}

Condition keys for AWS Batch

AWS Batch defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
batch:AWSLogsCreateGroup	Filters access by the specified logging driver to determine whether awslogs group will be created for the logs	Bool
batch:AWSLogsGroup	Filters access by the awslogs group where the logs are located	String
batch:AWSLogsRegion	Filters access by the region where the logs are sent to	String
batch:AWSLogsStreamPrefix	Filters access by the awslogs log stream prefix	String
batch:EKSImage	Filters access by the image used to start a container for an Amazon EKS job	String
batch:EKSNamespace	Filters access by the namespace of a cluster used to run the pod for an Amazon EKS job	String
batch:EKSPrivileged	Filters access by the specified privileged parameter value that determines whether the container is given elevated privileges on the host container instance (similar to the root user) for an Amazon EKS job	Bool
batch:EKSRunAsGroup	Filters access by the specified group numeric ID (gid) used to start a container in an Amazon EKS job	Numeric
batch:EKSRunAsUser	Filters access by the specified user numeric ID (uid) used to start a a container in an Amazon EKS job	Numeric

Condition keys	Description	Type
batch:EKSServiceAccountName	Filters access by the name of the service account used to run the pod for an Amazon EKS job	String
batch:Image	Filters access by the image used to start a container	String
batch:LogDriver	Filters access by the log driver used for the container	String
batch:Privileged	Filters access by the specified privileged parameter value that determines whether the container is given elevated privileges on the host container instance (similar to the root user)	Bool
batch:ShareIdentifier	Filters access by the shareIdentifier used inside submit job	String
batch:User	Filters access by user name or numeric uid used inside the container	String

Actions, resources, and condition keys for Amazon Bedrock

Amazon Bedrock (service prefix: `bedrock`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Bedrock
- Resource types defined by Amazon Bedrock
- Condition keys for Amazon Bedrock

Actions defined by Amazon Bedrock

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllowVendedLogDeliveryForResource [permission only]	Grants permission to configure vended log delivery for a knowledge base	Permissions management	knowledge-base		
ApplyGuardrail	Grants permission to apply a guardrail	Read	guardrail*		
			guardrail-profile		
AssociateAgentCollaborator	Grants permission to associate another existing agent as a collaborator to an existing agent	Write	agent*		
AssociateAgentKnowledgeBase	Grants permission to associate a knowledge base with an agent	Write	agent*		
			knowledge-base*		
AssociateThirdPartyKnowledgeBase	Grants permission to use 3rd party platform to store knowledge data	Write		bedrock:ThirdPartyKnowledgeBaseCrede	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]				ntialsSecretArn	
BatchDeleteEvaluationJob	Grants permission to batch delete list of bedrock evaluation jobs	Write	evaluation-job*		
CallWithBearerToken	Grants permission to use bearer token	Read		bedrock:BearerTokenType	
CancelAutomatedReasoningPolicyBuildWorkflow	Grants permission to cancel a build workflow for an automated reasoning policy	Write	automated-reasoning-policy*		
CountTokens	Grants permission to count the number of tokens in an input prompt	Read	foundation-model*		
CreateAgent	Grants permission to create a new agent and a test agent alias pointing to the DRAFT agent version	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAgentActionGroup	Grants permission to create a new action group in an existing agent	Write	agent*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAgentAlias	Grants permission to create a new alias for an agent	Write	agent*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAutomatedReasoningPolicy	Grants permission to create a new automated reasoning policy	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAutomatedReasoningPolicyTestCase	Grants permission to create a test case for an automated reasoning policy	Write	automated-reasoning-policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAutomatedReasoningPolicyVersion	Grants permission to create a new automated reasoning policy version	Write	automated-reasoning-policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBlueprint	Grants permission to create a blueprint for custom output from data automation	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateBlueprintVersion	Grants permission to create a new version for an existing blueprint	Write	blueprint*		
CreateCustomModel	Grants permission to create a custom model into Bedrock	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCustomModelDeployment	Grants permission to create a custom model deployment for custom model	Write	custom-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataAutomationProject	Grants permission to create a data automation project	Write	blueprint		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	Grants permission to create a data source	Write	knowledge-base*		
CreateEvaluationJob	Grants permission to create a job for evaluation foundation models or custom models	Write	custom-model*		
			default-prompt-router*		
			foundation-model*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			prompt-router*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFlow	Grants permission to create a prompt flow	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFlowAlias	Grants permission to create an alias of a prompt flow	Write	flow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFlowVersion	Grants permission to create an immutable version of a prompt flow	Write	flow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFoundationModelAgreement	Grants permission to create a new foundation model agreement	Write			
CreateGuardrail	Grants permission to create a new guardrail	Write	automated-reasoning-policy		
			automated-reasoning-policy-version		
			guardrail-profile		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateGuardrailVersion	Grants permission to create a new guardrail version	Write	guardrail*		
CreateInferenceProfile	Grants permission to create inference profiles	Write	application-inference-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			foundation-model*		
			inference-profile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInvocation	Grants permission to create a new invocation in an existing session	Write	session*		
CreateKnowledgeBase	Grants permission to create a knowledge base	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateMarketplaceModelEndpoint	Grants permission to create a marketplace model endpoint	Write			
CreateModelCopyJob	Grants permission to create a job for copying a custom model across region or across account	Write	custom-model*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelCustomizationJob	Grants permission to create a job for customizing the model with your custom training data	Write	custom-model*		
			foundation-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelEvaluationJob	Grants permission to create a job for evaluation foundation models or custom models	Write	custom-model*		
			foundation-model*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelImportJob	Grants permission to create a job for importing model into Bedrock	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelInvocationJob	Grants permission to create a new model invocation job	Write	custom-model*		
			foundation-model*		
			model-invocation-job*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePrompt	Grants permission to create a prompt	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePromptRouter	Grants permission to create a custom prompt router	Write	application-inference-profile*		
			foundation-model*		
			inference-profile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePromptVersion	Grants permission to create a version of a prompt	Write	prompt*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProvisionedModelThroughput	Grants permission to create a new provisioned model throughput	Write	custom-model*		
			foundation-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSession	Grants permission to create a new session	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAgent	Grants permission to delete an Agent that you created earlier	Write	agent*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAgentActionGroup	Grants permission to delete an actionGroup that you created earlier	Write	agent*		
DeleteAgentAlias	Grants permission to delete an AgentAlias that you created earlier	Write	agent-alias*		
DeleteAgentMemory	Grants permission to delete existing memory for an alias	Write	agent-alias*		
DeleteAgentVersion	Grants permission to delete an Agent Version that you created earlier	Write	agent*		
DeleteAutomatedReasoningPolicy	Grants permission to delete an automated reasoning policy or its version	Write	automated-reasoning-policy*		
			automated-reasoning-policy-version*		
DeleteAutomatedReasoningPolicyBuildWorkflow	Grants permission to delete a build workflow for an automated reasoning policy	Write	automated-reasoning-policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAutomatedReasoningPolicyTestCase	Grants permission to delete a test case for an automated reasoning policy	Write	automated-reasoning-policy*		
DeleteBlueprint	Grants permission to delete a blueprint for data automation	Write	blueprint*		
DeleteCustomModel	Grants permission to delete a custom model that you created earlier	Write	custom-model*		
DeleteCustomModelDeployment	Grants permission to delete a custom model deployment that you created earlier	Write	custom-model-deployment*		
DeleteDataAutomationProject	Grants permission to delete a data automation project	Write	data-automation-project*		
DeleteDataSource	Grants permission to delete a data source	Write	knowledge-base*		
DeleteEnforcedGuardrailConfiguration	Grants permission to delete account-level enforced guardrail configuration	Write			
DeleteFlow	Grants permission to delete a prompt flow	Write	flow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFlowAlias	Grants permission to delete an alias of a prompt flow	Write	flow-alias*		
DeleteFlowVersion	Grants permission to delete a version of a prompt flow	Write	flow*		
DeleteFoundationModelAgreement	Grants permission to delete a foundation model agreement that you created earlier	Write			
DeleteGuardrail	Grants permission to delete a guardrail or its version	Write	guardrail*		
DeleteImportedModel	Grants permission to delete previously created Bedrock imported model	Write	imported-model*		
DeleteInferenceProfile	Grants permission to delete inference profiles	Write	application-inference-profile*		
DeleteKnowledgeBase	Grants permission to delete a knowledge base	Write	knowledge-base*		
DeleteKnowledgeBaseDocuments	Grants permission to delete documents from a knowledge base	Write	knowledge-base*		
DeleteMarketplaceModelAgreement	Grants permission to unsubscribe from a bedrock marketplace enabled AWS marketplace model	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteMarketplaceModelEndpoint	Grants permission to delete a marketplace model endpoint	Write	bedrock-marketplace-model-endpoint*		
DeleteModelInvocationLoggingConfiguration	Grants permission to delete an existing Invocation logging configuration	Write			
DeletePrompt	Grants permission to delete a prompt or its version	Write	prompt*		
			prompt-version*		
DeletePromptRouter	Grants permission to delete a custom prompt router	Write	prompt-router*		
DeleteProvisionedModelThroughput	Grants permission to delete a provisioned model throughput that you created earlier	Write	provisioned-model*		
DeleteResourcePolicy [permission only]	Deletes a previously created Bedrock resource policy	Write	custom-model		
			guardrail		
			guardrail-profile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSession	Grants permission to delete a Session that you created earlier	Write	session*		
DeregisterMarketplaceModelEndpoint	Grants permission to deregister a marketplace model endpoint to make it unusable in Bedrock Marketplace	Write	bedrock-marketplace-model-endpoint*		
DetectGeneratedContent	Grants permission to detect if the provided content is generated using Amazon Bedrock	Read	foundation-model*		
DisassociateAgentCollaborator	Grants permission to diassociate a collaborator that you associated earlier	Write	agent*		
DisassociateAgentKnowledgeBase	Grants permission to disassociate a knowledge base from the agent	Write	agent* knowledge-base*		
EndSession	Grants permission to end a Session that you created earlier	Write	session*		
ExportAutomatedReasoningPolicyVersion	Grants permission to retrieve an automated reasoning policy version artifact	Read	automated-reasoning-policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			automated-reasoning-policy-version*		
GenerateQuery	Grants permission to generate queries associated with user input	Read			
GetAgent	Grants permission to retrieve an existing agent	Read	agent*		
GetAgentActionGroup	Grants permission to retrieve an existing action group	Read	agent*		
GetAgentAlias	Grants permission to retrieve an existing alias	Read	agent-alias*		
GetAgentCollaborator	Grants permission to retrieve an existing collaborator	Read	agent*		
GetAgentKnowledgeBase	Grants permission to describe a knowledge base associated with an agent	Read	agent*		
			knowledge-base*		
GetAgentMemory	Grants permission to retrieve existing memory for an alias	Read	agent-alias*		
GetAgentVersion	Grants permission to retrieve an existing version of an agent	Read	agent*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAsyncInvoke	Grants permission to get the properties associated with an asynchronous invocation that you have submitted	Read	async-invoke*		
GetAutomatedReasoningPolicy	Grants permission to retrieve an automated reasoning policy or its version	Read	automated-reasoning-policy*		
			automated-reasoning-policy-version*		
GetAutomatedReasoningPolicyAnnotations	Grants permission to retrieve annotations for a build workflow for an automated reasoning policy	Read	automated-reasoning-policy*		
GetAutomatedReasoningPolicyBuildWorkflow	Grants permission to retrieve a build workflow for an automated reasoning policy	Read	automated-reasoning-policy*		
GetAutomatedReasoningPolicyBuildWorkflowResultAssets	Grants permission to retrieve assets for a build workflow for an automated reasoning policy	Read	automated-reasoning-policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAutomatedReasoningPolicyNextScenario	Grants permission to retrieve the next unreviewed generated scenario for a build workflow for an automated reasoning policy	Read	automated-reasoning-policy*		
GetAutomatedReasoningPolicyTestCase	Grants permission to retrieve a test case for an automated reasoning policy	Read	automated-reasoning-policy*		
GetAutomatedReasoningPolicyTestResult	Grants permission to retrieve result for a test case for an automated reasoning policy	Read	automated-reasoning-policy*		
GetBlueprint	Grants permission to retrieve an existing blueprint for data automation	Read	blueprint*		
GetBlueprintRecommendation [permission only]	Grants permission to retrieve blueprint recommendation	Read			
GetCustomModel	Grants permission to get the properties associated with a Bedrock custom model that you have created	Read	custom-model*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCustomModelDeployment	Grants permission to get the properties associated with a custom model deployment. Use this operation to get the status of a custom model deployment	Read	custom-model-deployment*		
GetDataAutomationProject	Grants permission to retrieve an existing data automation project	Read	data-automation-project*		
GetDataAutomationStatus	Grants permission to retrieve the status of a data automation invocation job	Read	data-automation-invocation-job*		
GetDataSource	Grants permission to retrieve an existing data source	Read	knowledge-base*		
GetEvaluationJob	Grants permission to get the properties associated with a evaluation job. Use this operation to get the status of a evaluation job	Read	evaluation-job*		
GetExecutionFlowSnapshot	Grants permission to retrieve the flow definition for a flow execution	Read	flow* flow-alias*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			flow-execution*		
GetFlow	Grants permission to retrieve an existing prompt flow	Read	flow*		
GetFlowAlias	Grants permission to retrieve an existing alias of a prompt flow	Read	flow-alias*		
GetFlowExecution	Grants permission to retrieve an existing execution of a flow alias	Read	flow*		
			flow-alias*		
			flow-execution*		
GetFlowVersion	Grants permission to retrieve an existing version of a prompt flow	Read	flow*		
GetFoundationModel	Grants permission to get the properties associated with a Bedrock foundation model	Read	foundation-model*		
GetFoundationModelAvailability	Grants permission to get the availability of a foundation model	Read			
GetGuardrail	Grants permission to retrieve a guardrail or its version	Read	guardrail*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetImportedModel	Grants permission to get the properties associated with Bedrock imported model	Read	imported-model*		
GetInferenceProfile	Grants permission to get the properties associated with an inference profile	Read	application-inference-profile*		
			inference-profile*		
GetIngestionJob	Grants permission to retrieve an existing ingestion job	Read	knowledge-base*		
GetInvocationStep	Grants permission to get an invocation step from a session	Read	session*		
GetKnowledgeBase	Grants permission to retrieve an existing knowledge base	Read	knowledge-base*		
GetKnowledgeBaseDocuments	Grants permission to get details for documents in a knowledge base	Read	knowledge-base*		
GetMarketplaceModelEndpoint	Grants permission to get the properties of a marketplace model endpoint	Read	bedrock-marketplace-model-endpoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetModelCopyJob	Grants permission to get the properties associated with a model-copy job. Use this operation to get the status of a model-copy job	Read	model-copy-job*		
GetModelCustomizationJob	Grants permission to get the properties associated with a model-customization job. Use this operation to get the status of a model-customization job	Read	model-customization-job*		
GetModelEvaluationJob	Grants permission to get the properties associated with a model-evaluation job. Use this operation to get the status of a model-evaluation job	Read	model-evaluation-job*		
GetModelImportJob	Grants permission to get the properties associated with a model import job and is used to get the status of a model import job	Read	model-import-job*		
GetModelInvocationJob	Grants permission to retrieve a model invocation job	Read	model-invocation-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetModelInvocationLoggingConfiguration	Grants permission to retrieve an existing Invocation logging configuration	Read			
GetPrompt	Grants permission to retrieve an existing prompt or its version	Read	prompt*		
			prompt-version*		
GetPromptRouter	Grants permission to get the properties associated with a prompt router	Read	default-prompt-router*		
			prompt-router*		
GetProvisionedModelThroughput	Grants permission to retrieve a provisioned model throughput	Read	provisioned-model*		
GetResourcePolicy [permission only]	Gets the resource policy document for a Bedrock resource	Read	custom-model		
			guardrail		
			guardrail-profile		
GetSession	Grants permission to retrieve an existing session	Read	session*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUseCaseForModelAccess	Grants permission to retrieve a use case for model access	Read			
IngestKnowledgeBaseDocuments	Grants permission to directly ingest documents into a knowledge base	Write	knowledge-base*		
InvokeAgent	Grants permission to send user input (text-only) to the alias of an agent for Bedrock	Read	agent-alias*		
InvokeAutomatedReasoningPolicy [permission only]	Grants permission to invoke an Automated Reasoning policy	Read	automated-reasoning-policy*		
			automated-reasoning-policy-version*		
InvokeBlueprintRecommendationAsync [permission only]	Grants permission to invoke blueprint recommendations asynchronously	Write	data-automation-profile*		
InvokeBuilder [permission only]	Grants permission to use the conversational builder which aids in building supported bedrock resources	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
InvokeDataAutomation	Grants permission to invoke a call to Sync API of Bedrock data automation	Write	blueprint*		
			data-automation-profile*		
			data-automation-project*		
InvokeDataAutomationAsync	Grants permission to invoke a Bedrock data automation job	Write	blueprint*		
			data-automation-profile*		
			data-automation-project*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
InvokeFlow	Grants permission to invoke a prompt flow with user input	Read	flow-alias*		
InvokeInlineAgent	Grants permission to send user input (text-only) to the inline agent for Bedrock	Read		bedrock:InlineAgentName	
InvokeModel	Grants permission to invoke the specified Bedrock model to run inference using the input provided in the request body	Read	application-inference-profile*		
			async-invoke*		
			bedrock-marketplace-model-endpoint*		
			custom-model-deployment*		
			default-prompt-router*		
			foundation-model*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			imported-model*		
			inference-profile*		
			prompt-router*		
			provisioned-model*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				bedrock:InferenceProfileArn bedrock:PromptRouterArn aws:RequestTag/${TagKey} aws:TagKeys bedrock:GuardrailIdentifier bedrock:ServiceTier	
InvokeModelWithResponseStream	Grants permission to invoke the specified Bedrock model to run inference using the input provided in the request body with streaming response	Read	application-inference-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			bedrock-marketplace-model-endpoint*		
			custom-model-deployment*		
			default-prompt-router*		
			foundation-model*		
			imported-model*		
			inference-profile*		
			prompt-router*		
			provisioned-model*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				bedrock:InferenceProfileArn bedrock:PromptRouterArn bedrock:GuardrailIdentifier bedrock:ServiceTier	
InvokeTool	Grants permission to invoke the specified Bedrock tool to run inference	Read	system-tool*		
ListAgentActionGroups	Grants permission to list action groups in an agent	List	agent*		
ListAgentAliases	Grants permission to list aliases for an agent	List	agent*		
ListAgentCollaborators	Grants permission to list collaborators for an agent	List	agent*		
ListAgentKnowledgeBases	Grants permission to list knowledge bases associated with an agent	List	agent*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAgentVersions	Grants permission to list existing versions of an agent	List	agent*		
ListAgents	Grants permission to list existing agents	List			
ListAsyncInvokes	Grants permission to get a list of asynchronous invocations that you have submitted	List			
ListAutomatedReasoningPolicies	Grants permission to list automated reasoning policies or its versions	List	automated-reasoning-policy		
ListAutomatedReasoningPolicyBuildWorkflows	Grants permission to list build workflows for an automated reasoning policy	List	automated-reasoning-policy*		
ListAutomatedReasoningPolicyTestCases	Grants permission to list test cases for an automated reasoning policy	List	automated-reasoning-policy*		
ListAutomatedReasoningPolicyTestResults	Grants permission to list test result for an automated reasoning policy	List	automated-reasoning-policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListBlueprints	Grants permission to list existing blueprints for data automation	List	data-automation-project		
ListCustomModelDeployments	Grants permission to get the list of custom model deployments that you have submitted	List			
ListCustomModels	Grants permission to get a list of Bedrock custom models that you have created	List			
ListDataAutomationProjects	Grants permission to list existing data automation projects	List	blueprint		
ListDataSources	Grants permission to list existing data sources in an knowledge base	List	knowledge-base*		
ListEnforcedGuardrailsConfiguration	Grants permission to list account-level enforced guardrail configurations	List			
ListEvaluationJobs	Grants permission to get the list of evaluation jobs that you have submitted	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListFlowAliases	Grants permission to list existing aliases of a prompt flow	List	flow*		
ListFlowExecutionEvents	Grants permission to retrieve events for a flow execution	List	flow*		
			flow-alias*		
			flow-execution*		
ListFlowExecutions	Grants permission to list executions of a flow or a flow alias	List	flow*		
			flow-alias		
ListFlowVersions	Grants permission to list existing versions of a prompt flow	List	flow*		
ListFlows	Grants permission to list existing prompt flows	List			
ListFoundationModelAgreementOffers	Grants permission to get a list of foundation model agreement offers	List			
ListFoundationModels	Grants permission to list Bedrock foundation models that you can use	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListGuardrails	Grants permission to list guardrails or its versions	List	guardrail		
ListImportedModels	Grants permission to get list of Bedrock imported models	List			
ListInferenceProfiles	Grants permission to list inference profiles that you can use	List			
ListIngestionJobs	Grants permission to list ingestion jobs in a data source	List	knowledge-base*		
ListInvocationSteps	Grants permission to get list of invocation step from a session	List	session*		
ListInvocations	Grants permission to list invocations in a session	List	session*		
ListKnowledgeBaseDocuments	Grants permission to list documents in a knowledge base	List	knowledge-base*		
ListKnowledgeBases	Grants permission to list existing knowledge bases	List			
ListMarketplaceModelEndpoints	Grants permission to list marketplace model endpoints that you can use	Read			
ListModelCopyJobs	Grants permission to get the list of model copy jobs that you have submitted	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListModelCustomizationJobs	Grants permission to get the list of model customization jobs that you have submitted	List			
ListModelEvaluationJobs	Grants permission to get the list of model evaluation jobs that you have submitted	List			
ListModelImportJobs	Grants permission to get list of model import jobs	List			
ListModelInvocationJobs	Grants permission to list model invocation jobs that you created earlier	List			
ListPromptRouters	Grants permission to list prompt routers that you can use	List			
ListPrompts	Grants permission to list existing prompts	List	prompt		
ListProvisionedModelThroughputs	Grants permission to list provisioned model throughputs that you created earlier	List			
ListSessions	Grants permission to list existing sessions	List			
ListTagsForResource	Grants permission to list tags for a Bedrock resource	Read	agent*		
			agent-alias*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			application-inference-profile*		
			async-invoke*		
			automated-reasoning-policy*		
			automated-reasoning-policy-version*		
			blueprint*		
			custom-model*		
			custom-model-deployment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			data-automation-invocation-job*		
			data-automation-project*		
			evaluation-job*		
			flow*		
			flow-alias*		
			guardrail*		
			imported-model*		
			knowledge-base*		
			model-copy-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-customization-job*		
			model-evaluation-job*		
			model-import-job*		
			model-invocation-job*		
			prompt*		
			prompt-router*		
			prompt-version*		
			provisioned-model*		
			session*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
OptimizePrompt	Grants permission to optimize a prompt with user input	Read			
PrepareAgent	Grants permission to prepare an existing agent to receive runtime requests	Write	agent*		
PrepareFlow	Grants permission to apply the latest changes made to a prompt flow, so that they are reflected at runtime	Write	flow*		
PutEnforcedGuardrailConfiguration	Grants permission to set account-level enforced guardrail configuration	Write			
PutFoundationModelEntitlement	Grants permission to put entitlement to access a serverless foundation model. Do not use to restrict model access	Write			
PutInvocationStep	Grants permission to put an invocation step into an invocation in session	Write	session*		
PutModelInvocationLoggingConfiguration	Grants permission to create an existing Invocation logging configuration	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutResourcePolicy [permission only]	Adds a resource policy for a Bedrock resource	Write	custom-model		
			guardrail		
			guardrail-profile		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutUseCaseForModelAccess	Grants permission to put a use case for model access	Write			
RegisterMarketplaceModelEndpoint	Grants permission to register a sagemaker endpoint as a marketplace model endpoint	Write	bedrock-marketplace-model-endpoint*		
RenderPrompt [permission only]	Grants permission to render an existing prompt or its version	Read	prompt*		
			prompt-version*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Rerank	Grants permission to rank documents based on user input	Write			
Retrieve	Grants permission to retrieve ingested data from a knowledge base	Read	knowledge-base*		
RetrieveAndGenerate	Grants permission to send user input to perform retrieval and generation	Write			
StartAutomatedReasoningPolicyBuildWorkflow	Grants permission to start a build workflow for an automated reasoning policy	Write	automated-reasoning-policy*		
StartAutomatedReasoningPolicyTestWorkflow	Grants permission to start a test workflow for an automated reasoning policy	Write	automated-reasoning-policy*		
StartFlowExecution	Grants permission to start an execution of a flow alias	Write	flow*		
			flow-alias*		
StartIngestionJob	Grants permission to start an ingestion job	Write	knowledge-base*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopEvaluationJob	Grants permission to stop a evaluation job while in progress	Write	evaluation-job*		
StopFlowExecution	Grants permission to stop an execution of a flow alias	Write	flow*		
			flow-alias*		
			flow-execution*		
StopIngestionJob	Grants permission to stop an ingestion job	Write	knowledge-base*		
StopModelCustomizationJob	Grants permission to stop a Bedrock model customization job while in progress	Write	model-customization-job*		
StopModelInvocationJob	Grants permission to stop a model invocation job that you started earlier	Write	model-invocation-job*		
TagResource	Grants permission to Tag a Bedrock resource	Tagging	agent		
			agent-alias		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			application-inference-profile		
			async-invoke		
			automated-reasoning-policy		
			automated-reasoning-policy-version		
			blueprint		
			custom-model		
			custom-model-deployment		
			data-automation-invocation-job		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			data-automation-project		
			evaluation-job		
			flow		
			flow-alias		
			guardrail		
			imported-model		
			knowledge-base		
			model-copy-job		
			model-customization-job		
			model-evaluation-job		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-import-job		
			model-invocation-job		
			prompt		
			prompt-router		
			prompt-version		
			provisioned-model		
			session		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to Untag a Bedrock resource	Tagging	agent		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			agent-alias		
			application-inference-profile		
			async-invoke		
			automated-reasoning-policy		
			automated-reasoning-policy-version		
			blueprint		
			custom-model		
			custom-model-deployment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			data-automation-invocation-job		
			data-automation-project		
			evaluation-job		
			flow		
			flow-alias		
			guardrail		
			imported-model		
			knowledge-base		
			model-copy-job		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-customization-job		
			model-evaluation-job		
			model-import-job		
			model-invocation-job		
			prompt		
			prompt-router		
			prompt-version		
			provisioned-model		
			session		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateAgent	Grants permission to update an existing agent	Write	agent*		
UpdateAgentActionGroup	Grants permission to update an existing action group	Write	agent*		
UpdateAgentAlias	Grants permission to update an existing alias	Write	agent-alias*		
UpdateAgentCollaborator	Grants permission to update an existing collaborator	Write	agent*		
UpdateAgentKnowledgeBase	Grants permission to update a knowledge base associated with an agent	Write	agent* knowledge-base*		
UpdateAutomatedReasoningPolicy	Grants permission to update an automated reasoning policy	Write	automated-reasoning-policy*		
UpdateAutomatedReasoningPolicyAnnotations	Grants permission to update annotations for a build workflow for an automated reasoning policy	Write	automated-reasoning-policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAutomatedReasoningPolicyTestCase	Grants permission to update a test case for automated reasoning policy	Write	automated-reasoning-policy*		
UpdateBlueprint	Grants permission to update a blueprint for data automation	Write	blueprint*		
UpdateCustomModelDeployment	Grants permission to update an existing custom model deployment with a new custom model	Write	custom-model*		
			custom-model-deployment*		
UpdateDataAutomationProject	Grants permission to update a data automation project	Write	data-automation-project*		
			blueprint		
UpdateDataSource	Grants permission to update a data source	Write	knowledge-base*		
UpdateFlow	Grants permission to update a prompt flow	Write	flow*		
UpdateFlowAlias	Grants permission to update the configuration of an alias of a prompt flow	Write	flow-alias*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateGuardrail	Grants permission to update a guardrail	Write	guardrail*		
			automated-reasoning-policy		
			automated-reasoning-policy-version		
			guardrail-profile		
UpdateKnowledgeBase	Grants permission to update a knowledge base	Write	knowledge-base*		
UpdateMarketplaceModelEndpoint	Grants permission to update a marketplace model endpoint	Write	bedrock-marketplace-model-endpoint*		
UpdatePrompt	Grants permission to update a prompt	Write	prompt*		
UpdateProvisionedModelThroughput	Grants permission to update a provisioned model throughput that you created earlier	Write	custom-model*		
			foundation-model*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			provisioned-model*		
UpdateSession	Grants permission to update an existing session	Write	session*		
ValidateFlowDefinition	Grants permission to validate prompt flow definitions	Read			

Resource types defined by Amazon Bedrock

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
foundation-model	`arn:${Partition}:bedrock:${Region}::foundation-model/${ResourceId}`	
system-tool	`arn:${Partition}:bedrock::${Account}:system-tool/${ResourceId}`	
async-invoke	`arn:${Partition}:bedrock:${Region}:${Account}:async-invoke/${ResourceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
inference-profile	arn:${Partition}:bedrock:${Region}:${Account}:inference-profile/${ResourceId}	
default-prompt-router	arn:${Partition}:bedrock:${Region}:${Account}:default-prompt-router/${ResourceId}	
prompt-router	arn:${Partition}:bedrock:${Region}:${Account}:prompt-router/${ResourceId}	
application-inference-profile	arn:${Partition}:bedrock:${Region}:${Account}:application-inference-profile/${ResourceId}	aws:ResourceTag/${TagKey}
custom-model	arn:${Partition}:bedrock:${Region}:${Account}:custom-model/${ResourceId}	aws:ResourceTag/${TagKey}
provisioned-model	arn:${Partition}:bedrock:${Region}:${Account}:provisioned-model/${ResourceId}	aws:ResourceTag/${TagKey}
model-customization-job	arn:${Partition}:bedrock:${Region}:${Account}:model-customization-job/${ResourceId}	aws:ResourceTag/${TagKey}
agent	arn:${Partition}:bedrock:${Region}:${Account}:agent/${AgentId}	aws:ResourceTag/${TagKey}
agent-alias	arn:${Partition}:bedrock:${Region}:${Account}:agent-alias/${AgentId}/${AgentAliasId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
knowledge-base	arn:${Partition}:bedrock:${Region}:${Account}:knowledge-base/${KnowledgeBaseId}	aws:ResourceTag/${TagKey}
model-evaluation-job	arn:${Partition}:bedrock:${Region}:${Account}:model-evaluation-job/${ResourceId}	aws:ResourceTag/${TagKey}
evaluation-job	arn:${Partition}:bedrock:${Region}:${Account}:evaluation-job/${ResourceId}	aws:ResourceTag/${TagKey}
model-invocation-job	arn:${Partition}:bedrock:${Region}:${Account}:model-invocation-job/${JobIdentifier}	aws:ResourceTag/${TagKey}
guardrail	arn:${Partition}:bedrock:${Region}:${Account}:guardrail/${GuardrailId}	aws:ResourceTag/${TagKey}
guardrail-profile	arn:${Partition}:bedrock:${Region}:${Account}:guardrail-profile/${ResourceId}	
automated-reasoning-policy	arn:${Partition}:bedrock:${Region}:${Account}:automated-reasoning-policy/${AutomatedReasoningPolicyId}	aws:ResourceTag/${TagKey}
automated-reasoning-policy-version	arn:${Partition}:bedrock:${Region}:${Account}:automated-reasoning-policy/${AutomatedReasoningPolicyId}:${AutomatedReasoningPolicyVersion}	aws:ResourceTag/${TagKey}
flow	arn:${Partition}:bedrock:${Region}:${Account}:flow/${FlowId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
flow-alias	arn:${Partition}:bedrock:${Region}:${Account}:flow/${FlowId}/alias/${FlowAliasId}	aws:ResourceTag/${TagKey}
flow-execution	arn:${Partition}:bedrock:${Region}:${Account}:flow/${FlowId}/alias/${FlowAliasId}/execution/${FlowExecutionId}	
model-copy-job	arn:${Partition}:bedrock:${Region}:${Account}:model-copy-job/${ResourceId}	aws:ResourceTag/${TagKey}
prompt	arn:${Partition}:bedrock:${Region}:${Account}:prompt/${PromptId}	aws:ResourceTag/${TagKey}
prompt-version	arn:${Partition}:bedrock:${Region}:${Account}:prompt/${PromptId}:${PromptVersion}	aws:ResourceTag/${TagKey}
model-import-job	arn:${Partition}:bedrock:${Region}:${Account}:model-import-job/${ResourceId}	aws:ResourceTag/${TagKey}
imported-model	arn:${Partition}:bedrock:${Region}:${Account}:imported-model/${ResourceId}	aws:ResourceTag/${TagKey}
bedrock-marketplace-model-endpoint	arn:${Partition}:bedrock:${Region}:${Account}:marketplace/model-endpoint/all-access	

Resource types	ARN	Condition keys
data-automation-project	arn:${Partition}:bedrock:${Region}:${Account}:data-automation-project/${ProjectId}	aws:ResourceTag/${TagKey}
blueprint	arn:${Partition}:bedrock:${Region}:${Account}:blueprint/${BlueprintId}	aws:ResourceTag/${TagKey}
data-automation-invocation-job	arn:${Partition}:bedrock:${Region}:${Account}:data-automation-invocation/${JobId}	aws:ResourceTag/${TagKey}
data-automation-profile	arn:${Partition}:bedrock:${Region}:${Account}:data-automation-profile/${ProfileId}	
session	arn:${Partition}:bedrock:${Region}:${Account}:session/${SessionId}	aws:ResourceTag/${TagKey}
custom-model-deployment	arn:${Partition}:bedrock:${Region}:${Account}:custom-model-deployment/${ResourceId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Bedrock

Amazon Bedrock defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by creating requests based on the allowed set of values for each of the mandatory tags	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by having actions based on the tag value associated with the resource	String
aws:TagKeys	Filters access by creating requests based on the presence of mandatory tags in the request	ArrayOfString
bedrock:BearerTokenType	Filters access by the Short-term or Long-term bearer tokens	String
bedrock:GuardrailIdentifier	Filters access by the GuardrailIdentifier containing the GuardrailArn or the GuardrailArn:NumericVersion	ARN
bedrock:InferenceProfileArn	Filters access by the specified inference profile	ARN
bedrock:InlineAgentName	Filters access by the Inline Agent Names, this will be used in InvokeInlineAgent API names	String
bedrock:PromptRouterArn	Filters access by the specified prompt router	ARN
bedrock:ServiceTier	Filters access by the specified ServiceTier	String
bedrock:ThirdPartyKnowledgeBaseCredentialsSecretArn	Filters access by the secretArn containing the credentials of the third party platform	ARN

Actions, resources, and condition keys for AWS Billing And Cost Management Data Exports

AWS Billing And Cost Management Data Exports (service prefix: `bcm-data-exports`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Billing And Cost Management Data Exports
- Resource types defined by AWS Billing And Cost Management Data Exports
- Condition keys for AWS Billing And Cost Management Data Exports

Actions defined by AWS Billing And Cost Management Data Exports

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit

resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateExport	Grants permission to create an export	Write	table*		
			billingview		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
DeleteExport	Grants permission to delete an export	Write	export*		
				aws:ResourceTag/${TagKey}	
GetExecution	Grants permission to get the execution of an export	Read	export*		
				aws:ResourceTag/${TagKey}	
GetExport	Grants permission to get an export	Read	export*		
				aws:ResourceTag/${TagKey}	
GetTable	Grants permission to get the details of a table	Read	table*		
ListExecutions	Grants permission to list all executions of an export	List	export*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListExports	Grants permission to list all exports	List			
ListTables	Grants permission to list all available tables	List			
ListTagsForResource	Grants permission to list tags for a resource	Read	export*		
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to tag a resource	Tagging	export*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag a resource	Tagging	export*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateExport	Grants permission to update an export	Write	export*		
			table*		
			billingview		
				aws:ResourceTag/${TagKey}	

Resource types defined by AWS Billing And Cost Management Data Exports

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
export	arn:${Partition}:bcm-data-exports:${Region}:${Account}:export/${Identifier}	aws:ResourceTag/${TagKey}
table	arn:${Partition}:bcm-data-exports:${Region}:${Account}:table/${Identifier}	
billingview	arn:${Partition}:billing::${Account}:billingview/${ResourceId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Billing And Cost Management Data Exports

AWS Billing And Cost Management Data Exports defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Budget Service

AWS Budget Service (service prefix: `budgets`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Budget Service
- Resource types defined by AWS Budget Service
- Condition keys for AWS Budget Service

Actions defined by AWS Budget Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

> **Note**
>
> The actions in this table are not APIs, but are instead permissions that grant access to the AWS Billing and Cost Management APIs that access budgets.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBudgetAction	Grants permission to configure a response that executes once your budget exceeds a specific budget	Write	budgetAction*		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	threshold. Creating a budget action with tags also requires the 'budgets:TagResource' permission			aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteBudgetAction	Grants permission to delete an action that is associated with a specific budget	Write	budgetAction*		
DescribeBudgetAction	Grants permission to retrieve the details of a specific budget action associated with a budget	Read	budgetAction*		
DescribeBudgetActionHistories	Grants permission to retrieve a historical view of the budget actions statuses associated with a particular budget action. These status include statues such as 'Standby', 'Pending' and 'Executed'	Read	budgetAction*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeBudgetActionsForAccount	Grants permission to retrieve the details of all of the budget actions associated with your account	Read			
DescribeBudgetActionsForBudget	Grants permission to retrieve the details of all of the budget actions associated with a budget	Read	budget*		
ExecuteBudgetAction	Grants permission to initiate a pending budget action as well as reverse a previously executed budget action	Write	budgetAction*		
ListTagsForResource	Grants permission to view resource tags for a budget or budget action	Read	budget		
			budgetAction		
ModifyBudget	Grants permission to create and modify budgets, and edit budget details. Creating a budget with tags also requires the 'budgets:TagResource' permission	Write	budget*		iam:CreateServiceLinkedRole
TagResource	Grants permission to apply resource tags to a budget or budget action. Also needed to create a budget or budget action with tags	Tagging	budget		
			budgetAction		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove resource tags from a budget or budget action	Tagging	budget		
			budgetAction		
				aws:TagKeys	
UpdateBudgetAction	Grants permission to update the details of a specific budget action associated with a budget	Write	budgetAction*		iam:PassRole
ViewBudget	Grants permission to view budgets and budget details	Read	budget*		billing:GetBillingViewData

Resource types defined by AWS Budget Service

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
budget	arn:${Partition}:budgets::${Account}:budget/${BudgetName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
budgetAction	arn:${Partition}:budgets::${Account}:budget/${BudgetName}/action/${ActionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Condition keys for AWS Budget Service

AWS Budget Service defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access based on the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access based on the tags associated with the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access based on the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Certificate Manager

AWS Certificate Manager (service prefix: `acm`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Certificate Manager
- Resource types defined by AWS Certificate Manager
- Condition keys for AWS Certificate Manager

Actions defined by AWS Certificate Manager

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddTagsToCertificate	Grants permission to add one or more tags to a certificate	Tagging	certificate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCertificate	Grants permission to delete a certificate and its associated private key	Write	certificate*		
DescribeCertificate	Grants permission to retreive a certificates and its metadata	Read	certificate*		
ExportCertificate	Grants permission to export an exportable certificate for use anywhere	Read	certificate*		
				acm:DomainNames	
GetAccountConfiguration	Grants permission to retrieve account level configuration from AWS Certificate Manager	Read			
GetCertificate	Grants permission to retrieve a certificate and certificate chain for a certificate ARN	Read	certificate*		
ImportCertificate	Grants permission to import a 3rd party certificate into AWS Certificate Manager (ACM)	Write	certificate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
ListCertificates	Grants permission to retrieve a list of the certificate ARNs and the domain name for each ARN	List			
ListTagsForCertificate	Grants permission to lists the tags that have been associated with a certificate	Read	certificate*		
PutAccountConfiguration	Grants permission to update account level configuration in AWS Certificate Manager	Write			
RemoveTagsFromCertificate	Grants permission to remove one or more tags from a certificate	Tagging	certificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RenewCertificate	Grants permission to renew an eligible private certificate	Write	certificate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RequestCertificate	Grants permission to requests a public or private certificate	Write		aws:RequestTag/${TagKey} aws:TagKeys acm:DomainNames acm:CertificateTransparencyLogging acm:ValidationMethod acm:KeyAlgorithm acm:CertificateAuthority acm:Export	
ResendValidationEmail	Grants permission to resend an email to request domain ownership validation	Write	certificate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RevokeCertificate	Grants permission to revoke an exportable certificate	Write	certificate*		
				acm:DomainNames	
UpdateCertificateOptions	Grants permission to update a certificate configuration. Use this to specify whether to opt in to or out of certificate transparency logging	Write	certificate*		

Resource types defined by AWS Certificate Manager

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
certificate	`arn:${Partition}:acm:${Region}:${Account}:certificate/${CertificateId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Certificate Manager

AWS Certificate Manager defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the

policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
acm:CertificateAuthority	Filters access by certificateAuthority in the request. Can be used to restrict which Certificate Authorites certificates can be issued from	String
acm:CertificateTransparencyLogging	Filters access by certificateTransparencyLogging option in the request. Default 'ENABLED' if no key is present in the request	String
acm:DomainNames	Filters access by domainNames in the request. This key can be used to restrict which domains can be in certificate requests	ArrayOfString
acm:Export	Filters access by the export option in the request. Can be used to restrict creation of certificates that can be exported	String
acm:KeyAlgorithm	Filters access by keyAlgorithm in the request	String
acm:ValidationMethod	Filters access by validationMethod in the request. Default 'EMAIL' if no key is present in the request	String
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for AWS CloudTrail

AWS CloudTrail (service prefix: `cloudtrail`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS CloudTrail
- Resource types defined by AWS CloudTrail
- Condition keys for AWS CloudTrail

Actions defined by AWS CloudTrail

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddTags	Grants permission to add one or more tags to a trail, event data store, channel or dashboard, up to a limit of 50	Tagging	channel		
			dashboard		
			eventdatastore		
			trail		
				aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
CancelQuery	Grants permission to cancel a running query	Write	eventdatastore*		
CreateChannel	Grants permission to create a channel	Write	channel*		cloudtrail:AddTags
			eventdatastore*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDashboard	Grants permission to create a dashboard	Write	dashboard*		cloudtrail:AddTags cloudtrail:StartDashboardRefresh cloudtrail:StartQuery

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventDataStore	Grants permission to create an event data store	Write	eventdatastore*		cloudtrail:AddTags iam:CreateServiceLinkedRole iam:GetRole kms:Decrypt kms:GenerateDataKey organizations:ListAWSServiceAccessForOrganization

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateServiceLinkedChannel [permission only]	Grants permission to create a service-linked channel that specifies the settings for delivery of log data to an AWS service	Write	channel*		
CreateTrail	Grants permission to create a trail that specifies the settings for delivery of log data to an Amazon S3 bucket	Write	trail*		cloudtrail:AddTags iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Grants permission to delete a channel	Write	channel*		
DeleteDashboard	Grants permission to delete a dashboard	Write	dashboard*		
DeleteEventDataStore	Grants permission to delete an event data store	Write	eventdatastore*		
DeleteResourcePolicy	Grants permission to delete a resource policy from the provided resource	Write	channel		
			dashboard		
			eventdatastore		
DeleteServiceLinkedChannel [permission only]	Grants permission to delete a service-linked channel	Write	channel*		
DeleteTrail	Grants permission to delete a trail	Write	trail*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterOrganizationDelegatedAdmin	Grants permission to deregister an AWS Organizations member account as a delegated administrator	Write			organizations:DeregisterDelegatedAdministrator organizations:ListAWSServiceAccessForOrganization
DescribeQuery	Grants permission to list details for the query	Read	eventdatastore*		
DescribeTrails	Grants permission to list settings for the trails associated with the current region for your account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableFederation	Grants permission to disable federation of event data store data by using the AWS Glue Data Catalog	Write	eventdatastore*		glue:DeleteDatabase glue:DeleteTable glue:PassConnection lakeformation:DeregisterResource lakeformation:RegisterResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableFederation	Grants permission to enable federation of event data store data by using the AWS Glue Data Catalog	Write	eventdatastore*		glue:CreateDatabase glue:CreateTable iam:GetRole iam:PassRole lakeformation:DeregisterResource lakeformation:RegisterResource
GenerateQuery	Grants permission to generate a query for a specified event data store using the CloudTrail Lake query generator	Write	eventdatastore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateQueryResultsSummary [permission only]	Grants permission to generate a results summary for specified queries using the CloudTrail natural language generator	Read	eventdatastore*		cloudtrail:GetQueryResults kms:Decrypt kms:GenerateDataKey
GetChannel	Grants permission to return information about a specific channel	Read	channel*		
GetDashboard	Grants permission to list settings for the dashboard	Read	dashboard*		
GetEventConfiguration	Grants permission to list event configurations that are configured for a trail or an event data store	Read	eventdatastore		
			trail		
GetEventDataStore	Grants permission to list settings for the event data store	Read	eventdatastore*		
GetEventDataStoreData	Grants permission to get data from an event data store by using the AWS Glue Data Catalog	Read	eventdatastore*		kms:Decrypt kms:GenerateDataKey

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEventSelectors	Grants permission to list settings for event selectors configured for a trail	Read	trail*		
GetImport	Grants permission to return information about a specific import	Read			
GetInsightSelectors	Grants permission to list CloudTrail Insights selectors that are configured for a trail or event data store	Read	eventdatastore		
			trail		
GetQueryResults	Grants permission to fetch results of a complete query	Read	eventdatastore*		kms:Decrypt kms:GenerateDataKey
GetResourcePolicy	Grants permission to get the resource policy attached to the provided resource	Read	channel		
			dashboard		
			eventdatastore		
GetServiceLinkedChannel [permission only]	Grants permission to list settings for the service-linked channel	Read	channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTrail	Grants permission to list settings for the trail	Read	trail*		
GetTrailStatus	Grants permission to retrieve a JSON-formatted list of information about the specified trail	Read	trail*		
ListChannels	Grants permission to list the channels in the current account, and their source names	List			
ListDashboards	Grants permission to list dashboards associated with the current region for your account	List			
ListEventDataStores	Grants permission to list event data stores associated with the current region for your account	List			
ListImportFailures	Grants permission to return a list of failures for the specified import	Read			
ListImports	Grants permission to return information on all imports, or a select set of imports by ImportStatus or Destination	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListInsightsData	Grants permission to retrieve data captured by CloudTrail Insights	List	trail*		
ListPublicKeys	Grants permission to list the public keys whose private keys were used to sign trail digest files within a specified time range	Read			
ListQueries	Grants permission to list queries associated with an event data store	List	eventdatastore*		
ListServiceLinkedChannels [permission only]	Grants permission to list service-linked channels associated with the current region for a specified account	List			
ListTags	Grants permission to list the tags for trails, event data stores, channels or dashboards in the current region	Read	channel		
			dashboard		
			eventdatastore		
			trail		
ListTrails	Grants permission to list trails associated with the current region for your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
LookupEvents	Grants permission to look up and retrieve metric data for API activity events captured by CloudTrail that create, update, or delete resources in your account	Read			
PutEventConfiguration	Grants permission to create and update event configurations for a trail or an event data store	Write	eventdatastore		iam:CreateServiceLinkedRole iam:GetRole
			trail		
PutEventSelectors	Grants permission to create and update event selectors for a trail	Write	trail*		
PutInsightSelectors	Grants permission to create and update CloudTrail Insights selectors for a trail or event data store	Write	eventdatastore		
			trail		
PutResourcePolicy	Grants permission to attach a resource policy to the provided resource	Write	channel		
			dashboard		
			eventdatastore		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterOrganizationDelegatedAdmin	Grants permission to register an AWS Organizations member account as a delegated administrator	Write			iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization organizations:RegisterDelegatedAdministrator
RemoveTags	Grants permission to remove tags from a trail, event data store, channel or dashboard	Tagging	channel		
			dashboard		
			eventdatastore		
			trail		
				aws:TagKeys	
RestoreEventDataStore	Grants permission to restore an event data store	Write	eventdatastore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchSampleQueries	Grants permission to perform semantic search for CloudTrail Lake sample queries	Read			
StartDashboardRefresh	Grants permission to start a refresh on the specified dashboard	Write	dashboard*		cloudtrail:StartQuery
StartEventDataStoreIngestion	Grants permission to start ingestion on an event data store	Write	eventdatastore*		
StartImport	Grants permission to start an import of logged trail events from a source S3 bucket to a destination event data store	Write			
StartLogging	Grants permission to start the recording of AWS API calls and log file delivery for a trail	Write	trail*		
StartQuery	Grants permission to start a new query on a specified event data store	Write	eventdatastore*		kms:Decrypt kms:GenerateDataKey
StopEventDataStoreIngestion	Grants permission to stop ingestion on an event data store	Write	eventdatastore*		
StopImport	Grants permission to stop a specified import	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopLogging	Grants permission to stop the recording of AWS API calls and log file delivery for a trail	Write	trail*		
UpdateChannel	Grants permission to update a channel	Write	channel*		
UpdateDashboard	Grants permission to update a dashboard	Write	dashboard*		cloudtrail:StartDashboardRefresh cloudtrail:StartQuery

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEventDataStore	Grants permission to update an event data store	Write	eventdatastore*		iam:CreateServiceLinkedRole iam:GetRole kms:Decrypt kms:GenerateDataKey organizations:ListAWSServiceAccessForOrganization
UpdateServiceLinkedChannel [permission only]	Grants permission to update the service-linked channel settings for delivery of log data to an AWS service	Write	channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateTrail	Grants permission to update the settings that specify delivery of log files	Write	trail*		iam:CreateServiceLinkedRole iam:GetRole organizations:ListAWSServiceAccessForOrganization

Resource types defined by AWS CloudTrail

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Note

For policies that control access to CloudTrail actions, the Resource element is always set to "*". For information about using resource ARNs in an IAM policy, see How AWS CloudTrail works with IAM in the *AWS CloudTrail User Guide*.

Resource types	ARN	Condition keys
trail	arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}	aws:ResourceTag/${TagKey}
eventdatastore	arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/${EventDataStoreId}	aws:ResourceTag/${TagKey}
channel	arn:${Partition}:cloudtrail:${Region}:${Account}:channel/${ChannelId}	aws:ResourceTag/${TagKey}
dashboard	arn:${Partition}:cloudtrail:${Region}:${Account}:dashboard/${DashboardName}	aws:ResourceTag/${TagKey}

Condition keys for AWS CloudTrail

AWS CloudTrail defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags attached to the resource	String
aws:TagKeys	Filters access by the tag keys in a request	ArrayOfString

Actions, resources, and condition keys for Amazon CloudWatch

Amazon CloudWatch (service prefix: `cloudwatch`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon CloudWatch
- Resource types defined by Amazon CloudWatch
- Condition keys for Amazon CloudWatch

Actions defined by Amazon CloudWatch

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetServiceLevelIndicatorReport	Grants permission to batch get service level indicator report	Read			
BatchGetServiceLevelObjectiveBudgetReport	Grants permission to batch retrieve a service level objective budget report	Read	slo*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateServiceLevelObjective	Grants permission to create a service level objective	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlarms	Grants permission to delete a collection of alarms	Write	alarm*		
DeleteAnomalyDetector	Grants permission to delete the specified anomaly detection model from your account	Write			
DeleteDashboards	Grants permission to delete all CloudWatch dashboards that you specify	Write	dashboard*		
DeleteInsightRules	Grants permission to delete a collection of insight rules	Write	insight-rule*		
DeleteMetricStream	Grants permission to delete the CloudWatch metric stream that you specify	Write	metric-stream*		
DeleteServiceLevelObjective	Grants permission to delete a service level objective	Write	slo*		
DescribeAlarmHistory	Grants permission to retrieve the history for the specified alarm	Read	alarm*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAlarms	Grants permission to describe all alarms, currently owned by the user's account	Read	alarm*		
DescribeAlarmsForMetric	Grants permission to describe all alarms configured on the specified metric, currently owned by the user's account	Read			
DescribeAnomalyDetectors	Grants permission to list the anomaly detection models that you have created in your account	Read			
DescribeInsightRules	Grants permission to describe all insight rules, currently owned by the user's account	Read			
DisableAlarmActions	Grants permission to disable actions for a collection of alarms	Write	alarm*		
DisableInsightRules	Grants permission to disable a collection of insight rules	Write	insight-rule*		
EnableAlarmActions	Grants permission to enable actions for a collection of alarms	Write	alarm*		
EnableInsightRules	Grants permission to enable a collection of insight rules	Write	insight-rule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableTopologyDiscovery	Grants permission to enable a CloudWatch topology discovery	Write			
GenerateQuery	Grants permission to generate a Metrics Insights or Logs Insights query string from a natural language prompt	Read			
GenerateQueryResultsSummary	Grants permission to generate a summary of CloudWatch LogInsights query results in natural language using generative AI	Read			
GetDashboard	Grants permission to display the details of the CloudWatch dashboard you specify	Read	dashboard*		
GetInsightRuleReport	Grants permission to return the top-N report of unique contributors over a time range for a given insight rule	Read	insight-rule*		
GetMetricData	Grants permission to retrieve batch amounts of CloudWatch metric data and perform metric math on retrieved data	Read			
GetMetricStatistics	Grants permission to retrieve statistics for the specified metric	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMetricStream	Grants permission to return the details of a CloudWatch metric stream	Read	metric-stream*		
GetMetricWidgetImage	Grants permission to retrieve snapshots of metric widgets	Read			
GetService	Grants permission to retrieve information about a service	Read	service*		
GetServiceData [permission only]	Grants permission to retrieve service data	Read	service*		
GetServiceLevelObjective	Grants permission to retrieve information about service level objective	Read	slo*		
GetTopologyDiscoveryStatus [permission only]	Grants permission to retrieve a CloudWatch topology discovery status	Read			
GetTopologyMap	Grants permission to retrieve a CloudWatch topology map	Read			
Link [permission only]	Grants permission to share CloudWatch resources with a monitoring account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDashboards	Grants permission to return a list of all CloudWatch dashboards in your account	List			
ListEntitiesForMetric [permission only]	Grants permission to retrieve all the entities that are emitting a given metric	List			
ListManagedInsightRules	Grants permission to list available managed Insight Rules for a given Resource ARN	Read		aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestManagedResourceARNs	
ListMetricStreams	Grants permission to return a list of all CloudWatch metric streams in your account	List			
ListMetrics	Grants permission to retrieve a list of valid metrics stored for the AWS account owner	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListServiceLevelObjectives	Grants permission to list service level objectives	List			
ListServices	Grants permission to list services	List			
ListTagsForResource	Grants permission to list tags for an Amazon CloudWatch resource	List	alarm		
			alarm-mute-rule		
			insight-rule		
			slo		
	SCENARIO: CloudWatch-Alarm		alarm*		
	SCENARIO: CloudWatch-AlarmMuteRule		alarm-mute-rule*		
	SCENARIO: CloudWatch-InsightRule		insight-rule*		
	SCENARIO: CloudWatch-ServiceLevelObjective		slo*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAnomalyDetector	Grants permission to create or update an anomaly detection model for a CloudWatch metric	Write			
PutCompositeAlarm	Grants permission to create or update a composite alarm	Write	alarm*		
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:AlarmActions	
PutDashboard	Grants permission to create a CloudWatch dashboard, or update an existing dashboard if it already exists	Write	dashboard*		
PutInsightRule	Grants permission to create a new insight rule or replace an existing insight rule	Write	insight-rule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestInsightRuleLogGroups	
PutManagedInsightRules	Grants permission to create managed Insight Rules	Write		aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:requestManagedResourceARNs	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutMetricAlarm	Grants permission to create or update an alarm and associates it with the specified Amazon CloudWatch metric	Write	alarm*		
				aws:RequestTag/${TagKey} aws:TagKeys cloudwatch:AlarmActions	
PutMetricData	Grants permission to publish metric data points to Amazon CloudWatch	Write		cloudwatch:namespace	
PutMetricStream	Grants permission to create a CloudWatch metric stream, or update an existing metric stream if it already exists	Write	metric-stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
SetAlarmState	Grants permission to temporarily set the state of an alarm for testing purposes	Write	alarm*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartMetricStreams	Grants permission to start all CloudWatch metric streams that you specify	Write	metric-stream*		
StopMetricStreams	Grants permission to stop all CloudWatch metric streams that you specify	Write	metric-stream*		
TagResource	Grants permission to add tags to an Amazon CloudWatch resource	Tagging	alarm		
			alarm-mute-rule		
			insight-rule		
			slo		
				aws:TagKeys aws:RequestTag/${TagKey}	
	SCENARIO: CloudWatch-Alarm		alarm*		
	SCENARIO: CloudWatch-AlarmMuteRule		alarm-mute-rule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: CloudWatch-InsightRule		insight-rule*		
	SCENARIO: CloudWatch-ServiceLevelObjective		slo*		
UntagResource	Grants permission to remove a tag from an Amazon CloudWatch resource	Tagging	alarm		
			alarm-mute-rule		
			insight-rule		
			slo		
				aws:TagKeys	
	SCENARIO: CloudWatch-Alarm		alarm*		
	SCENARIO: CloudWatch-AlarmMuteRule		alarm-mute-rule*		
	SCENARIO: CloudWatch-InsightRule		insight-rule*		
	SCENARIO: CloudWatch-ServiceLevelObjective		slo*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateServiceLevelObjective	Grants permission to update a service level objective	Write	slo*		

Resource types defined by Amazon CloudWatch

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
alarm	`arn:${Partition}:cloudwatch:${Region}:${Account}:alarm:${AlarmName}`	aws:ResourceTag/${TagKey}
dashboard	`arn:${Partition}:cloudwatch::${Account}:dashboard/${DashboardName}`	
insight-rule	`arn:${Partition}:cloudwatch:${Region}:${Account}:insight-rule/${InsightRuleName}`	aws:ResourceTag/${TagKey}
metric-stream	`arn:${Partition}:cloudwatch:${Region}:${Account}:metric-stream/${MetricStreamName}`	aws:ResourceTag/${TagKey}
slo	`arn:${Partition}:cloudwatch:${Region}:${Account}:slo/${SloName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
service	`arn:${Partition}:cloudwatch:${Region}:${Account}:service/${ServiceName}-${UniqueAttributesHex}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon CloudWatch

Amazon CloudWatch defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters actions based on tag-value associated with the resource	String
aws:TagKeys	Filters actions based on the presence of mandatory tags in the request	ArrayOfString
cloudwatch:AlarmActions	Filters actions based on defined alarm actions	ArrayOfString
cloudwatch:namespace	Filters actions based on the presence of optional namespace values	String
cloudwatch:request	Filters actions based on the Log Groups specified in an Insight Rule	ArrayOfString

Condition keys	Description	Type
InsightRuleLogGroups		
cloudwatch:requestManagedResourceARNs	Filters access by the Resource ARNs specified in a managed Insight Rule	ArrayOfARN

Actions, resources, and condition keys for Amazon CloudWatch Logs

Amazon CloudWatch Logs (service prefix: `logs`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon CloudWatch Logs
- Resource types defined by Amazon CloudWatch Logs
- Condition keys for Amazon CloudWatch Logs

Actions defined by Amazon CloudWatch Logs

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateKmsKey	Grants permission to associate the specified AWS Key Management Service (AWS KMS) customer master key (CMK) with the specified log group	Write	log-group*		
AssociateSourceToS3TableIntegration	Grants permission to associate a log source to an S3 Tables integration	Write			
CancelExportTask	Grants permission to cancel an export task if it is in PENDING or RUNNING state	Write			
CancelImportTask	Grants permission to cancel an import from CloudTrail Lake to CloudWatch	Write			
CreateDelivery	Grants permission to create a delivery connecting a delivery source to a delivery destination	Write	delivery*		
			delivery-destination*		
			delivery-source*		
				aws:TagKeys aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey}	
CreateExportTask	Grants permission to create an ExportTask which allows you to efficiently export data from a Log Group to your Amazon S3 bucket	Write	log-group*		
CreateImportTask	Grants permission to start an asynchronous process to import data from a CloudTrail Lake event data store into a managed log group in CloudWatch	Write			
CreateLogAnomalyDetector	Grants permission to create a log anomaly detector	Write	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLogDelivery [permission only]	Grants permission to create the log delivery	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLogGroup	Grants permission to create a new log group with the specified name	Write	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLogStream	Grants permission to create a new log stream with the specified name	Write	log-stream*		
CreateScheduledQuery	Grants permission to create a scheduled query	Write	scheduled-query*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteAccountPolicy	Grants permission to delete an account policy	Write			
DeleteDataProtectionPolicy	Grants permission to delete a data protection policy attached to a log group	Write	log-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDelivery	Grants permission to delete a delivery	Write	delivery*		
DeleteDeliveryDestination	Grants permission to delete a delivery destination after all associated deliveries are deleted	Write	delivery-destination*		
DeleteDeliveryDestinationPolicy	Grants permission to delete a delivery destination policy associated with a delivery destination	Write	delivery-destination*		
DeleteDeliverySource	Grants permission to delete a delivery source after all associated deliveries are deleted	Write	delivery-destination*		
DeleteDestination	Grants permission to delete the destination with the specified name	Write	destination*		
DeleteIndexPolicy	Grants permission to delete an index policy attached to a log group	Write			
DeleteIntegration	Grants permission to delete the integration	Write			
DeleteLogAnomalyDetector	Grants permission to delete a log anomaly detector	Write	anomaly-detector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLogDelivery [permission only]	Grants permission to delete the log delivery information for specified log delivery	Write			
DeleteLogGroup	Grants permission to delete the log group with the specified name	Write	log-group*		
DeleteLogStream	Grants permission to delete a log stream	Write	log-stream*		
DeleteMetricFilter	Grants permission to delete a metric filter associated with the specified log group	Write	log-group*		
DeletePipelineRule [permission only]	Grants permission to delete telemetry pipeline	Write			
DeleteQueryDefinition	Grants permission to delete a saved CloudWatch Logs Insights query definition	Write			
DeleteResourcePolicy	Grants permission to delete a resource policy from this account	Permissions management			
DeleteRetentionPolicy	Grants permission to delete the retention policy of the specified log group	Write	log-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteScheduledQuery	Grants permission to delete a scheduled query	Write	scheduled-query*		
DeleteSubscriptionFilter	Grants permission to delete a subscription filter associated with the specified log group	Write	log-group*		
DeleteTransformer	Grants permission to delete a transformer associated with the specified log group	Write	log-group*		
DescribeAccountPolicies	Grants permission to retrieve account policies	List			
DescribeConfigurationTemplates	Grants permission to retrieve a list of configuration templates of available log types	List			
DescribeDeliveries	Grants permission to retrieve a list of deliveries an account	List			
DescribeDeliveryDestinations	Grants permission to retrieve a list of delivery destinations an account	List			
DescribeDeliverySources	Grants permission to retrieve a list of delivery sources in an account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDestinations	Grants permission to return all the destinations that are associated with the AWS account making the request	List			
DescribeExportTasks	Grants permission to return all the export tasks that are associated with the AWS account making the request	List			
DescribeFieldIndexes	Grants permission to return all the indexing attributes that are attached with the log groups	List			
DescribeImportTaskBatches	Grants permission to return detailed information about the individual batches within an import task, including status and any error	List			
DescribeImportTasks	Grants permission to return all the import tasks associated with the AWS account making the request	List			
DescribeIndexPolicies	Grants permission to return all the index policies that are attached with the log groups	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLogGroups	Grants permission to return all the log groups that are associated with the AWS account making the request	List			
DescribeLogStreams	Grants permission to return all the log streams that are associated with the specified log group	List	log-group*		
DescribeMetricFilters	Grants permission to return all the metrics filters associated with the specified log group	List	log-group*		
DescribeQueries	Grants permission to return a list of CloudWatch Logs Insights queries that are scheduled, executing, or have been executed recently in this account	List			
DescribeQueryDefinitions	Grants permission to return a paginated list of your saved CloudWatch Logs Insights query definitions	List			
DescribeResourcePolicies	Grants permission to return all the resource policies in this account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSubscriptionFilters	Grants permission to return all the subscription filters associated with the specified log group	List	log-group*		
DisassociateKmsKey	Grants permission to disassociate the associated AWS Key Management Service (AWS KMS) customer master key (CMK) from the specified log group	Write	log-group*		
DisassociateSourceFromS3TableIntegration	Grants permission to disassociate a log source from an S3 Tables integration	Write			
FilterLogEvents	Grants permission to retrieve log events, optionally filtered by a filter pattern from the specified log group	Read	log-group*		
GetDataProtectionPolicy	Grants permission to retrieve a data protection policy attached to a log group	Read	log-group*		
GetDelivery	Grants permission to retrieve a single delivery	Read	delivery*		
GetDeliveryDestination	Grants permission to retrieve a single delivery destination	Read	delivery-destination*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDeliveryDestinationPolicy	Grants permission to retrieve a delivery destination policy attached to a delivery destination	Read	delivery-destination*		
GetDeliverySource	Grants permission to retrieve a single delivery source	Read	delivery-source*		
GetIntegration	Grants permission to retrieve a single integration	Read			
GetLogAnomalyDetector	Grants permission to get a log anomaly detector	Read	anomaly-detector*		
GetLogDelivery [permission only]	Grants permission to get the log delivery information for specified log delivery	Read			
GetLogEvents	Grants permission to retrieve log events from the specified log stream	Read	log-stream*		
GetLogFields	Grants permission to retrieve a list of log fields for a data source	Read			
GetLogGroupFields	Grants permission to return a list of the fields that are included in log events in the specified log group, along with the percentage of log events that contain each field	Read	log-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLogRecord	Grants permission to retrieve all the fields and values of a single log event	Read	log-group*		
GetQueryResults	Grants permission to return the results from the specified query	Read	log-group*		
GetScheduledQuery	Grants permission to retrieve information about a specified scheduled query	Read	scheduled-query*		
GetScheduledQueryHistory	Grants permission to return the execution history for a specified scheduled query	Read	scheduled-query*		
GetTransformer	Grants permission to return transformer associated with the specified log group	Read	log-group*		
IntegrateWithS3Table [permission only]	Grants permission to deliver log events to S3 Tables	Write	log-group*		
Link [permission only]	Grants permission to share CloudWatch resources with a monitoring account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAggregateLogGroupSummaries	Grants permission to return an aggregate summary of all log groups in the region grouped by specified data-source characteristics	List			
ListAnomalies	Grants permission to list all anomalies detected in the AWS account making the request	List	anomaly-detector		
ListEntitiesForLogGroup [permission only]	Grants permission to retrieve all the entities that are associated with log group	List			
ListIntegrations	Grants permission to list all integrations associated with the AWS account making the request	List			
ListLogAnomalyDetectors	Grants permission to return all the anomaly detectors that are associated with the AWS account making the request	List	anomaly-detector		
ListLogDeliveries [permission only]	Grants permission to list all the log deliveries for specified account and/or log source	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListLogGroups	Grants permission to return all the log groups that are associated with the AWS account making the request	List			
ListLogGroupsForEntity [permission only]	Grants permission to retrieve all the log groups that are associated with entity	List			
ListLogGroupsForQuery	Grants permission to return all the log groups that are associated with the specified query	List			
ListScheduledQueries	Grants permission to return all scheduled queries that are associated with the AWS account making the request	List			
ListSourcesForS3TableIntegration	Grants permission to return all log sources associated with an S3 Tables integration	List			
ListTagsForResource	Grants permission to list the tags for the specified resource	List	anomaly-detector		
			delivery		
			delivery-destination		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			delivery-source		
			destination		
			log-group		
ListTagsLogGroup	Grants permission to list the tags for the specified log group	List	log-group*		
ProcessWithPipeline [permission only]	Grants permission to process and transform log events through pipeline transformers before storage	Write	log-group*		
PutAccountPolicy	Grants permission to attach an account policy	Write			
PutDataProtectionPolicy	Grants permission to attach a data protection policy to detect and redact sensitive information from log events	Write	log-group*		
PutDeliveryDestination	Grants permission to create/update a delivery destination	Write	delivery-destination*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} logs:DeliveryDestinationResourceArn	
PutDeliveryDestinationPolicy	Grants permission to attach a delivery destination policy to a delivery destination	Write	delivery-destination*		
PutDeliverySource	Grants permission to create/update a delivery source	Write	delivery-source*		
				aws:TagKeys aws:RequestTag/${TagKey} logs:LogGeneratingResourceArns	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutDestination	Grants permission to create or update a Destination	Write	destination*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
PutDestinationPolicy	Grants permission to create or update an access policy associated with an existing Destination	Write	destination*		
PutIndexPolicy	Grants permission to attach an index policy at log group level to optimize search and query	Write			
PutIntegration	Grants permission to create integration between cloudwatch logs and opensearch	Write			
PutLogEvents	Grants permission to upload a batch of log events to the specified log stream	Write	log-stream*		
PutLogGroupDeletionProtection	Grants permission to enable or disable deletion protection for the specified log group	Write	log-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutMetricFilter	Grants permission to create or update a metric filter and associates it with the specified log group	Write	log-group*		
PutPipelineRule [permission only]	Grants permission to create telemetry pipeline	Write			
PutQueryDefinition	Grants permission to create or update a query definition	Write			
PutResourcePolicy	Grants permission to create or update a resource policy allowing other AWS services to put log events to this account	Permissions management			
PutRetentionPolicy	Grants permission to set the retention of the specified log group	Write	log-group*		
PutSubscriptionFilter	Grants permission to create or update a subscription filter and associates it with the specified log group	Write	log-group*		iam:PassRole
			destination		
PutTransformer	Grants permission to create or update a transformer and associates it with the specified log group	Write	log-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartLiveTail	Grants permission to start a Live Tail session in CloudWatch Logs	Read	log-group*		
StartQuery	Grants permission to schedule a query of a log group using CloudWatch Logs Insights	Read	log-group*		
StopLiveTail [permission only]	Grants permission to stop a Live Tail session that is in progress	Read			
StopQuery	Grants permission to stop a CloudWatch Logs Insights query that is in progress	Read			
TagLogGroup	Grants permission to add or update the specified tags for the specified log group	Tagging	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource	Grants permission to add or update the specified tags for the specified resource	Tagging	anomaly-detector		
			delivery		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			delivery-destination		
			delivery-source		
			destination		
			log-group		
			scheduled-query		
				aws:TagKeys aws:RequestTag/${TagKey}	
TestMetricFilter	Grants permission to test the filter pattern of a metric filter against a sample of log event messages	Read			
TestTransformer	Grants permission to test the transformer against a sample of log event messages	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Unmask [permission only]	Grants permission to fetch unmasked log events that have been redacted with a data protection policy	Read	log-group*		
UntagLogGroup	Grants permission to remove the specified tags from the specified log group	Tagging	log-group*		
				aws:TagKeys	
UntagResource	Grants permission to remove the specified tags from the specified resource	Tagging	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		
			destination		
			log-group		
			scheduled-query		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAnomaly	Grants permission to update an anomaly reported by a log anomaly detector	Write	anomaly-detector*		
UpdateDeliveryConfiguration	Grants permission to update configuration related to a delivery	Write	delivery*		
			delivery-destination*		
			delivery-source*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateLogAnomalyDetector	Grants permission to update a log anomaly detector	Write	anomaly-detector*		
UpdateLogDelivery [permission only]	Grants permission to update the log delivery information for specified log delivery	Write			
UpdateScheduledQuery	Grants permission to update a scheduled query	Write	scheduled-query*		

Resource types defined by Amazon CloudWatch Logs

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
log-group	`arn:${Partition}:logs:${Region}:${Account}:log-group:${LogGroupName}`	aws:ResourceTag/${TagKey}
log-stream	`arn:${Partition}:logs:${Region}:${Account}:log-group:${LogGroupName}:log-stream:${LogStreamName}`	aws:ResourceTag/${TagKey}
destination	`arn:${Partition}:logs:${Region}:${Account}:destination:${DestinationName}`	aws:ResourceTag/${TagKey}
delivery-source	`arn:${Partition}:logs:${Region}:${Account}:delivery-source:${DeliverySourceName}`	aws:ResourceTag/${TagKey}
delivery	`arn:${Partition}:logs:${Region}:${Account}:delivery:${DeliveryName}`	aws:ResourceTag/${TagKey}
delivery-destination	`arn:${Partition}:logs:${Region}:${Account}:delivery-destination:${DeliveryDestinationName}`	aws:ResourceTag/${TagKey}
anomaly-detector	`arn:${Partition}:logs:${Region}:${Account}:anomaly-detector:${DetectorId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
scheduled-query	arn:${Partition}:logs:${Region}:${Account}:scheduled-query:${ScheduledQueryId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon CloudWatch Logs

Amazon CloudWatch Logs defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
logs:DeliveryDestinationResourceArn	Filters access by the Log Destination ARN passed in the request	ARN
logs:LogGeneratingResourceArns	Filters access by the Log Generating Resource ARNs passed in the request	ArrayOfARN

Actions, resources, and condition keys for Amazon CloudWatch Synthetics

Amazon CloudWatch Synthetics (service prefix: `synthetics`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon CloudWatch Synthetics
- Resource types defined by Amazon CloudWatch Synthetics
- Condition keys for Amazon CloudWatch Synthetics

Actions defined by Amazon CloudWatch Synthetics

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate Resource	Grants permission to associate a resource with a group	Write	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCanary	Grants permission to create a canary	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGroup	Grants permission to create a group	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCanary	Grants permission to delete a canary. Amazon Synthetics deletes all the resources except for the Lambda function and the CloudWatch Alarms if you created one	Write	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
DeleteGroup	Grants permission to delete a group	Write	group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeCanaries	Grants permission to list information of all canaries	Read		synthetics:Names	
DescribeCanariesLastRun	Grants permission to list information about the last test run associated with all canaries	Read		synthetics:Names	
DescribeRuntimeVersions	Grants permission to list information about Synthetics canary runtime versions	Read			
DisassociateResource	Grants permission to disassociate a resource from a group	Write	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetCanary	Grants permission to view the details of a canary	Read	canary*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetCanaryRuns	Grants permission to list information about all the test runs associated with a canary	Read	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
GetGroup	Grants permission to view the details of a group	Read	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListAssociatedGroups	Grants permission to list information about the associated groups of a canary	List	canary*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListGroupResources	Grants permission to list information about canaries in a group	List	group*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListGroups	Grants permission to list information of all groups	List			
ListTagsForResource	Grants permission to list all tags and values associated with a resource	Read	canary		
			group		
StartCanary	Grants permission to start a canary, so that Amazon CloudWatch Synthetics starts monitoring a website	Write	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartCanaryDryRun	Grants permission to start a canary dry run, so that Amazon CloudWatch Synthetics can execute a test execution of a canary with provided parameters	Write	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
StopCanary	Grants permission to stop a canary	Write	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
TagResource	Grants permission to add one or more tags to a resource	Tagging	canary		
			group		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove one or more tags from a resource	Tagging	canary		
			group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCanary	Grants permission to update a canary	Write	canary*		
				aws:ResourceTag/${TagKey} aws:TagKeys	

Resource types defined by Amazon CloudWatch Synthetics

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
canary	`arn:${Partition}:synthetics:${Region}:${Account}:canary:${CanaryName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
group	arn:${Partition}:synthetics:${Region}:${Account}:group:${GroupId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon CloudWatch Synthetics

Amazon CloudWatch Synthetics defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access based on the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access based on the tags associated with the resource	String
aws:TagKeys	Filters access based on the tag keys that are passed in the request	ArrayOfString
synthetics:Names	Filters access based on the name of the canary	ArrayOfString

Actions, resources, and condition keys for AWS Cost Explorer Service

AWS Cost Explorer Service (service prefix: ce) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Cost Explorer Service
- Resource types defined by AWS Cost Explorer Service
- Condition keys for AWS Cost Explorer Service

Actions defined by AWS Cost Explorer Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAnomalyMonitor	Grants permission to create a new Anomaly Monitor	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAnomalySubscription	Grants permission to create a new Anomaly Subscription	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCostCategoryDefinition	Grants permission to create a new Cost Category with the requested name and rules	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateNotificationSubscription [permission only]	Grants permission to create Reservation expiration alerts	Write			
CreateReport [permission only]	Grants permission to create Cost Explorer Reports	Write			
DeleteAnomalyMonitor	Grants permission to delete an Anomaly Monitor	Write	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
DeleteAnomalySubscription	Grants permission to delete an Anomaly Subscription	Write	anomalysubscription*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DeleteCostCategoryDefinition	Grants permission to delete a Cost Category	Write	costcategory*		
				aws:ResourceTag/${TagKey}	
DeleteNotificationSubscription [permission only]	Grants permission to delete Reservation expiration alerts	Write			
DeleteReport [permission only]	Grants permission to delete Cost Explorer Reports	Write			
DescribeCostCategoryDefinition	Grants permission to retrieve descriptions such as the name, ARN, rules, definition, and effective dates of a Cost Category	Read	costcategory*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeNotificationSubscription [permission only]	Grants permission to view Reservation expiration alerts	Read			
DescribeReport [permission only]	Grants permission to view Cost Explorer Reports page	Read			
GetAnomalies	Grants permission to retrieve anomalies	Read	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
GetAnomalyMonitors	Grants permission to query Anomaly Monitors	Read	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
GetAnomalySubscriptions	Grants permission to query Anomaly Subscriptions	Read	anomalysubscription*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetApproximateUsageRecords	Grants permission to retrieve approximate usage record count for the chosen resource, level, and hourly granularity preferences, derived from the past month's usage	Read			
GetCommitmentPurchaseAnalysis	Grants permission to retrieve the commitment purchase analysis for your account	Read			
GetConsoleActionSetEnforced [permission only]	Grants permission to view whether existing or fine-grained IAM actions are being used to control authorization to Billing, Cost Management, and Account consoles	Read			
GetCostAndUsage	Grants permission to retrieve the cost and usage metrics for your account	Read	billingview		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCostAndUsageComparisons	Grants permission to retrieve the cost and usage comparisons for your account	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetCostAndUsageWithResources	Grants permission to retrieve the cost and usage metrics with resources for your account	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetCostCategories	Grants permission to query Cost Catagory names and values for a specified time period	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetCostComparisonDrivers	Grants permission to retrieve the cost drivers for your account	Read	billingview		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCostForecast	Grants permission to retrieve a cost forecast for a forecast time period	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetDimensionValues	Grants permission to retrieve all available filter values for a filter for a period of time	Read	billingview		
				aws:ResourceTag/${TagKey}	
GetPreferences [permission only]	Grants permission to view Cost Explorer Preferences page	Read			
GetReservationCoverage	Grants permission to retrieve the reservation coverage for your account	Read			
GetReservationPurchaseRecommendation	Grants permission to retrieve the reservation recommendations for your account	Read			
GetReservationUtilization	Grants permission to retrieve the reservation utilization for your account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRightsizingRecommendation	Grants permission to retrieve the rightsizing recommendations for your account	Read			
GetSavingsPlanPurchaseRecommendationDetails	Grants permission to retrieve the Savings Plan recommendation details for your account	Read			
GetSavingsPlansCoverage	Grants permission to retrieve the Savings Plans coverage for your account	Read			
GetSavingsPlansPurchaseRecommendation	Grants permission to retrieve the Savings Plans recommendations for your account	Read			
GetSavingsPlansUtilization	Grants permission to retrieve the Savings Plans utilization for your account	Read			
GetSavingsPlansUtilizationDetails	Grants permission to retrieve the Savings Plans utilization details for your account	Read			
GetTags	Grants permission to query tags for a specified time period	Read	billingview		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetUsageForecast	Grants permission to retrieve a usage forecast for a forecast time period	Read	billingview		
				aws:ResourceTag/${TagKey}	
ListCommitmentPurchaseAnalyses	Grants permission to retrieve a list of your historical commitment purchase analyses	List			
ListCostAllocationTagBackfillHistory	Grants permission to list Cost Allocation Tag backfill history	List			
ListCostAllocationTags	Grants permission to list Cost Allocation Tags	List			
ListCostCategoryDefinitions	Grants permission to retrieve names, ARN, and effective dates for all Cost Categories	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCostCategoryResourceAssociations	Grants permission to retrieve resource associations of all Cost Categories defined in the account	List			
ListSavingsPlansPurchaseRecommendationGeneration	Grants permission to retrieve a list of your historical recommendation generations	List			
ListTagsForResource	Grants permission to list tags for a Cost Explorer resource	Read	anomalymonitor		
			anomalysubscription		
			costcategory		
				aws:ResourceTag/${TagKey}	
ProvideAnomalyFeedback	Grants permission to provide feedback on detected anomalies	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartCommitmentPurchaseAnalysis	Grants permission to request a commitment purchase analysis	Write			
StartCostAllocationTagBackfill	Grants permission to request a Cost Allocation Tag backfill	Write			
StartSavingsPlansPurchaseRecommendationGeneration	Grants permission to request a Savings Plans recommendation generation	Write			
TagResource	Grants permission to tag a Cost Explorer resource	Tagging	anomalymonitor		
			anomalysubscription		
			costcategory		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to remove tags from a Cost Explorer resource	Tagging	anomalymonitor		
			anomalysubscription		
			costcategory		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAnomalyMonitor	Grants permission to update an existing Anomaly Monitor	Write	anomalymonitor*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
UpdateAnomalySubscription	Grants permission to update an existing Anomaly Subscription	Write	anomalysubscription*		
				aws:ResourceTag/${TagKey}	
UpdateConsoleActionSetEnforced [permission only]	Grants permission to change whether existing or fine-grained IAM actions will be used to control authorization to Billing, Cost Management, and Account consoles	Write			
UpdateCostAllocationTagsStatus	Grants permission to update existing Cost Allocation Tags status	Write			
UpdateCostCategoryDefinition	Grants permission to update an existing Cost Category	Write	costcategory*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateNotification Subscription [permission only]	Grants permission to update Reservation expiration alerts	Write			
UpdatePreferences [permission only]	Grants permission to edit Cost Explorer Preferences page	Write			
UpdateReport [permission only]	Grants permission to update Cost Explorer Reports	Write			

Resource types defined by AWS Cost Explorer Service

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
anomalysubscription	`arn:${Partition}:ce::${Account}:anomalysubscription/${Identifier}`	aws:ResourceTag/${TagKey}
anomalymonitor	`arn:${Partition}:ce::${Account}:anomalymonitor/${Identifier}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
costcategory	arn:${Partition}:ce::${Account}:costcategory/${Identifier}	aws:ResourceTag/${TagKey}
billingview	arn:${Partition}:billing::${Account}:billingview/${ResourceId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Cost Explorer Service

AWS Cost Explorer Service defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Data Lifecycle Manager

Amazon Data Lifecycle Manager (service prefix: dlm) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Data Lifecycle Manager
- Resource types defined by Amazon Data Lifecycle Manager
- Condition keys for Amazon Data Lifecycle Manager

Actions defined by Amazon Data Lifecycle Manager

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLifecyclePolicy	Grants permission to create a data lifecycle policy to manage the scheduled creation and retention of Amazon EBS snapshots. You may have up to 100 policies	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteLifecyclePolicy	Grants permission to delete an existing data lifecycle policy. In addition, this action halts the creation and deletion of snapshots that	Write	policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	the policy specified. Existing snapshots are not affected				
GetLifecyclePolicies	Grants permission to returns a list of summary descriptions of data lifecycle policies	List			
GetLifecyclePolicy	Grants permission to return a complete description of a single data lifecycle policy	Read	policy*		
ListTagsForResource	Grants permission to list the tags associated with a resource	Read	policy*		
TagResource	Grants permission to add or update tags of a resource	Tagging	policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags associated with a resource	Tagging	policy*		
				aws:TagKeys	
UpdateLifecyclePolicy	Grants permission to update an existing data lifecycle policy	Write	policy*		

Resource types defined by Amazon Data Lifecycle Manager

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
policy	`arn:${Partition}:dlm:${Region}:${Account}:policy/${ResourceName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Data Lifecycle Manager

Amazon Data Lifecycle Manager defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS DataSync

AWS DataSync (service prefix: `datasync`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS DataSync
- Resource types defined by AWS DataSync
- Condition keys for AWS DataSync

Actions defined by AWS DataSync

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddStorageSystem	Grants permission to create a storage system	Write	agent*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CancelTaskExecution	Grants permission to cancel execution of a sync task	Write	taskexecution*		
				aws:ResourceTag/${TagKey}	
CreateAgent	Grants permission to activate an agent that you have deployed on your host	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationAzureBlob	Grants permission to create an endpoint for a Microsoft Azure Blob Storage container	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationEfs	Grants permission to create an endpoint for an Amazon EFS file system	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLocationFsxLustre	Grants permission to create an endpoint for an Amazon Fsx Lustre	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxOntap	Grants permission to create an endpoint for Amazon FSx for ONTAP	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxOpenZfs	Grants permission to create an endpoint for Amazon FSx for OpenZFS	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationFsxWindows	Grants permission to create an endpoint for an Amazon FSx Windows File Server file system	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLocationHdfs	Grants permission to create an endpoint for an Amazon Hdfs	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationNfs	Grants permission to create an endpoint for a NFS file system	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationObjectStorage	Grants permission to create an endpoint for a self-managed object storage bucket	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLocationS3	Grants permission to create an endpoint for an Amazon S3 bucket	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLocationSmb	Grants permission to create an endpoint for an SMB file system	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTask	Grants permission to create a sync task	Write	location*		
			agent		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAgent	Grants permission to delete an agent	Write	agent*		
DeleteLocation	Grants permission to delete a location used by AWS DataSync	Write	location*		
DeleteTask	Grants permission to delete a sync task	Write	task*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAgent	Grants permission to view metadata such as name, network interfaces, and the status (that is, whether the agent is running or not) about a sync agent	Read	agent*		
DescribeDiscoveryJob	Grants permission to describe metadata about a discovery job	Read	discovery job*		
DescribeLocationAzureBlob	Grants permission to view metadata, such as the path information about an Azure Blob Storage sync location	Read	location*		
DescribeLocationEfs	Grants permission to view metadata, such as the path information about an Amazon EFS sync location	Read	location*		
DescribeLocationFsxLustre	Grants permission to view metadata, such as the path information about an Amazon FSx Lustre sync location	Read	location*		
DescribeLocationFsxOntap	Grants permission to view metadata, such as the path information about an Amazon FSx for ONTAP sync location	Read	location*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLocationFsxOpenZfs	Grants permission to view metadata, such as the path information about an Amazon FSx OpenZFS sync location	Read	location*		
DescribeLocationFsxWindows	Grants permission to view metadata, such as the path information about an Amazon FSx Windows sync location	Read	location*		
DescribeLocationHdfs	Grants permission to view metadata, such as the path information about an Amazon HDFS sync location	Read	location*		
DescribeLocationNfs	Grants permission to view metadata, such as the path information, about a NFS sync location	Read	location*		
DescribeLocationObjectStorage	Grants permission to view metadata about a self-managed object storage server location	Read	location*		
DescribeLocationS3	Grants permission to view metadata, such as bucket name, about an Amazon S3 bucket sync location	Read	location*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLocationSmb	Grants permission to view metadata, such as the path information, about an SMB sync location	Read	location*		
DescribeStorageSystem	Grants permission to view metadata about a storage system	Read	storagesystem*		
DescribeStorageSystemResourceMetrics	Grants permission to describe resource metrics collected by a discovery job	List	discoveryjob*		
DescribeStorageSystemResources	Grants permission to describe resources identified by a discovery job	List	discoveryjob*		
DescribeTask	Grants permission to view metadata about a sync task	Read	task*		
DescribeTaskExecution	Grants permission to view metadata about a sync task that is being executed	Read	taskexecution*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateRecommendations	Grants permission to generate recommendations for a resource identified by a discovery job	Write	discoveryjob*		
ListAgents	Grants permission to list agents owned by an AWS account in a region specified in the request	List			
ListDiscoveryJobs	Grants permission to list discovery jobs	List			
ListLocations	Grants permission to list source and destination sync locations	List			
ListStorageSystems	Grants permission to list storage systems	List			
ListTagsForResource	Grants permission to list tags that have been added to the specified resource	Read	agent		
			discoveryjob		
			location		
			storagesystem		
			task		
			taskexecution		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTaskExecutions	Grants permission to list executed sync tasks	List		aws:ResourceTag/${TagKey}	
ListTasks	Grants permission to list of all the sync tasks	List			
RemoveStorageSystem	Grants permission to delete a storage system	Write	storagesystem*		
StartDiscoveryJob	Grants permission to start a discovery job for a storage system	Write	storagesystem*		
StartTaskExecution	Grants permission to start a specific invocation of a sync task	Write	task*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
StopDiscoveryJob	Grants permission to stop a discovery job	Write	discoveryjob*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to apply a key-value pair to an AWS resource	Tagging	agent		
			discovery job		
			location		
			storagesystem		
			task		
			taskexecution		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove one or more tags from the specified resource	Tagging	agent		
			discovery job		
			location		
			storagesystem		
			task		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			taskexecution		
				aws:TagKeys	
UpdateAgent	Grants permission to update the name of an agent	Write	agent*		
UpdateDiscoveryJob	Grants permission to update a discovery job	Write	discoveryjob*		
UpdateLocationAzureBlob	Grants permission to update an Azure Blob Storage sync location	Write	location*		
UpdateLocationEfs	Grants permission to update an EFS sync Location	Write	location*		
UpdateLocationFsxLustre	Grants permission to update an FSx Lustre sync Location	Write	location*		
UpdateLocationFsxOntap	Grants permission to update an FSx ONTAP sync Location	Write	location*		
UpdateLocationFsxOpenZfs	Grants permission to update an FSx OpenZFS sync Location	Write	location*		
UpdateLocationFsxWindows	Grants permission to update an FSx Windows sync Location	Write	location*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateLocationHdfs	Grants permission to update an HDFS sync Location	Write	location*		
UpdateLocationNfs	Grants permission to update an NFS sync Location	Write	location*		
UpdateLocationObjectStorage	Grants permission to update a self-managed object storage server location	Write	location*		
UpdateLocationS3	Grants permission to update an S3 sync Location	Write	location*		
UpdateLocationSmb	Grants permission to update a SMB sync location	Write	location*		
UpdateStorageSystem	Grants permission to update a storage system	Write	storagesystem*		
UpdateTask	Grants permission to update metadata associated with a sync task	Write	task*		
UpdateTaskExecution	Grants permission to update execution of a sync task	Write	taskexecution*		
				aws:ResourceTag/${TagKey}	

Resource types defined by AWS DataSync

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
agent	`arn:${Partition}:datasync:${Region}:${AccountId}:agent/${AgentId}`	aws:ResourceTag/${TagKey}
location	`arn:${Partition}:datasync:${Region}:${AccountId}:location/${LocationId}`	aws:ResourceTag/${TagKey}
task	`arn:${Partition}:datasync:${Region}:${AccountId}:task/${TaskId}`	aws:ResourceTag/${TagKey}
taskexecution	`arn:${Partition}:datasync:${Region}:${AccountId}:task/${TaskId}/execution/${ExecutionId}`	aws:ResourceTag/${TagKey}
storagesystem	`arn:${Partition}:datasync:${Region}:${AccountId}:system/${StorageSystemId}`	aws:ResourceTag/${TagKey}
discoveryjob	`arn:${Partition}:datasync:${Region}:${AccountId}:system/${StorageSystemId}/job/${DiscoveryJobId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS DataSync

AWS DataSync defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tag key-value pairs associated with the resource	String
aws:TagKeys	Filters access by the tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon EC2

Amazon EC2 (service prefix: ec2) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon EC2
- Resource types defined by Amazon EC2
- Condition keys for Amazon EC2

Actions defined by Amazon EC2

You can specify the following actions in the Action element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptAddressTransfer	Grants permission to accept an Elastic IP address transfer	Write	elastic-ip*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AllocationId ec2:Domain ec2:PublicIpAddress	ec2:CreateTags
				ec2:Region	
AcceptCapacityReservationBillingOwnership	Grants permission to accept assign billing of the available capacity of a shared Capacity Reservation to the calling account	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CapacityReservationFleet	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:CreateDate ec2:DestinationCapacityReservationId ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:OutpostArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptReservedInstancesExchangeQuote	Grants permission to accept a Convertible Reserved Instance exchange quote	Write	reserved-instances*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:InstanceType ec2:ReservedInstancesOfferingType ec2:ResourceTag/${TagKey} ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptTransitGatewayMulticastDomainAssociations	Grants permission to accept a request to associate subnets with a transit gateway multicast domain	Write	transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-multicast-domain	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptTransitGatewayPeeringAttachment	Grants permission to accept a transit gateway peering attachment request	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	
AcceptTransitGatewayVpcAttachment	Grants permission to accept a request to attach a VPC to a transit gateway	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
AcceptVpcEndpointConnections	Grants permission to accept one or more interface VPC endpoint connections to your VPC endpoint service	Write	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptVpcPeeringConnection	Grants permission to accept a VPC peering connection request	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
			vpc-peering-connection*	aws:ResourceTag/${TagKey} ec2:AccepterVpc ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
AdvertiseByoipCidr	Grants permission to advertise an IP address range that is provisioned for use in AWS through bring your own IP addresses (BYOIP)	Write		ec2:Region	
AllocateAddress	Grants permission to allocate an Elastic IP address (EIP) to your account	Write	elastic-ip*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv4pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllocateHosts	Grants permission to allocate a Dedicated Host to your account	Write	dedicated-host*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AutoPlacement ec2:AvailabilityZone ec2:HostRecovery ec2:InstanceType ec2:Quantity	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllocateIpamPoolCidr	Grants permission to allocate a CIDR from an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ApplySecurityGroupsToClientVpnTargetNetwork	Grants permission to apply a security group to the association between a Client VPN endpoint and a target network	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssignIpv6Addresses	Grants permission to assign one or more IPv6 addresses to a network interface	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssignPrivateIpAddresses	Grants permission to assign one or more secondary private IP addresses to a network interface	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssignPrivateNatGatewayAddress	Grants permission to assign one or more secondary private IP addresses to a private NAT gateway	Write	natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
AssociateAddress	Grants permission to associate an Elastic IP address (EIP) with an instance or a network interface	Write	elastic-ip	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateCapacityReservationBillingOwner	Grants permission to assign billing of the unused capacity of a shared Capacity Reservation to a consumer account	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CapacityReservationFleet ec2:CreateDate ec2:DestinationCapacityReservationId ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:OutpostArn ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateClientVpnTargetNetwork	Grants permission to associate a target network with a Client VPN endpoint	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID	
				ec2:Region	
AssociateDhcpOptions	Grants permission to associate or disassociate a set of DHCP options with a VPC	Write	dhcp-options*	aws:ResourceTag/${TagKey} ec2:DhcpOptionsID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
AssociateEnclaveCertificateIamRole	Grants permission to associate an ACM certificate with an IAM role to be used in an EC2 Enclave	Write	certificate*		
			role*		
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateIamInstanceProfile	Grants permission to associate an IAM instance profile with a running or stopped instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
AssociateInstanceEventWindow	Grants permission to associate one or more targets with an event window	Write	instance-event-window*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
AssociateIpamByoasn	Grants permission to associate an Autonomous System Number (ASN) with a BYOIP CIDR	Write		ec2:Region	
AssociateIpamResourceDiscovery	Grants permission to associate an IPAM resource discovery with an Amazon VPC IPAM	Write	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-resource-discovery-association*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	
AssociateNatGatewayAddress	Grants permission to associate an Elastic IP address and private IP address with a public Nat gateway	Write	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
AssociateRouteServer	Grants permission to associate a route server with a VPC	Write	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate RouteTable	Grants permission to associate a subnet or gateway with a route table	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
			internet-gateway	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv4pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
AssociateSecurityGroupVpc	Grants permission to associate a security group with another VPC in the same Region	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateSubnetCidrBlock	Grants permission to associate a CIDR block with a subnet	Write	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Ipv6IpamPoolId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateTransitGatewayMulticastDomain	Grants permission to associate an attachment and list of subnets with a transit gateway multicast domain	Write	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateTransitGatewayPolicyTable	Grants permission to associate a policy table with a transit gateway attachment	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-policy-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateTransitGatewayRouteTable	Grants permission to associate an attachment with a transit gateway route table	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateTrunkInterface	Grants permission to associate a branch network interface with a trunk network interface	Write		ec2:Region	
AssociateVerifiedAccessInstanceWebAcl [permission only]	Grants permission to associate an AWS Web Application Firewall (WAF) web access control list (ACL) with a Verified Access instance	Write	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate VpcCidrBlock	Grants permission to associate a CIDR block with a VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv6pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
AttachAppliance ToNatGateway [permission only]	Grants permission to attach an appliance with a public/private Natgateway	Permissions management	natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachClassicLinkVpc	Grants permission to link an EC2-Classic instance to a ClassicLink-enabled VPC through one or more of the VPC's security groups	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
			security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
AttachInternetGateway	Grants permission to attach an internet gateway to a VPC	Write	internet-gateway*	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachNetworkInterface	Grants permission to attach a network interface to an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachVerifiedAccessTrustProvider	Grants permission to attach a trust provider to a Verified Access instance	Write	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			verified-access-trust-provider*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachVolume	Grants permission to attach an EBS volume to a running or stopped instance and expose it to the instance with the specified device name	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:VolumeID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachVpnGateway	Grants permission to attach a virtual private gateway to a VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
			vpn-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AuthorizeClientVpnIngress	Grants permission to add an inbound authorization rule to a Client VPN endpoint	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
AuthorizeSecurityGroupEgress	Grants permission to add one or more outbound rules to a VPC security group. Policies using the security-group-rule resource-level permission are only enforced when the API request includes TagSpecifications	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	ec2:CreateTags
			security-group-rule	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AuthorizeSecurityGroupIngress	Grants permission to add one or more inbound rules to a VPC security group. Policies using the security-group-rule resource-level permission are only enforced when the API request includes TagSpecifications	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	ec2:CreateTags
			security-group-rule	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	
BundleInstance	Grants permission to bundle an instance store-backed Windows instance	Write		ec2:Region	
CancelBundleTask	Grants permission to cancel a bundling operation	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelCapacityReservation	Grants permission to cancel a Capacity Reservation and release the reserved capacity	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:CapacityReservationFleet	
				ec2:Region	
CancelCapacityReservationFleets	Grants permission to cancel one or more Capacity Reservation Fleets	Write	capacity-reservation-fleet*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CancelCapacityReservation
				ec2:Region	
CancelConversionTask	Grants permission to cancel an active conversion task	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelDeclarativePoliciesReport	Grants permission to cancel a declarative policies report	Write	declarative-policies-report*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CancelExportTask	Grants permission to cancel an active export task	Write	export-image-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			export-instance-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
CancelImageLaunchPermission	Grants permission to remove your AWS account from the launch permissions for the specified AMI	Permissions management	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelImportTask	Grants permission to cancel an in-process import virtual machine or import snapshot task	Write	import-image-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			import-snapshot-task	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CancelReservedInstancesListing	Grants permission to cancel a Reserved Instance listing on the Reserved Instance Marketplace	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelSpotFleetRequests	Grants permission to cancel one or more Spot Fleet requests	Write	spot-fleet-request*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CancelSpotInstanceRequests	Grants permission to cancel one or more Spot Instance requests	Write	spot-instances-request*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ConfirmProductInstance	Grants permission to determine whether an owned product code is associated with an instance	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CopyFpgaImage	Grants permission to copy a source Amazon FPGA image (AFI) to the current Region. Resource-level permissions specified for this action apply to the new AFI only. They do not apply to the source AFI	Write	fpga-image*	ec2:Owner	
				ec2:Region	
CopyImage	Grants permission to copy an Amazon Machine Image (AMI) from a source Region to the current Region	Write	image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ImageID ec2:Owner	ec2:CreateTags
			snapshot*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CopySnapshot	Grants permission to copy a point-in-time snapshot of an EBS volume and store it in Amazon S3. Resource-level permissions specified for this action apply to both the snapshot copy and the source snapshot	Write	snapshot*	aws:RequestTag/${TagKey} aws:TagKeys ec2:Encrypted ec2:OutpostArn ec2:Owner ec2:ParentSnapshot ec2:ParentVolume ec2:ProductCode ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CopyVolumes	Grants permission to create a copy of an EBS volume. Resource-level permissions specified for this action apply to the source and copied volume. Condition keys for the copied volume correspond to parameters specified in the CopyVolumes API request	Write	volume*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume ec2:VolumeInitializationRate	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	
CreateCapacityManagerDataExport	Grants permission to create a new S3 Data Export for Capacity Manager	Write	capacity-manager-data-export*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCapacityReservation	Grants permission to create a Capacity Reservation	Write	capacity-reservation*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CapacityReservationFleet ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:EphemeralStorage	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceCount ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:OutpostArn ec2:PlacementGroup ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCapacityReservationBySplitting	Grants permission to create a new Capacity Reservation by splitting the available capacity of the source Capacity Reservation	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CapacityReservationFleet ec2:CreateDate ec2:DestinationCapacityReservationId ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:OutpostArn ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCapacityReservationFleet	Grants permission to create a Capacity Reservation Fleet	Write	capacity-reservation-fleet*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateCapacityReservation ec2:CreateTags ec2:DescribeCapacityReservations ec2:DescribeInstances
				ec2:Region	
CreateCarrierGateway	Grants permission to create a carrier gateway and provides CSP connectivity to VPC customers	Write	carrier-gateway*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateClientVpnEndpoint	Grants permission to create a Client VPN endpoint	Write	client-vpn-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:SamlProviderArn ec2:ServerCertificateArn	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID	
			vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateClientVpnRoute	Grants permission to add a network route to a Client VPN endpoint's route table	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID	
				ec2:Region	
CreateCoipCidr	Grants permission to create a range of customer-owned IP (CoIP) addresses	Write	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCoipPool	Grants permission to create a pool of customer-owned IP (CoIP) addresses	Write	coip-pool*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateCoipPoolPermission [permission only]	Grants permission to allow a service to access a customer-owned IP (CoIP) pool	Permissions management	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCustomerGateway	Grants permission to create a customer gateway, which provides information to AWS about your customer gateway device	Write	customer-gateway*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	
CreateDefaultSubnet	Grants permission to create a default subnet in a specified Availability Zone in a default VPC	Write		ec2:Region	
CreateDefaultVpc	Grants permission to create a default VPC with a default subnet in each Availability Zone	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDelegateMacVolumeOwnershipTask	Grants permission to create a volume ownership delegation task for an Apple silicon Mac instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceMarketType ec2:InstanceMetadataTags	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			mac-modification-task*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	
CreateDhcpOptions	Grants permission to create a set of DHCP options for a VPC	Write	dhcp-options*	aws:RequestTag/${TagKey} aws:TagKeys ec2:DhcpOptionsID	ec2:CreateTags
				ec2:Region	
CreateEgressOnlyInternetGateway	Grants permission to create an egress-only internet gateway for a VPC	Write	egress-only-internet-gateway*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFleet	Grants permission to launch an EC2 Fleet. Resource-level permissions for this action do not include the resources specified in a launch template. To specify resource-level permissions for resources specified in a launch template, you must include the resources in the RunInstances action statement	Write	fleet*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			instance*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceBandwi	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				dthWeighting ec2:InstanceID ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
			launch-template	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:KmsKeyId ec2:ParentSnapshot ec2:VolumeID ec2:VolumeIops ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	
CreateFlowLogs	Grants permission to create one or more flow logs to capture IP traffic for a network interface	Write	vpc-flow-log*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags ecs:ListClusters ecs:ListContainerInstances ecs:ListServices ecs:ListTaskDefinitions ecs:ListTasks iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			natgateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Vpc	
			network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
			transit-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFpgaImage	Grants permission to create an Amazon FPGA Image (AFI) from a design checkpoint (DCP)	Write	fpga-image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:Owner ec2:Public	ec2:CreateTags
				ec2:Region	
CreateImage	Grants permission to create an Amazon EBS-backed AMI from a stopped or running Amazon EBS-backed instance. This action can reboot instances as part of the image creation process, even without RebootInstances permissions. To prevent instance reboots during image creation, use the NoReboot parameter	Write	image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ImageID ec2:Owner	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot*	aws:RequestTag/${TagKey} aws:TagKeys ec2:OutpostArn ec2:ParentVolume ec2:SnapshotID ec2:SnapshotTime ec2:SourceOutpostArn ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateImageUsageReport	Grants permission to create an AMI usage report	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	ec2:CreateTags
			image-usage-report*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInstanceConnectEndpoint	Grants permission to create an EC2 Instance Connect Endpoint that allows you to connect to an instance without a public IPv4 address	Write	instance-connect-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys ec2:SubnetID	ec2:CreateTags
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	
CreateInstanceEventWindow	Grants permission to create an event window in which scheduled events for the associated Amazon EC2 instances can run	Write	instance-event-window*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInstanceExportTask	Grants permission to export a running or stopped instance to an Amazon S3 bucket	Write	export-instance-task*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ProductCode	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
CreateInternetGateway	Grants permission to create an internet gateway for a VPC	Write	internet-gateway*	aws:RequestTag/${TagKey} aws:TagKeys ec2:InternetGatewayID	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInterruptibleCapacityReservationAllocation	Grants permission to create an interruptible Capacity Reservation by specifying the number of unused instances you want to allocate from your source reservation	Write	capacity-reservation*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CreateDate ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount ec2:InstanceMatchCriteria	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstancePlatform ec2:InstanceType ec2:InterruptibleCapacityReservationId ec2:InterruptionType ec2:IsInterruptible ec2:SourceCapacityReservationId ec2:TargetInstanceCount ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
CreateIpam	Grants permission to create an Amazon VPC IP Address Manager (IPAM)	Write	ipam*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags iam:CreateServiceLinkedRole
				ec2:Region	
CreateIpamExternalResourceVerificationToken	Grants permission to create a verification token, which proves ownership of an external resource	Write	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			ipam-external-resource-verification-token*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateIpamPolicy	Grants permission to create a policy in Amazon VPC IP Address Manager (IPAM) that defines rules for allocating public IPv4 addresses from IPAM pools to AWS resources	Write	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			ipam-policy*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	
CreateIpamPool	Grants permission to create an IP address pool for Amazon VPC IP Address Manager (IPAM), which is a collection of contiguous IP address CIDRs	Write	ipam-pool*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateIpamPrefixListResolver	Grants permission to create an IPAM prefix list resolver that defines rules for selecting CIDRs to include in prefix lists	Write	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			ipam-prefix-list-resolver*	aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-scope	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateIpamPrefixListResolverTarget	Grants permission to create an IPAM prefix list resolver target that links a resolver to a managed prefix list	Write	ipam-prefix-list-resolver*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			ipam-prefix-list-resolver-target*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateIpamResourceDiscovery	Grants permission to create an IPAM resource discovery	Write	ipam-resource-discovery*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags iam:CreateServiceLinkedRole
				ec2:Region	
CreateIpamScope	Grants permission to create an Amazon VPC IP Address Manager (IPAM) scope, which is the highest-level container within IPAM	Write	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			ipam-scope*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateKeyPair	Grants permission to create a 2048-bit RSA key pair	Write	key-pair*	aws:RequestTag/${TagKey} aws:TagKeys ec2:KeyPairType	ec2:CreateTags
				ec2:Region	
CreateLaunchTemplate	Grants permission to create a launch template	Write	launch-template*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags ssm:GetParameters
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLaunchTemplateVersion	Grants permission to create a new version of a launch template	Write	launch-template*	aws:ResourceTag/${TagKey} ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	ssm:GetParameters
				ec2:Region	
CreateLocalGatewayRoute	Grants permission to create a static route for a local gateway route table	Write	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-virtual-interface-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			prefix-list	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateLocalGatewayRouteTable	Grants permission to create a local gateway route table	Write	local-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			local-gateway-route-table*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLocalGatewayRouteTablePermission [permission only]	Grants permission to allow a service to access a local gateway route table	Permissions management	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateLocalGatewayRouteTableVirtualInterfaceGroupAssociation	Grants permission to create a local gateway route table virtual interface group association	Write	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			local-gateway-route-table-virtual-interface-group-association*	aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-virtual-interface-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateLocalGatewayRouteTableVpcAssociation	Grants permission to associate a VPC with a local gateway route table	Write	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			local-gateway-route-table-vpc-association*	aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
CreateLocalGatewayVirtualInterface	Grants permission to create a local gateway virtual interface	Write	local-gateway-virtual-interface*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-virtual-interface-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			outpost-lag*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateLocalGatewayVirtualInterfaceGroup	Grants permission to create a local gateway virtual interface group	Write	local-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-virtual-interface-group*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMacSystemIntegrityProtectionModificationTask	Grants permission to create a System Integrity Protection (SIP) modification task for an Amazon EC2 Mac instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceMarketType ec2:InstanceMetadataTags	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			mac-modification-task*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	
CreateManagedPrefixList	Grants permission to create a managed prefix list	Write	prefix-list*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	
CreateNatGateway	Grants permission to create a NAT gateway in a subnet	Write	natgateway*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			elastic-ip	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc	aws:ResourceTag/${TagKey} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
CreateNetworkAcl	Grants permission to create a network ACL in a VPC	Write	network-acl*	aws:RequestTag/${TagKey} aws:TagKeys ec2:NetworkAclID	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
CreateNetworkAclEntry	Grants permission to create a numbered entry (a rule) in a network ACL	Write	network-acl*	aws:ResourceTag/${TagKey} ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
CreateNetworkInsightsAccessScope	Grants permission to create a Network Access Scope	Write	network-insights-access-scope*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	
CreateNetworkInsightsPath	Grants permission to create a path to analyze for reachability	Write	network-insights-path*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
			internet-gateway	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	
			vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpc-endpoint-service	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-peering-connection	aws:ResourceTag/${TagKey} ec2:AccepterVpc ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateNetworkInterface	Grants permission to create a network interface in a subnet	Write	network-interface*	aws:RequestTag/${TagKey} aws:TagKeys ec2:NetworkInterfaceID	ec2:CreateTags
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateNetworkInterfacePermission	Grants permission to create a permission for an AWS-authorized user to perform certain operations on a network interface	Permissions management	network-interface*	aws:ResourceTag/${TagKey} ec2:AuthorizedService ec2:AuthorizedUser ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/${TagKey} ec2:Subnet	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Vpc	
				ec2:Region	
CreateOdbNetworkPeering [permission only]	Grants permission to allow Oracle Database@AWS to create a peering connection between an ODB network and a VPC	Permissions management	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePlacementGroup	Grants permission to create a placement group	Write	placement-group*	aws:RequestTag/${TagKey} aws:TagKeys ec2:PlacementGroupName ec2:PlacementGroupStrategy	ec2:CreateTags
				ec2:Region	
CreatePublicIpv4Pool	Grants permission to create a public IPv4 address pool for public IPv4 CIDRs that you own and bring to Amazon to manage with Amazon VPC IP Address Manager (IPAM)	Write	ipv4pool-ec2*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateReplaceRootVolumeTask	Grants permission to create a root volume replacement task	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
			replace-root-volume-task*	aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume*	aws:RequestTag/${TagKey} aws:TagKeys ec2:VolumeID ec2:VolumeInitializationRate	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:ResourceTag/${TagKey} ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	
CreateReservedInstancesListing	Grants permission to create a listing for Standard Reserved Instances to be sold in the Reserved Instance Marketplace	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRestoreImageTask	Grants permission to start a task that restores an AMI from an S3 object previously created by using CreateStoreImageTask	Write	image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ImageID ec2:Owner	ec2:CreateTags
				ec2:Region	
CreateRoute	Grants permission to create a route in a VPC route table	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRouteServer	Grants permission to create a route server	Write	route-server*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags sns:CreateTopic
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRouteServerEndpoint	Grants permission to create a route server endpoint	Write	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeSecurityGroups

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-server-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone	
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
CreateRouteServerPeer	Grants permission to create a route server peer	Write	route-server-endpoint*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey}	ec2:AuthorizeSecurityGroupIngress ec2:CreateTags
			route-server-peer*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRouteTable	Grants permission to create a route table for a VPC	Write	route-table*	aws:RequestTag/${TagKey} aws:TagKeys ec2:RouteTableID	ec2:CreateTags
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSecurityGroup	Grants permission to create a security group	Write	security-group*	aws:RequestTag/${TagKey} aws:TagKeys ec2:SecurityGroupID	ec2:CreateTags
			vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSnapshot	Grants permission to create a snapshot of an EBS volume and store it in Amazon S3	Write	snapshot*	aws:RequestTag/${TagKey} aws:TagKeys ec2:Location ec2:OutpostArn ec2:ParentVolume ec2:SnapshotID ec2:SourceAvailabilityZone ec2:SourceOutpostArn ec2:VolumeSize	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeInitializationRate ec2:VolumeIops	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSnapshots	Grants permission to create crash-consistent snapshots of multiple EBS volumes and store them in Amazon S3	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceProfile ec2:InstanceType ec2:PlacementGroup	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot*	aws:RequestTag/${TagKey} aws:TagKeys ec2:Location ec2:OutpostArn ec2:ParentVolume ec2:SnapshotID ec2:SourceAvailabilityZone ec2:SourceOutpostArn ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
CreateSpotDatafeedSubscription	Grants permission to create a data feed for Spot Instances to view Spot Instance usage logs	Write		ec2:Region	
CreateStoreImageTask	Grants permission to store an AMI as a single object in an S3 bucket	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSubnet	Grants permission to create a subnet in a VPC	Write	subnet*	aws:RequestTag/${TagKey} aws:TagKeys ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:SubnetID	ec2:CreateTags
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSubnetCidrReservation	Grants permission to create a subnet CIDR reservation	Write	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTags	Grants permission to add or overwrite one or more tags for Amazon EC2 resources	Tagging	capacity-block	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			capacity-manager-data-export	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	
			capacity-reservation	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			capacity-reservation-fleet	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			carrier-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			client-vpn-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:SamlProviderArn ec2:ServerCertificateArn	
			coip-pool	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			customer-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			declarative-policies-report	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			dedicated-host	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AutoPlacement ec2:AvailabilityZone ec2:HostRecovery ec2:InstanceType ec2:Quantity ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			dhcp-options	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:DhcpOptionsID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			egress-only-internet-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			elastic-gpu	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ElasticGpuType ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			elastic-ip	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			export-image-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			export-instance-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			fleet	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			fpga-image	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Owner ec2:Public ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			host-reservation	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image-usage-report	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			import-image-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			import-snapshot-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwi	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				dthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance-connect-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:SubnetID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance-event-window	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			internet-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-external-resource-verification-token	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-policy	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-pool	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-prefix-list-resolver	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-prefix-list-resolver-target	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-resource-discovery	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-resource-discovery-association	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-scope	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv4pool-ec2	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv6pool-ec2	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			key-pair	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:KeyPairName ec2:KeyPairType ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			launch-template	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-route-table	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-route-table-virtual-interface-group-association	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-route-table-vpc-association	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-virtual-interface	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-virtual-interface-group	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			natgateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-acl	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-insights-access-scope	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-insights-access-scope-analysis	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-insights-analysis	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-insights-path	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AuthorizedUser ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} ec2:Subnet ec2:Vpc	
			placement-group	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			prefix-list	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:IpamPrefixListResolverTargetId ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			replace-root-volume-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			reserved-instances	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:InstanceType ec2:ReservedInstancesOfferingType ec2:ResourceTag/${TagKey} ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-server	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-server-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-server-peer	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-table	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group-rule	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			spot-fleet-request	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			spot-instances-request	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet-cidr-reservation	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-filter	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-filter-rule	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-session	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-target	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:transitGatewayId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-connect-peer	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:transitGatewayConnectPeerId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-metering-policy	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:transitGatewayMeteringPolicyId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-multicast-domain	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-policy-table	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table-announcement	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableAnnouncementId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-endpoint-target	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-group	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-instance	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-policy	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-trust-provider	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-block-public-access-exclusion	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-encryption-control	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint-connection	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint-service	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceServiceRegion ec2:VpceSupportedRegion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint-service-permission	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-flow-log	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-peering-connection	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AccepterVpc ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-concentrator	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-connection	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AuthenticationType ec2:DPDTimeoutSeconds ec2:GatewayType ec2:IKEVersions ec2:InsideTunnelCidr ec2:InsideTunnelIpv6Cidr	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Phase1DHGroup ec2:Phase1EncryptionAlgorithms ec2:Phase1IntegrityAlgorithms ec2:Phase1LifetimeSeconds ec2:Phase2DHGroup ec2:Phase2EncryptionAlgorithms ec2:Phase2IntegrityAlgorithms ec2:Phase2LifetimeSeconds	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:RekeyFuzzPercentage ec2:RekeyMarginTimeSeconds ec2:ReplayWindowSizePackets ec2:ResourceTag/${TagKey} ec2:RoutingType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	
				ec2:CreateAction ec2:Region	
CreateTrafficMirrorFilter	Grants permission to create a traffic mirror filter	Write	traffic-mirror-filter*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTrafficMirrorFilterRule	Grants permission to create a traffic mirror filter rule	Write	traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			traffic-mirror-filter-rule*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTrafficMirrorSession	Grants permission to create a traffic mirror session	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			traffic-mirror-session*	aws:RequestTag/${TagKey} aws:TagKeys	
			traffic-mirror-target*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTrafficMirrorTarget	Grants permission to create a traffic mirror target	Write	traffic-mirror-target*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			network-interface	aws:ResourceTag/${TagKey} ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceServiceName ec2:VpceServiceOwner	
				ec2:Region	
CreateTransitGateway	Grants permission to create a transit gateway	Write	transit-gateway*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayId	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
CreateTransitGatewayConnect	Grants permission to create a Connect attachment from a specified transit gateway attachment	Write	transit-gateway-attachment*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayAttachmentId	ec2:CreateTags
				ec2:Region	
CreateTransitGatewayConnectPeer	Grants permission to create a Connect peer between a transit gateway and an appliance	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-connect-peer*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayConnectPeerId	
				ec2:Region	
CreateTransitGatewayMeteringPolicy	Grants permission to create a metering policy for a transit gateway	Write	transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-metering-policy*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayMeteringPolicyId	
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTransitGatewayMeteringPolicyEntry	Grants permission to create an entry for a transit gateway metering policy	Write	transit-gateway-metering-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMeteringPolicyId	
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTransitGatewayMulticastDomain	Grants permission to create a multicast domain for a transit gateway	Write	transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	ec2:CreateTags
			transit-gateway-multicast-domain*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTransitGatewayPeeringAttachment	Grants permission to request a transit gateway peering attachment between a requester and accepter transit gateway	Write	transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	ec2:CreateTags
			transit-gateway-attachment*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayAttachmentId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTransitGatewayPolicyTable	Grants permission to create a transit gateway policy table	Write	transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	ec2:CreateTags
			transit-gateway-policy-table*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayPolicyTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTransitGatewayPrefixListReference	Grants permission to create a transit gateway prefix list reference	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	
CreateTransitGatewayRoute	Grants permission to create a static route for a transit gateway route table	Write	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	
CreateTransitGatewayRouteTable	Grants permission to create a route table for a transit gateway	Write	transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayRouteTableId	
				ec2:Region	
CreateTransitGatewayRouteTableAnnouncement	Grants permission to create an announcement for a transit gateway route table	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
			transit-gateway-route-table-announcement*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayRouteTableAnnouncementId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTransitGatewayVpcAttachment	Grants permission to attach a VPC to a transit gateway	Write	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	ec2:CreateTags
			transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayAttachmentId	
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVerifiedAccessEndpoint	Grants permission to create a Verified Access endpoint	Write	verified-access-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			verified-access-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:ResourceTag/${TagKey} ec2:AuthorizedUser ec2:AvailabilityZone ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	
CreateVerifiedAccessGroup	Grants permission to create a Verified Access group	Write	verified-access-group*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateVerifiedAccessInstance	Grants permission to create a Verified Access instance	Write	verified-access-instance*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	
CreateVerifiedAccessTrustProvider	Grants permission to create a verified trust provider	Write	verified-access-trust-provider*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVolume	Grants permission to create an EBS volume	Write	volume*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:KmsKeyId ec2:ParentSnapshot ec2:VolumeID ec2:VolumeInitializationRate	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVpc	Grants permission to create a VPC with a specified CIDR block	Write	vpc*	aws:RequestTag/${TagKey} aws:TagKeys ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:VpcID	ec2:CreateTags
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv6pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateVpcBlockPublicAccessExclusion	Grants permission to create an exclusion list for blocked public access on a VPC	Write	vpc-block-public-access-exclusion*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc	aws:ResourceTag/${TagKey} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVpcEncryptionControl	Grants permission to create a VPC Encryption Control	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	ec2:CreateTags
			vpc-encryption-control*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVpcEndpoint	Grants permission to create a VPC endpoint for an AWS service	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpcID	ec2:CreateTags ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs route53:AssociateVPCWithHostedZone

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys ec2:VpceMultiRegion ec2:VpcePrivateDnsPreference ec2:VpcePrivateDnsSpecifiedDomains ec2:VpceServiceName ec2:VpceServiceOwner ec2:VpceServiceRegion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SubnetID	
				ec2:Region	
CreateVpcEndpointConnectionNotification	Grants permission to create a connection notification for a VPC endpoint or VPC endpoint service	Write	vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint-service	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceServiceRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVpcEndpointServiceConfiguration	Grants permission to create a VPC endpoint service configuration to which service consumers (AWS accounts, IAM users, and IAM roles) can connect	Write	vpc-endpoint-service*	aws:RequestTag/${TagKey} aws:TagKeys ec2:VpceMultiRegion ec2:VpceServicePrivateDnsName ec2:VpceServiceRegion	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVpcPeeringConnection	Grants permission to request a VPC peering connection between two VPCs	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	ec2:CreateTags
			vpc-peering-connection*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AccepterVpc ec2:RequesterVpc ec2:VpcPeeringConnectionID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
CreateVpnConcentrator	Grants permission to create a VPN concentrator that aggregates multiple VPN connections to a transit gateway	Write	vpn-concentrator*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			transit-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVpnConnection	Grants permission to create a VPN connection between a virtual private gateway or transit gateway and a customer gateway	Write	customer-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-connection*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AuthenticationType ec2:DPDTimeoutSeconds ec2:GatewayType ec2:IKEVersions ec2:InsideTunnelCidr ec2:InsideTunnelIpv6Cidr ec2:Phase1DHGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Phase1EncryptionAlgorithms ec2:Phase1IntegrityAlgorithms ec2:Phase1LifetimeSeconds ec2:Phase2DHGroup ec2:Phase2EncryptionAlgorithms ec2:Phase2IntegrityAlgorithms ec2:Phase2LifetimeSeconds ec2:RekeyFuzzPercentage	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:RekeyMarginTimeSeconds ec2:ReplayWindowSizePackets ec2:RoutingType	
			transit-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			vpn-concentrator	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateVpnConnectionRoute	Grants permission to create a static route for a VPN connection between a virtual private gateway and a customer gateway	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateVpnGateway	Grants permission to create a virtual private gateway	Write	vpn-gateway*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteCapacityManagerDataExport	Grants permission to delete an existing Capacity Manager data export configuration	Write	capacity-manager-data-export*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteCarrierGateway	Grants permission to delete a carrier gateway	Write	carrier-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteClientVpnEndpoint	Grants permission to delete a Client VPN endpoint	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteClientVpnRoute	Grants permission to delete a route from a Client VPN endpoint	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCoipCidr	Grants permission to delete a range of customer-owned IP (CoIP) addresses	Write	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteCoipPool	Grants permission to delete a pool of customer-owned IP (CoIP) addresses	Write	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCoipPoolPermission [permission only]	Grants permission to deny a service from accessing a customer-owned IP (CoIP) pool	Permissions management	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteCustomerGateway	Grants permission to delete a customer gateway	Write	customer-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDhcpOptions	Grants permission to delete a set of DHCP options	Write	dhcp-options*	aws:ResourceTag/${TagKey} ec2:DhcpOptionsID ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteEgressOnlyInternetGateway	Grants permission to delete an egress-only internet gateway	Write	egress-only-internet-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFleets	Grants permission to delete one or more EC2 Fleets	Write	fleet*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteFlowLogs	Grants permission to delete one or more flow logs	Write	vpc-flow-log*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFpgaImage	Grants permission to delete an Amazon FPGA Image (AFI)	Write	fpga-image*	aws:ResourceTag/${TagKey} ec2:Owner ec2:Public ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteImageUsageReport	Grants permission to delete an AMI usage report	Write	image-usage-report*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteInstanceConnectEndpoint	Grants permission to delete an EC2 Instance Connect Endpoint	Write	instance-connect-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SubnetID	
				ec2:Region	
DeleteInstanceEventWindow	Grants permission to delete the specified event window	Write	instance-event-window*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteInternetGateway	Grants permission to delete an internet gateway	Write	internet-gateway*	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteIpam	Grants permission to delete an Amazon VPC IP Address Manager (IPAM) and remove all monitored data associated with the IPAM including the historical data for CIDRs	Write	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteIpamExternalResourceVerificationToken	Grants permission to delete a verification token, which proves ownership of an external resource	Write	ipam-external-resource-verification-token*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteIpamPolicy	Grants permission to delete an Amazon VPC IP Address Manager (IPAM) policy	Write	ipam-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteIpamPool	Grants permission to delete an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteIpamPrefixListResolver	Grants permission to delete an IPAM prefix list resolver	Write	ipam-prefix-list-resolver*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteIpamPrefixListResolverTarget	Grants permission to delete an IPAM prefix list resolver target	Write	ipam-prefix-list-resolver-target*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteIpamResourceDiscovery	Grants permission to delete an IPAM resource discovery	Write	ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteIpamScope	Grants permission to delete the scope for an Amazon VPC IP Address Manager (IPAM)	Write	ipam-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteKeyPair	Grants permission to delete a key pair by removing the public key from Amazon EC2	Write	key-pair	aws:ResourceTag/${TagKey} ec2:KeyPairName ec2:KeyPairType ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLaunchTemplate	Grants permission to delete a launch template and its associated versions	Write	launch-template*	aws:ResourceTag/${TagKey} ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteLaunchTemplateVersions	Grants permission to delete one or more versions of a launch template	Write	launch-template*	aws:ResourceTag/${TagKey} ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLocalGatewayRoute	Grants permission to delete a route from a local gateway route table	Write	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			prefix-list	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteLocalGatewayRouteTable	Grants permission to delete a local gateway route table	Write	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteLocalGatewayRouteTablePermission [permission only]	Grants permission to deny a service from accessing a local gateway route table	Permissions management	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteLocalGatewayRouteTableVirtualInterfaceGroupAssociation	Grants permission to delete a local gateway route table virtual interface group association	Write	local-gateway-route-table-virtual-interface-group-association*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLocalGatewayRouteTableVpcAssociation	Grants permission to delete an association between a VPC and local gateway route table	Write	local-gateway-route-table-vpc-association*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteLocalGatewayVirtualInterface	Grants permission to delete a local gateway virtual interface	Write	local-gateway-virtual-interface*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLocalGatewayVirtualInterfaceGroup	Grants permission to delete a local gateway virtual interface group	Write	local-gateway-virtual-interface-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteManagedPrefixList	Grants permission to delete a managed prefix list	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:IpamPrefixListResolverTargetId ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteNatGateway	Grants permission to delete a NAT gateway	Write	natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteNetworkAcl	Grants permission to delete a network ACL	Write	network-acl*	aws:ResourceTag/${TagKey} ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteNetworkAclEntry	Grants permission to delete an inbound or outbound entry (rule) from a network ACL	Write	network-acl*	aws:ResourceTag/${TagKey} ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	
				ec2:Region	
DeleteNetworkInsightsAccessScope	Grants permission to delete a Network Access Scope	Write	network-insights-access-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteNetworkInsightsAccessScopeAnalysis	Grants permission to delete a Network Access Scope analysis	Write	network-insights-access-scope-analysis*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteNetworkInsightsAnalysis	Grants permission to delete a network insights analysis	Write	network-insights-analysis*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteNetworkInsightsPath	Grants permission to delete a network insights path	Write	network-insights-path*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteNetworkInterface	Grants permission to delete a detached network interface	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteNetworkInterfacePermission	Grants permission to delete a permission that is associated with a network interface	Permissions management	network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteOdbNetworkPeering [permission only]	Grants permission to allow Oracle Database@AWS to delete a peering connection between an ODB network and a VPC	Permissions management	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePlacementGroup	Grants permission to delete a placement group	Write	placement-group*	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeletePublicIpv4Pool	Grants permission to delete a public IPv4 address pool for public IPv4 CIDRs that you own and brought to Amazon to manage with Amazon VPC IP Address Manager (IPAM)	Write	ipv4pool-ec2*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteQueuedReservedInstances	Grants permission to delete the queued purchases for the specified Reserved Instances	Write	reserved-instances*	aws:ResourceTag/${TagKey} ec2:InstanceType ec2:ReservedInstancesOfferingType ec2:ResourceTag/${TagKey} ec2:Tenancy	
				ec2:Region	
DeleteResourcePolicy [permission only]	Grants permission to remove an IAM policy that enables cross-account sharing from a resource	Permissions management	ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
			verified-access-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRoute	Grants permission to delete a route from a route table	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
				ec2:Region	
DeleteRouteServer	Grants permission to delete a route server	Write	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	sns:DeleteTopic
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRouteServerEndpoint	Grants permission to delete a route server endpoint	Write	route-server-endpoint*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey}	ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:RevokeSecurityGroupIngress
				ec2:Region	
DeleteRouteServerPeer	Grants permission to delete a route server peer	Write	route-server-peer*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey}	ec2:RevokeSecurityGroupIngress
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRouteTable	Grants permission to delete a route table	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
				ec2:Region	
DeleteSecurityGroup	Grants permission to delete a security group	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteSnapshot	Grants permission to delete a snapshot of an EBS volume	Write	snapshot*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:OutpostArn ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteSpotDatafeedSubscription	Grants permission to delete a data feed for Spot Instances	Write		ec2:Region	
DeleteSubnet	Grants permission to delete a subnet	Write	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSubnetCidrReservation	Grants permission to delete a subnet CIDR reservation	Write		ec2:Region	
DeleteTags	Grants permission to delete one or more tags from Amazon EC2 resources	Tagging	capacity-block	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			capacity-manager-data-export	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			capacity-reservation	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			capacity-reservation-fleet	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			carrier-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			client-vpn-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			coip-pool	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			customer-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			declarative-policies-report	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			dedicated-host	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			dhcp-options	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			egress-only-internet-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			elastic-gpu	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			elastic-ip	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			export-image-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			export-instance-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			fleet	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			fpga-image	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			host-reservation	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image-usage-report	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			import-image-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			import-snapshot-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance-connect-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance-event-window	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			internet-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-external-resource-verification-token	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-policy	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-pool	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-prefix-list-resolver	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-prefix-list-resolver-target	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-resource-discovery	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-resource-discovery-association	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-scope	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv4pool-ec2	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv6pool-ec2	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			key-pair	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			launch-template	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-route-table	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-route-table-virtual-interface-group-association	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-route-table-vpc-association	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-virtual-interface	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			local-gateway-virtual-interface-group	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			natgateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-acl	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-insights-access-scope	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-insights-access-scope-analysis	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-insights-analysis	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-insights-path	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			placement-group	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			prefix-list	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			replace-root-volume-task	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			reserved-instances	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-server	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-server-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-server-peer	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-table	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group-rule	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			spot-fleet-request	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			spot-instances-request	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet-cidr-reservation	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-filter	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-filter-rule	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-session	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-target	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-connect-peer	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-metering-policy	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-multicast-domain	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-policy-table	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table-announcement	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-endpoint-target	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-group	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-instance	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-policy	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-trust-provider	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-block-public-access-exclusion	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-encryption-control	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint-connection	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint-service	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint-service-permission	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-flow-log	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-peering-connection	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-concentrator	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-connection	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-gateway	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ResourceTag/${TagKey}	
				aws:TagKeys ec2:Region	
DeleteTrafficMirrorFilter	Grants permission to delete a traffic mirror filter	Write	traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteTrafficMirrorFilterRule	Grants permission to delete a traffic mirror filter rule	Write	traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			traffic-mirror-filter-rule*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTrafficMirrorSession	Grants permission to delete a traffic mirror session	Write	traffic-mirror-session*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteTrafficMirrorTarget	Grants permission to delete a traffic mirror target	Write	traffic-mirror-target*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTransitGateway	Grants permission to delete a transit gateway	Write	transit-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	
				ec2:Region	
DeleteTransitGatewayConnect	Grants permission to delete a transit gateway connect attachment	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteTransitGatewayConnectPeer	Grants permission to delete a transit gateway connect peer	Write	transit-gateway-connect-peer*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayConnectPeerId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTransitGatewayMeteringPolicy	Grants permission to delete a transit gateway metering policy	Write	transit-gateway-metering-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMeteringPolicyId	
				ec2:Region	
DeleteTransitGatewayMeteringPolicyEntry	Grants permission to delete an entry from a transit gateway metering policy	Write	transit-gateway-metering-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMeteringPolicyId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteTransitGatewayMulticastDomain	Grants permission to delete a transit gateway multicast domain	Write	transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTransitGatewayPeeringAttachment	Grants permission to delete a peering attachment from a transit gateway	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	
DeleteTransitGatewayPolicyTable	Grants permission to delete a transit gateway policy table	Write	transit-gateway-policy-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteTransitGatewayPrefixListReference	Grants permission to delete a transit gateway prefix list reference	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTransitGatewayRoute	Grants permission to delete a route from a transit gateway route table	Write	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	
DeleteTransitGatewayRouteTable	Grants permission to delete a transit gateway route table	Write	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteTransitGatewayRouteTableAnnouncement	Grants permission to delete a transit gateway route table announcement	Write	transit-gateway-route-table-announcement*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableAnnouncementId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTransitGatewayVpcAttachment	Grants permission to delete a VPC attachment from a transit gateway	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	
DeleteVerifiedAccessEndpoint	Grants permission to delete a Verified Access endpoint	Write	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVerifiedAccessGroup	Grants permission to delete a Verified Access group	Write	verified-access-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteVerifiedAccessInstance	Grants permission to delete a Verified Access instance	Write	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVerifiedAccessTrustProvider	Grants permission to delete a verified trust provider	Write	verified-access-trust-provider*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVolume	Grants permission to delete an EBS volume	Write	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:VolumeID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVpc	Grants permission to delete a VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
DeleteVpcBlockPublicAccessExclusion	Grants permission to delete an exclusion list for blocked public access on a VPC	Write	vpc-block-public-access-exclusion*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVpcEncryptionControl	Grants permission to delete a VPC Encryption Control	Write	vpc-encryption-control*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteVpcEndpointConnectionNotifications	Grants permission to delete one or more VPC endpoint connection notifications	Write	vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-endpoint-service	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVpcEndpointServiceConfigurations	Grants permission to delete one or more VPC endpoint service configurations	Write	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVpcEndpoints	Grants permission to delete one or more VPC endpoints	Write	vpc-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceServiceName ec2:VpceServiceRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVpcPeeringConnection	Grants permission to delete a VPC peering connection	Write	vpc-peering-connection*	aws:ResourceTag/${TagKey} ec2:AccepterVpc ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	
				ec2:Region	
DeleteVpnConcentrator	Grants permission to delete a VPN concentrator	Write	vpn-concentrator*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DeleteVpnConnection	Grants permission to delete a VPN connection	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteVpnConnectionRoute	Grants permission to delete a static route for a VPN connection between a virtual private gateway and a customer gateway	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVpnGateway	Grants permission to delete a virtual private gateway	Write	vpn-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeprovisionByoipCidr	Grants permission to release an IP address range that was provisioned through bring your own IP addresses (BYOIP), and to delete the corresponding address pool	Write		ec2:Region	
DeprovisionIpamByoasn	Grants permission to deprovision an Autonomous System Number (ASN) from an Amazon Web Services account	Write	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeprovisionIpamPoolCidr	Grants permission to deprovision a CIDR provisioned from an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeprovisionPublicIpv4PoolCidr	Grants permission to deprovision a CIDR from a public IPv4 pool	Write	ipv4pool-ec2*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterImage	Grants permission to deregister an Amazon Machine Image (AMI)	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	
DeregisterInstanceEventNotificationAttributes	Grants permission to remove tags from the set of tags to include in notifications about scheduled events for your instances	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterTransitGatewayMulticastGroupMembers	Grants permission to deregister one or more network interface members from a group IP address in a transit gateway multicast domain	Write	network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-multicast-domain	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterTransitGatewayMulticastGroupSources	Grants permission to deregister one or more network interface sources from a group IP address in a transit gateway multicast domain	Write	network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-multicast-domain	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	
DescribeAccountAttributes	Grants permission to describe the attributes of the AWS account	List		ec2:Region	
DescribeAddressTransfers	Grants permission to describe an Elastic IP address transfer	List		ec2:Region	
DescribeAddresses	Grants permission to describe one or more Elastic IP addresses	List		ec2:Region	
DescribeAddressesAttribute	Grants permission to describe the attributes of the specified Elastic IP addresses	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAggregateIdFormat	Grants permission to describe the longer ID format settings for all resource types	List		ec2:Region	
DescribeAvailabilityZones	Grants permission to describe one or more of the Availability Zones that are available to you	List		ec2:Region	
DescribeAwsNetworkPerformanceMetricSubscriptions	Grants permission to describe the current infrastructure performance metric subscriptions	List		ec2:Region	
DescribeBundleTasks	Grants permission to describe one or more bundling tasks	List		ec2:Region	
DescribeByoipCidrs	Grants permission to describe the IP address ranges that were provisioned through bring your own IP addresses (BYOIP)	List		ec2:Region	
DescribeCapacityBlockExtensionHistory	Grants permission to describe Capacity Block extensions history	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCapacityBlockExtensionOfferings	Grants permission to describe Capacity Block extensions offerings	List	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CapacityReservationFleet ec2:CreateDate ec2:DestinationCapacityReservationId ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:OutpostArn ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCapacityBlockOfferings	Grants permission to describe Capacity Block offerings available for purchase	List		ec2:Region	
DescribeCapacityBlockStatus	Grants permission to describe the availability of capacity for the specified Capacity blocks, or all of your Capacity Blocks	List		ec2:Region	
DescribeCapacityBlocks	Grants permission to describe details about Capacity Blocks in the AWS Region that you're currently using	List		ec2:Region	
DescribeCapacityManagerDataExports	Grants permission to describe one or more Capacity Manager data export configurations	List		ec2:Region	
DescribeCapacityReservationBillingRequests	Grants permission to describe one or more requests to assign the billing of the unused capacity of a Capacity Reservation	List		ec2:Region	
DescribeCapacityReservationFleets	Grants permission to describe one or more Capacity Reservation Fleets	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCapacityReservationTopology	Grants permission to describe the topology of one or more Capacity Reservations	List		ec2:Region	
DescribeCapacityReservations	Grants permission to describe one or more Capacity Reservations	List		ec2:Region	
DescribeCarrierGateways	Grants permission to describe one or more Carrier Gateways	List		ec2:Region	
DescribeClassicLinkInstances	Grants permission to describe one or more linked EC2-Classic instances	List		ec2:Region	
DescribeClientVpnAuthorizationRules	Grants permission to describe the authorization rules for a Client VPN endpoint	List	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeClientVpnConnections	Grants permission to describe active client connections and connections that have been terminated within the last 60 minutes for a Client VPN endpoint	List	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DescribeClientVpnEndpoints	Grants permission to describe one or more Client VPN endpoints	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeClientVpnRoutes	Grants permission to describe the routes for a Client VPN endpoint	List	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeClientVpnTargetNetworks	Grants permission to describe the target networks that are associated with a Client VPN endpoint	List	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DescribeCoipPools	Grants permission to describe the specified customer-owned address pools or all of your customer-owned address pools	List		ec2:Region	
DescribeConversionTasks	Grants permission to describe one or more conversion tasks	List		ec2:Region	
DescribeCustomerGateways	Grants permission to describe one or more customer gateways	List		ec2:Region	
DescribeDeclarativePoliciesReports	Grants permission to describe one or more declarative policies reports	List		ec2:Region	
DescribeDhcpOptions	Grants permission to describe one or more DHCP options sets	List		ec2:Region	
DescribeEgressOnlyInternetGateways	Grants permission to describe one or more egress-only internet gateways	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeElasticGpus	Grants permission to describe an Elastic Graphics accelerator that is associated with an instance	List		ec2:Region	
DescribeExportImageTasks	Grants permission to describe one or more export image tasks	List		ec2:Region	
DescribeExportTasks	Grants permission to describe one or more export instance tasks	List		ec2:Region	
DescribeFastLaunchImages	Grants permission to describe fast-launch enabled Windows AMIs	List		ec2:Region	
DescribeFastSnapshotRestores	Grants permission to describe the state of fast snapshot restores for snapshots	List		ec2:Region	
DescribeFleetHistory	Grants permission to describe the events for an EC2 Fleet during a specified time	List	fleet*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFleetInstances	Grants permission to describe the running instances for an EC2 Fleet	List	fleet*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DescribeFleets	Grants permission to describe one or more EC2 Fleets	List		ec2:Region	
DescribeFlowLogs	Grants permission to describe one or more flow logs	List		ec2:Region	
DescribeFpgaImageAttribute	Grants permission to describe the attributes of an Amazon FPGA Image (AFI)	List	fpga-image*	aws:ResourceTag/${TagKey} ec2:Owner ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFpgaImages	Grants permission to describe one or more Amazon FPGA Images (AFIs)	List		ec2:Region	
DescribeHostReservationOfferings	Grants permission to describe the Dedicated Host Reservations that are available to purchase	List		ec2:Region	
DescribeHostReservations	Grants permission to describe the Dedicated Host Reservations that are associated with Dedicated Hosts in the AWS account	List		ec2:Region	
DescribeHosts	Grants permission to describe one or more Dedicated Hosts	List		ec2:Region	
DescribeIamInstanceProfileAssociations	Grants permission to describe the IAM instance profile associations	List		ec2:Region	
DescribeIdFormat	Grants permission to describe the ID format settings for resources	List		ec2:Region	
DescribeIdentityIdFormat	Grants permission to describe the ID format settings for resources for an IAM user, IAM role, or root user	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeImageAttribute	Grants permission to describe an attribute of an Amazon Machine Image (AMI)	List	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	
DescribeImageReferences	Grants permission to describe your AWS resources that are referencing specified images	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeImageUsageReportEntries	Grants permission to describe the entries of an AMI usage report	List		ec2:Region	
DescribeImageUsageReports	Grants permission to describe the configuration and status of an AMI usage report	List		ec2:Region	
DescribeImages	Grants permission to describe one or more images (AMIs, AKIs, and ARIs)	List		ec2:Region	
DescribeImportImageTasks	Grants permission to describe import virtual machine or import snapshot tasks	List		ec2:Region	
DescribeImportSnapshotTasks	Grants permission to describe import snapshot tasks	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInstanceAttribute	Grants permission to describe the attributes of an instance	List	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
DescribeInstanceConnectEndpoints	Grants permission to describe EC2 Instance Connect Endpoints	List		ec2:Region	
DescribeInstanceCreditSpecifications	Grants permission to describe the credit option for CPU usage of one or more burstable performance instances	List		ec2:Region	
DescribeInstanceEventNotificationAttributes	Grants permission to describe the set of tags to include in notifications about scheduled events for your instances	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInstanceEventWindows	Grants permission to describe the specified event windows or all event windows	List		ec2:Region	
DescribeInstanceImageMetadata	Grants permission to describe the AMI that was used to launch an instance	List		ec2:Region	
DescribeInstanceSqlHaHistoryStates	Grants permission to describe EC2 instance SQL HA history states	List		ec2:Region	
DescribeInstanceSqlHaStates	Grants permission to describe EC2 instance SQL HA states	List		ec2:Region	
DescribeInstanceStatus	Grants permission to describe the status of one or more instances	List		ec2:Region	
DescribeInstanceTopology	Grants permission to describe a tree-based hierarchy that represents the physical host placement of EC2 instances	List		ec2:Region	
DescribeInstanceTypeOfferings	Grants permission to describe the set of instance types that are offered in a location	List		ec2:Region	
DescribeInstanceTypes	Grants permission to describe the details of instance types that are offered in a location	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInstances	Grants permission to describe one or more instances	List		ec2:Region	
DescribeInternetGateways	Grants permission to describe one or more internet gateways	List		ec2:Region	
DescribeIpamByoasn	Grants permission to describe a bring your own Autonomous System Number (BYOASN) that you've brought to IPAM	List		ec2:Region	
DescribeIpamExternalResourceVerificationTokens	Grants permission to describe verification tokens, which proves ownership of an external resource	List		ec2:Region	
DescribeIpamPolicies	Grants permission to describe Amazon VPC IP Address Manager (IPAM) policies	List		ec2:Region	
DescribeIpamPools	Grants permission to describe Amazon VPC IP Address Manager (IPAM) pools	List		ec2:Region	
DescribeIpamPrefixListResolverTargets	Grants permission to describe IPAM prefix list resolver targets	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeIpamPrefixListResolvers	Grants permission to describe IPAM prefix list resolvers	List		ec2:Region	
DescribeIpamResourceDiscoveries	Grants permission to describe IPAM resource discoveries	List		ec2:Region	
DescribeIpamResourceDiscoveryAssociations	Grants permission to describe resource discovery associations with an Amazon VPC IPAM	List		ec2:Region	
DescribeIpamScopes	Grants permission to describe Amazon VPC IP Address Manager (IPAM) scopes	List		ec2:Region	
DescribeIpams	Grants permission to describe an Amazon VPC IP Address Manager (IPAM)	List		ec2:Region	
DescribeIpv6Pools	Grants permission to describe one or more IPv6 address pools	List		ec2:Region	
DescribeKeyPairs	Grants permission to describe one or more key pairs	List		ec2:Region	
DescribeLaunchTemplateVersions	Grants permission to describe one or more launch template versions	List		ec2:Region	ssm:GetParameters

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLaunchTemplates	Grants permission to describe one or more launch templates	List		ec2:Region	
DescribeLocalGatewayRouteTablePermissions [permission only]	Grants permission to allow a service to describe local gateway route table permissions	List		ec2:Region	
DescribeLocalGatewayRouteTableVirtualInterfaceGroupAssociations	Grants permission to describe the associations between virtual interface groups and local gateway route tables	List		ec2:Region	
DescribeLocalGatewayRouteTableVpcAssociations	Grants permission to describe an association between VPCs and local gateway route tables	List		ec2:Region	
DescribeLocalGatewayRouteTables	Grants permission to describe one or more local gateway route tables	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLocalGatewayVirtualInterfaceGroups	Grants permission to describe local gateway virtual interface groups	List		ec2:Region	
DescribeLocalGatewayVirtualInterfaces	Grants permission to describe local gateway virtual interfaces	List		ec2:Region	
DescribeLocalGateways	Grants permission to describe one or more local gateways	List		ec2:Region	
DescribeLockedSnapshots	Grants permission to describe the lock status for a snapshot	List		ec2:Region	
DescribeMacHosts	Grants permission to describe your EC2 Mac Dedicated hosts	List		ec2:Region	
DescribeMacModificationTasks	Grants permission to describe a System Integrity Protection (SIP) modification task or volume ownership delegation task for an Amazon EC2 Mac instance	List		ec2:Region	
DescribeManagedPrefixLists	Grants permission to describe your managed prefix lists and any AWS-managed prefix lists	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeMovingAddresses	Grants permission to describe Elastic IP addresses that are being moved to the EC2-VPC platform	List		ec2:Region	
DescribeNatGateways	Grants permission to describe one or more NAT gateways	List		ec2:Region	
DescribeNetworkAcls	Grants permission to describe one or more network ACLs	List		ec2:Region	
DescribeNetworkInsightsAccessScopeAnalyses	Grants permission to describe one or more Network Access Scope analyses	List		ec2:Region	
DescribeNetworkInsightsAccessScopes	Grants permission to describe the Network Access Scopes	List		ec2:Region	
DescribeNetworkInsightsAnalyses	Grants permission to describe one or more network insights analyses	List		ec2:Region	
DescribeNetworkInsightsPaths	Grants permission to describe one or more network insights paths	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeNetworkInterfaceAttribute	Grants permission to describe a network interface attribute	List		ec2:Region	
DescribeNetworkInterfacePermissions	Grants permission to describe the permissions that are associated with a network interface	List		ec2:Region	
DescribeNetworkInterfaces	Grants permission to describe one or more network interfaces	List		ec2:Region	
DescribeOutpostLags	Grants permission to describe Outpost LAGs	List		ec2:Region	
DescribePlacementGroups	Grants permission to describe one or more placement groups	List		ec2:Region	
DescribePrefixLists	Grants permission to describe available AWS services in a prefix list format	List		ec2:Region	
DescribePrincipalIdFormat	Grants permission to describe the ID format settings for the root user and all IAM roles and IAM users that have explicitly specified a longer ID (17-character ID) preference	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribePublicIpv4Pools	Grants permission to describe one or more IPv4 address pools	List		ec2:Region	
DescribeRegions	Grants permission to describe one or more AWS Regions that are currently available in your account	List		ec2:Region	
DescribeReplaceRootVolumeTasks	Grants permission to describe a root volume replacement task	List		ec2:Region	
DescribeReservedInstances	Grants permission to describe one or more purchased Reserved Instances in your account	List		ec2:Region	
DescribeReservedInstancesListings	Grants permission to describe your account's Reserved Instance listings in the Reserved Instance Marketplace	List		ec2:Region	
DescribeReservedInstancesModifications	Grants permission to describe the modifications made to one or more Reserved Instances	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeReservedInstancesOfferings	Grants permission to describe the Reserved Instance offerings that are available for purchase	List		ec2:Region	
DescribeRouteServerEndpoints	Grants permission to describe one or more route server endpoints	List		ec2:Region	
DescribeRouteServerPeers	Grants permission to describe one or more route server peers	List		ec2:Region	
DescribeRouteServers	Grants permission to describe one or more route servers	List		ec2:Region	
DescribeRouteTables	Grants permission to describe one or more route tables	List		ec2:Region	
DescribeScheduledInstanceAvailability	Grants permission to find available schedules for Scheduled Instances	List		ec2:Region	
DescribeScheduledInstances	Grants permission to describe one or more Scheduled Instances in your account	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSecurityGroupReferences	Grants permission to describe the VPCs on the other side of a VPC peering connection that are referencing specified VPC security groups	List	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	
DescribeSecurityGroupRules	Grants permission to describe one or more of your security group rules	List		ec2:Region	
DescribeSecurityGroupVpcAssociations	Grants permission to describe security group VPC associations	List		ec2:Region	
DescribeSecurityGroups	Grants permission to describe one or more security groups	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeServiceLinkVirtualInterfaces	Grants permission to describe service link virtual interfaces	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSnapshotAttribute	Grants permission to describe an attribute of a snapshot	List	snapshot*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:OutpostArn ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:SourceOutpostArn ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DescribeSnapshotTierStatus	Grants permission to describe the storage tier status for Amazon EBS snapshots	List		ec2:Region	
DescribeSnapshots	Grants permission to describe one or more EBS snapshots	List		ec2:Region	
DescribeSpotDatafeedSubscription	Grants permission to describe the data feed for Spot Instances	List		ec2:Region	
DescribeSpotFleetInstances	Grants permission to describe the running instances for a Spot Fleet	List	spot-fleet-request*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSpotFleetRequestHistory	Grants permission to describe the events for a Spot Fleet request during a specified time	List	spot-fleet-request*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DescribeSpotFleetRequests	Grants permission to describe one or more Spot Fleet requests	List		ec2:Region	
DescribeSpotInstanceRequests	Grants permission to describe one or more Spot Instance requests	List		ec2:Region	
DescribeSpotPriceHistory	Grants permission to describe the Spot Instance price history	List		ec2:Region	
DescribeStaleSecurityGroups	Grants permission to describe the stale security group rules for security groups in a specified VPC	List		ec2:Region	
DescribeStoreImageTasks	Grants permission to describe the progress of the AMI store tasks	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSubnets	Grants permission to describe one or more subnets	List		ec2:Region	
DescribeTags	Grants permission to describe one or more tags for an Amazon EC2 resource	List		ec2:Region	
DescribeTrafficMirrorFilterRules	Grants permission to describe traffic mirror filters that determine the traffic that is mirrored	List		ec2:Region	
DescribeTrafficMirrorFilters	Grants permission to describe one or more traffic mirror filters	List		ec2:Region	
DescribeTrafficMirrorSessions	Grants permission to describe one or more traffic mirror sessions	List		ec2:Region	
DescribeTrafficMirrorTargets	Grants permission to describe one or more traffic mirror targets	List		ec2:Region	
DescribeTransitGatewayAttachments	Grants permission to describe one or more attachments between resources and transit gateways	List		ec2:Region	
DescribeTransitGatewayConnectPeers	Grants permission to describe one or more transit gateway connect peers	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTransitGatewayConnects	Grants permission to describe one or more transit gateway connect attachments	List		ec2:Region	
DescribeTransitGatewayMeteringPolicies	Grants permission to describe one or more transit gateway metering policies	List		ec2:Region	
DescribeTransitGatewayMulticastDomains	Grants permission to describe one or more transit gateway multicast domains	List		ec2:Region	
DescribeTransitGatewayPeeringAttachments	Grants permission to describe one or more transit gateway peering attachments	List		ec2:Region	
DescribeTransitGatewayPolicyTables	Grants permission to describe a transit gateway policy table	List		ec2:Region	
DescribeTransitGatewayRouteTableAnnouncements	Grants permission to describe a transit gateway route table announcement	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTransitGatewayRouteTables	Grants permission to describe one or more transit gateway route tables	List		ec2:Region	
DescribeTransitGatewayVpcAttachments	Grants permission to describe one or more VPC attachments on a transit gateway	List		ec2:Region	
DescribeTransitGateways	Grants permission to describe one or more transit gateways	List		ec2:Region	
DescribeTrunkInterfaceAssociations	Grants permission to describe one or more network interface trunk associations	List		ec2:Region	
DescribeVerifiedAccessEndpoints	Grants permission to describe the specified Verified Access endpoints or all Verified Access endpoints	List		ec2:Region	
DescribeVerifiedAccessGroups	Grants permission to describe the specified Verified Access groups or all Verified Access groups	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVerifiedAccessInstanceLoggingConfigurations	Grants permission to describe the current logging configuration for the Verified Access instances	List		ec2:Region	
DescribeVerifiedAccessInstanceWebAclAssociations [permission only]	Grants permission to describe the AWS Web Application Firewall (WAF) web access control list (ACL) associations for a Verified Access instance	List		ec2:Region	
DescribeVerifiedAccessInstances	Grants permission to describe the specified Verified Access instances or all Verified Access instances	List		ec2:Region	
DescribeVerifiedAccessTrustProviders	Grants permission to describe details of existing Verified Access trust providers	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVolumeAttribute	Grants permission to describe an attribute of an EBS volume	List	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:VolumeID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	
DescribeVolumeStatus	Grants permission to describe the status of one or more EBS volumes	List		ec2:Region	
DescribeVolumes	Grants permission to describe one or more EBS volumes	List		ec2:Region	
DescribeVolumesModifications	Grants permission to describe the current modification status of one or more EBS volumes	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVpcAttribute	Grants permission to describe an attribute of a VPC	List	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
DescribeVpcBlockPublicAccessExclusions	Grants permission to describe an exclusion list for blocked public access on a VPC	List		ec2:Region	
DescribeVpcBlockPublicAccessOptions	Grants permission to describe options for blocked public access on a VPC	List		ec2:Region	
DescribeVpcClassicLink	Grants permission to describe the ClassicLink status of one or more VPCs	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVpcClassicLinkDnsSupport	Grants permission to describe the ClassicLink DNS support status of one or more VPCs	List		ec2:Region	
DescribeVpcEncryptionControls	Grants permission to describe one or more VPC Encryption Controls	List		ec2:Region	
DescribeVpcEndpointAssociations	Grants permission to describe the VPC endpoint associations	List		ec2:Region	
DescribeVpcEndpointConnectionNotifications	Grants permission to describe the connection notifications for VPC endpoints and VPC endpoint services	List		ec2:Region	
DescribeVpcEndpointConnections	Grants permission to describe the VPC endpoint connections to your VPC endpoint services	List		ec2:Region	
DescribeVpcEndpointServiceConfigurations	Grants permission to describe VPC endpoint service configurations (your services)	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVpcEndpointServicePermissions	Grants permission to describe the principals (service consumers) that are permitted to discover your VPC endpoint service	List	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	
DescribeVpcEndpointServices	Grants permission to describe all supported AWS services that can be specified when creating a VPC endpoint	List		ec2:Region	
DescribeVpcEndpoints	Grants permission to describe one or more VPC endpoints	List		ec2:Region	
DescribeVpcPeeringConnections	Grants permission to describe one or more VPC peering connections	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVpcs	Grants permission to describe one or more VPCs	List		ec2:Region	
DescribeVpnConcentrators	Grants permission to describe one or more VPN concentrators	List		ec2:Region	
DescribeVpnConnections	Grants permission to describe one or more VPN connections	List		ec2:Region	
DescribeVpnGateways	Grants permission to describe one or more virtual private gateways	List		ec2:Region	
DetachApplianceFromNatGateway [permission only]	Grants permission to detach an appliance from a public/private Natgateway	Permissions management	natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachClassicLinkVpc	Grants permission to unlink (detach) a linked EC2-Classic instance from a VPC	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceProfile ec2:InstanceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
DetachInternetGateway	Grants permission to detach an internet gateway from a VPC	Write	internet-gateway*	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachNetworkInterface	Grants permission to detach a network interface from an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachVerifiedAccessTrustProvider	Grants permission to detach a trust provider from a Verified Access instance	Write	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			verified-access-trust-provider*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachVolume	Grants permission to detach an EBS volume from an instance	Write	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:VolumeID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
DetachVpnGateway	Grants permission to detach a virtual private gateway from a VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DisableAddressTransfer	Grants permission to disable Elastic IP address transfer	Write	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DisableAllowedImagesSettings	Grants permission to disable allowed images settings	Write		ec2:Region	
DisableAwsNetworkPerformanceMetricSubscription	Grants permission to disable infrastructure performance metric subscriptions	Write		ec2:Region	
DisableCapacityManager	Grants permission to disable EC2 Capacity Manager for your account	Write		ec2:Region	
DisableEbsEncryptionByDefault	Grants permission to disable EBS encryption by default for your account	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableFastLaunch	Grants permission to disable faster launching for Windows AMIs	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableFastSnapshotRestores	Grants permission to disable fast snapshot restores for one or more snapshots in specified Availability Zones	Write	snapshot*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableImage	Grants permission to disable an AMI	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	
DisableImageBlockPublicAccess	Grants permission to disable block public access for AMIs at the account level in the specified AWS Region	Permissions management		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableImageDeprecation	Grants permission to cancel the deprecation of the specified AMI	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableImageDeregistrationProtection	Grants permission to disable deregistration protection for an AMI. When deregistration protection is disabled, the AMI can be deregistered	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableInstanceSqlHaStandbyDetections	Grants permission to disable EC2 instance SQL HA standby detections	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DisableIpamOrganizationAdminAccount	Grants permission to disable an AWS Organizations member account as an Amazon VPC IP Address Manager (IPAM) admin account	Write		ec2:Region	organizations:DeregisterDelegatedAdministrator
DisableIpamPolicy	Grants permission to disable a policy in Amazon VPC IP Address Manager (IPAM) that controls public IPv4 address allocation	Write	ipam-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DisableRouteServerPropagation	Grants permission to disable route server propagation	Write	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
				ec2:Region	
DisableSerialConsoleAccess	Grants permission to disable access to the EC2 serial console of all instances for your account	Write		ec2:Region	
DisableSnapshotBlockPublicAccess	Grants permission to disable the block public access for snapshots setting for a Region	Permissions management		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableTransitGatewayRouteTablePropagation	Grants permission to disable a resource attachment from propagating routes to the specified propagation route table	Write	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table-announcement	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableAnnouncementId	
				ec2:Region	
DisableVgwRoutePropagation	Grants permission to disable a virtual private gateway from propagating routes to a specified route table of a VPC	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpn-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DisableVpcClassicLink	Grants permission to disable ClassicLink for a VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableVpcClassicLinkDnsSupport	Grants permission to disable ClassicLink DNS support for a VPC	Write	vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateAddress	Grants permission to disassociate an Elastic IP address from an instance or network interface	Write	elastic-ip	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateCapacityReservationBillingOwner	Grants permission to cancel a pending request to assign billing of the unused capacity of a Capacity Reservation to a consumer account	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CapacityReservationFleet ec2:CreateDate ec2:DestinationCapacityReservationId ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:OutpostArn ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateClientVpnTargetNetwork	Grants permission to disassociate a target network from a Client VPN endpoint	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DisassociateEnclaveCertificateIamRole	Grants permission to disassociate an ACM certificate from a IAM role	Write	certificate*		
			role*		
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateIamInstanceProfile	Grants permission to disassociate an IAM instance profile from a running or stopped instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
DisassociateInstanceEventWindow	Grants permission to disassociate one or more targets from an event window	Write	instance-event-window*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DisassociateIpamByoasn	Grants permission to disassociate an Autonomous System Number (ASN) from a BYOIP CIDR	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateIpamResourceDiscovery	Grants permission to disassociate a resource discovery from an Amazon VPC IPAM	Write	ipam-resource-discovery-association*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DisassociateNatGatewayAddress	Grants permission to disassociate a secondary Elastic IP address from a public NAT gateway	Write	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:ResourceTag/${TagKey} ec2:AuthorizedUser ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DisassociateRouteServer	Grants permission to disassociate a route server from a VPC	Write	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpc*	aws:ResourceTag/${TagKey} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DisassociateRouteTable	Grants permission to disassociate a subnet from a route table	Write	internet-gateway	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	
			ipv4pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv6pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
DisassociateSecurityGroupVpc	Grants permission to disassociate a security group from a VPC	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc	aws:ResourceTag/${TagKey} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateSubnetCidrBlock	Grants permission to disassociate a CIDR block from a subnet	Write	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateTransitGatewayMulticastDomain	Grants permission to disassociate one or more subnets from a transit gateway multicast domain	Write	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateTransitGatewayPolicyTable	Grants permission to disassociate a policy table from a transit gateway	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-policy-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateTransitGatewayRouteTable	Grants permission to disassociate a resource attachment from a transit gateway route table	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateTrunkInterface	Grants permission to disassociate a branch network interface to a trunk network interface	Write		ec2:Region	
DisassociateVerifiedAccessInstanceWebAcl [permission only]	Grants permission to disassociate an AWS Web Application Firewall (WAF) web access control list (ACL) from a Verified Access instance	Write	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DisassociateVpcCidrBlock	Grants permission to disassociate a CIDR block from a VPC	Write	vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
EnableAddressTransfer	Grants permission to enable Elastic IP address transfer	Write	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	
				ec2:Region	
EnableAllowedImagesSettings	Grants permission to enable allowed images settings	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableAwsNetworkPerformanceMetricSubscription	Grants permission to enable infrastructure performance subscriptions	Write		ec2:Region	
EnableCapacityManager	Grants permission to enable EC2 Capacity Manager for your account	Write		ec2:Region	
EnableEbsEncryptionByDefault	Grants permission to enable EBS encryption by default for your account	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableFastLaunch	Grants permission to enable faster launching for Windows AMIs	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	ec2:CreateLaunchTemplate ec2:CreateSnapshot ec2:CreateTags ec2:DeleteSnapshot ec2:DescribeImages ec2:DescribeInstanceAttribute ec2:DescribeInstanceStatus ec2:DescribeInstanceTypeOfferings ec2:DescribeInstances

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeLaunchTemplateVersions ec2:DescribeLaunchTemplates ec2:DescribeSnapshots ec2:DescribeSubnets ec2:RunInstances ec2:StopInstances ec2:TerminateInstances iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			launch-template	aws:ResourceTag/${TagKey} ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableFastSnapshotRestores	Grants permission to enable fast snapshot restores for one or more snapshots in specified Availability Zones	Write	snapshot*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableImage	Grants permission to re-enable a disabled AMI	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	
EnableImageBlockPublicAccess	Grants permission to enable block public access for AMIs at the account level in the specified AWS Region	Permissions management		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableImageDeprecation	Grants permission to enable deprecation of the specified AMI at the specified date and time	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableImageDeregistrationProtection	Grants permission to enable deregistration protection for an AMI. When deregistration protection is enabled, the AMI can't be deregistered	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableInstanceSqlHaStandbyDetections	Grants permission to enable EC2 instance SQL HA standby detections	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
EnableIpamOrganizationAdminAccount	Grants permission to enable an AWS Organizations member account as an Amazon VPC IP Address Manager (IPAM) admin account	Write		ec2:Region	iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess organizations:RegisterDelegatedAdministrator
EnableIpamPolicy	Grants permission to enable an Amazon VPC IP Address Manager (IPAM) policy	Write	ipam-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableReachabilityAnalyzerOrganizationSharing	Grants permission to enable organization sharing of reachability analyzer	Write		ec2:Region	iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess
EnableRouteServerPropagation	Grants permission to enable route server propagation	Write	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
EnableSerialConsoleAccess	Grants permission to enable access to the EC2 serial console of all instances for your account	Write		ec2:Region	
EnableSnapshotBlockPublicAccess	Grants permission to enable or modify the block public access for snapshots setting for a Region	Permissions management		ec2:Region	
EnableTransitGatewayRouteTablePropagation	Grants permission to enable an attachment to propagate routes to a propagation route table	Write	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-route-table-announcement	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableAnnouncementId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableVgwRoutePropagation	Grants permission to enable a virtual private gateway to propagate routes to a VPC route table	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
			vpn-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableVolumeIO	Grants permission to enable I/O operations for a volume that had I/O operations disabled	Write	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	
EnableVpcClassicLink	Grants permission to enable a VPC for ClassicLink	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableVpcClassicLinkDnsSupport	Grants permission to enable a VPC to support DNS hostname resolution for ClassicLink	Write	vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExportClientVpnClientCertificateRevocationList	Grants permission to download the client certificate revocation list for a Client VPN endpoint	Read	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExportClientVpnClientConfiguration	Grants permission to download the contents of the Client VPN endpoint configuration file for a Client VPN endpoint	Read	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ExportImage	Grants permission to export an Amazon Machine Image (AMI) to a VM file	Write	export-image-task*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ExportTransitGatewayRoutes	Grants permission to export routes from a transit gateway route table to an Amazon S3 bucket	Write		ec2:Region	
ExportVerifiedAccessInstanceClientConfiguration	Grants permission to export a verified access instance client configuration	Read	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetActiveVpnTunnelStatus	Grants permission to retrieve the current security parameters for an active VPN tunnel	Read	vpn-connection*	ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetAllowedImagesSettings	Grants permission to get the allowed settings for images	Read		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAssociatedEnclaveCertificateIamRoles	Grants permission to get the list of roles associated with an ACM certificate	Read	certificate*		
				ec2:Region	
GetAssociatedIpv6PoolCidrs	Grants permission to get information about the IPv6 CIDR block associations for a specified IPv6 address pool	Read	ipv6pool-ec2*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetAwsNetworkPerformanceData	Grants permission to get network performance data	Read		ec2:Region	
GetCapacityManagerAttributes	Grants permission to retrieve the current configuration and status of EC2 Capacity Manager	Read		ec2:Region	
GetCapacityManagerMetricData	Grants permission to retrieve capacity usage metrics for your EC2 resources	Read		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCapacityManagerMetricDimensions	Grants permission to retrieve the available dimension values for capacity metrics within a specified time range	Read		ec2:Region	
GetCapacityReservationUsage	Grants permission to get usage information about a Capacity Reservation	Read	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:CapacityReservationFleet	
				ec2:Region	
GetCoipPoolUsage	Grants permission to describe the allocations from the specified customer-owned address pool	Read	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetConsoleOutput	Grants permission to get the console output for an instance	Read	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetConsoleScreenshot	Grants permission to retrieve a JPG-format screenshot of a running instance	Read	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
GetDeclarativePoliciesReportSummary	Grants permission to get the report summary of declarative policies	Read	declarative-policies-report*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
GetDefaultCreditSpecification	Grants permission to get the default credit option for CPU usage of a burstable performance instance family	Read		ec2:Region	
GetEbsDefaultKmsKeyId	Grants permission to get the ID of the default customer master key (CMK) for EBS encryption by default	Read		ec2:Region	
GetEbsEncryptionByDefault	Grants permission to describe whether EBS encryption by default is enabled for your account	Read		ec2:Region	
GetEnabledIpamPolicy	Grants permission to describe the currently enabled policy in Amazon VPC IP Address Manager (IPAM)	Read		ec2:Region	
GetFlowLogsIntegrationTemplate	Grants permission to generate a CloudFormation template to streamline the integration of VPC flow logs with Amazon Athena	Read	vpc-flow-log*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
GetGroupsForCapacityReservation	Grants permission to list the resource groups to which a Capacity Reservation has been added	List	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:CapacityReservationFleet	
				ec2:Region	
GetHostReservationPurchasePreview	Grants permission to preview a reservation purchase with configurations that match those of a Dedicated Host	Read		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetImageAncestry	Grants permission to retrieve the ancestry chain of an AMI back to its root AMI	Read	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	
				ec2:Region	
GetImageBlockPublicAccessState	Grants permission to get the current state of block public access for AMIs at the account level in the specified AWS Region	Read		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInstanceMetadataDefaults	Grants permission to view the default instance metadata service (IMDS) settings set for your account in the specified Region	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInstanceTpmEkPub	Grants permission to get the public endorsement key associated with the Nitro Trusted Platform Module (NitroTPM) for the specified instance	Read	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
GetInstanceTypesFromInstanceRequirements	Grants permission to view a list of instance types with specified instance attributes	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInstanceUefiData	Grants permission to retrieve the binary representation of the UEFI variable store	Read	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
GetIpamAddressHistory	Grants permission to retrieve historical information about a CIDR within an Amazon VPC IP Address Manager (IPAM) scope	Read	ipam-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
GetIpamDiscoveredAccounts	Grants permission to retrieve IPAM discovered accounts	Read	ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetIpamDiscoveredPublicAddresses	Grants permission to retrieve the public IP addresses that have been discovered by IPAM	Read	ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIpamDiscoveredResourceCidrs	Grants permission to retrieve the resource CIDRs that are monitored as part of a resource discovery	Read	ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetIpamPolicyAllocationRules	Grants permission to describe the rules that define how Amazon VPC IP Address Manager (IPAM) pools allocate IP addresses to AWS resource types within an IPAM policy	List	ipam-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIpamPolicyOrganizationTargets	Grants permission to retrieve the AWS Organizations targets associated with an Amazon VPC IP Address Manager (IPAM) policy	List	ipam-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetIpamPoolAllocations	Grants permission to get a list of all the CIDR allocations in an Amazon VPC IP Address Manager (IPAM) pool	List	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIpamPoolCidrs	Grants permission to get the CIDRs provisioned to an Amazon VPC IP Address Manager (IPAM) pool	Read	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetIpamPrefixListResolverRules	Grants permission to get rules for an IPAM prefix list resolver	Read	ipam-prefix-list-resolver*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIpamPrefixListResolverVersionEntries	Grants permission to get CIDR entries for a specific version of an IPAM prefix list resolver	Read	ipam-prefix-list-resolver*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetIpamPrefixListResolverVersions	Grants permission to get versions of an IPAM prefix list resolver	Read	ipam-prefix-list-resolver*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIpamResourceCidrs	Grants permission to get information about the resources in an Amazon VPC IP Address Manager (IPAM) scope	Read	ipam-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLaunchTemplateData	Grants permission to get the configuration data of the specified instance for use with a new launch template or launch template version	Read	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
GetManagedPrefixListAssociations	Grants permission to get information about the resources that are associated with the specified managed prefix list	Read	prefix-list*	aws:ResourceTag/${TagKey} ec2:IpamPrefixListResolverTargetId ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetManagedPrefixListEntries	Grants permission to get information about the entries for a specified managed prefix list	Read	prefix-list*	aws:ResourceTag/${TagKey} ec2:IpamPrefixListResolverTargetId ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetNetworkInsightsAccessScopeAnalysisFindings	Grants permission to get the findings for one or more Network Access Scope analyses	Read	network-insights-access-scope-analysis*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetNetworkInsightsAccessScopeContent	Grants permission to get the content for a specified Network Access Scope	Read	network-insights-access-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPasswordData	Grants permission to retrieve the encrypted administrator password for a running Windows instance	Read	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetReservedInstancesExchangeQuote	Grants permission to return a quote and exchange information for exchanging one or more Convertible Reserved Instances for a new Convertible Reserved Instance	Read	reserved-instances*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:InstanceType ec2:ReservedInstancesOfferingType ec2:ResourceTag/${TagKey} ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResourcePolicy [permission only]	Grants permission to describe an IAM policy that enables cross-account sharing	Read	ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetRouteServerAssociations	Grants permission to get associations for a route server	Read	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRouteServerPropagations	Grants permission to get propagations for a route server	Read	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRouteServerRoutingDatabase	Grants permission to get the routing database for a route server	Read	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetSecurityGroupsForVpc	Grants permission to retrieve a list of security groups for a specified VPC	Read	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSerialConsoleAccessStatus	Grants permission to retrieve the access status of your account to the EC2 serial console of all instances	Read		ec2:Region	
GetSnapshotBlockPublicAccessState	Grants permission to retrieve the current state of the block public access for snapshots setting for a Region	Read		ec2:Region	
GetSpotPlacementScores	Grants permission to calculate the Spot placement score for a Region or Availability Zone based on the specified target capacity and compute requirements	Read		ec2:Region	
GetSubnetCidrReservations	Grants permission to retrieve information about the subnet CIDR reservations	Read		ec2:Region	
GetTransitGatewayAttachmentPropagations	Grants permission to list the route tables to which a resource attachment propagates routes	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTransitGatewayMeteringPolicyEntries	Grants permission to list the entries for a transit gateway metering policy	List	transit-gateway-metering-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMeteringPolicyId	
				ec2:Region	
GetTransitGatewayMulticastDomainAssociations	Grants permission to get information about the associations for a transit gateway multicast domain	List	transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
GetTransitGatewayPolicyTableAssociations	Grants permission to get information about associations for a transit gateway policy table	List	transit-gateway-policy-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTransitGatewayPolicyTableEntries	Grants permission to get information about associations for a transit gateway policy table entry	List	transit-gateway-policy-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	
				ec2:Region	
GetTransitGatewayPrefixListReferences	Grants permission to get information about prefix list references for a transit gateway route table	List		ec2:Region	
GetTransitGatewayRouteTableAssociations	Grants permission to get information about associations for a transit gateway route table	List		ec2:Region	
GetTransitGatewayRouteTablePropagations	Grants permission to get information about the route table propagations for a transit gateway route table	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetVerifiedAccessEndpointPolicy	Grants permission to show the Verified Access policy associated with the endpoint	List	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetVerifiedAccessEndpointTargets	Grants permission to get verified access endpoint targets	List	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetVerifiedAccessGroupPolicy	Grants permission to show the contents of the Verified Access policy associated with the group	List	verified-access-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetVerifiedAccessInstanceWebAcl [permission only]	Grants permission to show the AWS Web Application Firewall (WAF) web access control list (ACL) for a Verified Access instance	List	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetVpcResourcesBlockingEncryptionEnforcement	Grants permission to describe resources that would block VPC Encryption Control enforcement	List	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
GetVpnConnectionDeviceSampleConfiguration	Grants permission to download an AWS-provided sample configuration file to be used with the customer gateway device	List	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpn-connection-device-type*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
GetVpnConnectionDeviceTypes	Grants permission to obtain a list of customer gateway devices for which sample configuration files can be provided	List		ec2:Region	
GetVpnTunnelReplacementStatus	Grants permission to view available tunnel endpoint maintenance events	List	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ImportByoipCidrToIpam [permission only]	Grants permission to transfer existing BYOIP IPv4 CIDRs to IPAM	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportClientVpnClientCertificateRevocationList	Grants permission to upload a client certificate revocation list to a Client VPN endpoint	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ImportImage	Grants permission to import single or multi-volume disk images or EBS snapshots into an Amazon Machine Image (AMI)	Write	image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:RootDeviceType	ec2:CreateTags
			import-image-task*	aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:ResourceTag/${TagKey} ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportInstance	Grants permission to create an import instance task using metadata from a disk image	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CpuOptionsAmdSevSnp ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeThroughput ec2:VolumeType	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	
ImportKeyPair	Grants permission to import a public key from an RSA key pair that was created with a third-party tool	Write	key-pair*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportSnapshot	Grants permission to import a disk into an EBS snapshot	Write	import-snapshot-task*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			snapshot*	aws:RequestTag/${TagKey} aws:TagKeys ec2:Owner ec2:ParentVolume ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportVolume	Grants permission to create an import volume task using metadata from a disk image	Write	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	
InjectApiError [permission only]	Grants permission to temporarily inject errors for target API requests	Write		ec2:FisActionId ec2:FisTargetArns ec2:Region	
ListImagesInRecycleBin	Grants permission to list Amazon Machine Images (AMIs) that are currently in the Recycle Bin	List		ec2:Region	
ListSnapshotsInRecycleBin	Grants permission to list the Amazon EBS snapshots that are currently in the Recycle Bin	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListVolumesInRecycleBin	Grants permission to list EBS volumes in Recycle Bin	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
LockSnapshot	Grants permission to lock an Amazon EBS snapshot in either governance or compliance mode to protect it against accidental or malicious deletions	Write	snapshot*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotCoolOffPeriod ec2:SnapshotID ec2:SnapshotLockDuration ec2:SnapshotTime ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ModifyAddressAttribute	Grants permission to modify an attribute of the specified Elastic IP address	Write	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Attribute ec2:Attribute/${AttributeName} ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyAvailabilityZoneGroup	Grants permission to modify the opt-in status of the Local Zone and Wavelength Zone group for your account	Write		ec2:Region	
ModifyCapacityReservation	Grants permission to modify a Capacity Reservation's capacity and the conditions under which it is to be released	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:CapacityReservationFleet	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyCapacityReservationFleet	Grants permission to modify a Capacity Reservation Fleet	Write	capacity-reservation-fleet*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	ec2:ModifyCapacityReservation
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyClientVpnEndpoint	Grants permission to modify a Client VPN endpoint	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:SamlProviderArn ec2:ServerCertificateArn	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
ModifyDefaultCreditSpecification	Grants permission to change the account level default credit option for CPU usage of burstable performance instances	Write		ec2:Region	
ModifyEbsDefaultKmsKeyId	Grants permission to change the default customer master key (CMK) for EBS encryption by default for your account	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyFleet	Grants permission to modify an EC2 Fleet	Write	fleet*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			launch-template	aws:ResourceTag/${TagKey} ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyFpgaImageAttribute	Grants permission to modify an attribute of an Amazon FPGA Image (AFI)	Write	fpga-image*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:Owner ec2:Public ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyHosts	Grants permission to modify a Dedicated Host	Write	dedicated-host*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyIdFormat	Grants permission to modify the ID format for a resource	Write		ec2:Region	
ModifyIdentityIdFormat	Grants permission to modify the ID format of a resource for a specific principal in your account	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyImageAttribute	Grants permission to modify an attribute of an Amazon Machine Image (AMI)	Write	image*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceAttribute	Grants permission to modify an attribute of an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeInitiali	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				zationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceCapacityReservationAttributes	Grants permission to modify the Capacity Reservation settings for a stopped instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
			capacity-reservation	aws:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceConnectEndpoint	Grants permission to modify an existing EC2 Instance Connect Endpoint	Write	instance-connect-endpoint*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceCpuOptions	Grants permission to modify the CPU options on an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceCreditSpecification	Grants permission to modify the credit option for CPU usage on an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceEventStartTime	Grants permission to modify the start time for a scheduled EC2 instance event	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceEventWindow	Grants permission to modify the specified event window	Write	instance-event-window*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceMaintenanceOptions	Grants permission to modify the recovery behaviour for an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceMetadataDefaults	Grants permission to modify the default instance metadata service (IMDS) settings for your account in the specified Region	Write		ec2:Attribute/${AttributeName} ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceMetadataOptions	Grants permission to modify the metadata options for an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceNetworkPerformanceOptions	Grants permission to modify the network performance options for an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstancePlacement	Grants permission to modify the placement attributes for an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
			dedicated-host	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyIpam	Grants permission to modify the configurations of an Amazon VPC IP Address Manager (IPAM)	Write	ipam*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyIpamPolicyAllocationRules	Grants permission to modify the rules that define how Amazon VPC IP Address Manager (IPAM) pools allocate IP addresses to AWS resource types within an IPAM policy	Write	ipam-policy*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyIpamPool	Grants permission to modify the configurations of an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ModifyIpamPrefixListResolver	Grants permission to modify an IPAM prefix list resolver	Write	ipam-prefix-list-resolver*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
			ipam-scope	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ModifyIpamPrefixListResolverTarget	Grants permission to modify an IPAM prefix list resolver target	Write	ipam-prefix-list-resolver-target*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyIpamResourceCidr	Grants permission to modify the configurations of an Amazon VPC IP Address Manager (IPAM) resource CIDR	Write	ipam-scope*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyIpamResourceDiscovery	Grants permission to modify a resource discovery	Write	ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyIpamScope	Grants permission to modify the configurations of an Amazon VPC IP Address Manager (IPAM) scope	Write	ipam-scope*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyLaunchTemplate	Grants permission to modify a launch template	Write	launch-template*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyLocalGatewayRoute	Grants permission to modify a local gateway route	Write	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
			local-gateway-virtual-interface-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:ResourceTag/${TagKey} ec2:AuthorizedUser ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			prefix-list	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyManagedPrefixList	Grants permission to modify a managed prefix list	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:IpamPrefixListResolverTargetId ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyNetworkInterfaceAttribute	Grants permission to modify an attribute of a network interface	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyOdbNetworkPeering [permission only]	Grants permission to allow Oracle Database@AWS to modify the settings of a peering connection between an ODB network and a VPC	Permissions management	vpc*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyPrivateDnsNameOptions	Grants permission to modify the options for instance hostnames for the specified instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyPublicIpDnsNameOptions	Grants permission to modify public hostname options for a network interface	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyReservedInstances	Grants permission to modify attributes of one or more Reserved Instances	Write	reserved-instances*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:InstanceType ec2:ReservedInstancesOfferingType ec2:ResourceTag/${TagKey} ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ModifyRouteServer	Grants permission to modify a route server	Write	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifySecurityGroupRules	Grants permission to modify the rules of a security group	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			security-group-rule*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			prefix-list	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifySnapshotAttribute	Grants permission to add or remove permission settings for a snapshot	Permissions management	snapshot*	aws:ResourceTag/${TagKey} ec2:Add/group ec2:Add/userId ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:Owner ec2:ParentVolume ec2:Remove/group ec2:Remove/userId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifySnapshotTier	Grants permission to archive Amazon EBS snapshots	Write	snapshot*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeSize	
				ec2:Region	
ModifySpotFleetRequest	Grants permission to modify a Spot Fleet request	Write	spot-fleet-request*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			launch-template	aws:ResourceTag/${TagKey} ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifySubnetAttribute	Grants permission to modify an attribute of a subnet	Write	subnet*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyTrafficMirrorFilterNetworkServices	Grants permission to allow or restrict mirroring network services	Write	traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyTrafficMirrorFilterRule	Grants permission to modify a traffic mirror rule	Write	traffic-mirror-filter*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-filter-rule*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyTrafficMirrorSession	Grants permission to modify a traffic mirror session	Write	traffic-mirror-session*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
			traffic-mirror-filter	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-target	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyTransitGateway	Grants permission to modify a transit gateway	Write	transit-gateway*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:transitGatewayId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyTransitGatewayMeteringPolicy	Grants permission to modify a transit gateway metering policy	Write	transit-gateway-metering-policy*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:transitGatewayMeteringPolicyId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyTransitGatewayPrefixListReference	Grants permission to modify a transit gateway prefix list reference	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyTransitGatewayVpcAttachment	Grants permission to modify a VPC attachment on a transit gateway	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVerifiedAccessEndpoint	Grants permission to modify the configuration of a Verified Access endpoint	Write	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
			verified-access-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ModifyVerifiedAccessEndpointPolicy	Grants permission to modify the specified Verified Access endpoint policy	Write	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVerifiedAccessGroup	Grants permission to modify the specified Verified Access Group configuration	Write	verified-access-group*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
			verified-access-instance	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVerifiedAccessGroupPolicy	Grants permission to modify the specified Verified Access group policy	Write	verified-access-group*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVerifiedAccessInstance	Grants permission to modify the configuration of the specified Verified Access instance	Write	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVerifiedAccessInstanceLoggingConfiguration	Grants permission to modify the logging configuration for the specified Verified Access instance	Write	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVerifiedAccessTrustProvider	Grants permission to modify the configuration of the specified Verified Access trust provider	Write	verified-access-trust-provider*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVolume	Grants permission to modify the parameters of an EBS volume	Write	volume*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVolumeAttribute	Grants permission to modify an attribute of a volume	Write	volume*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcAttribute	Grants permission to modify an attribute of a VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcBlockPublicAccessExclusion	Grants permission to modify an exclusion list for blocked public access on a VPC	Write	vpc-block-public-access-exclusion*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyVpcBlockPublicAccessOptions	Grants permission to modify options for blocked public access on a VPC	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcEncryptionControl	Grants permission to modify an existing VPC Encryption Control	Write	vpc-encryption-control*	aws:ResourceTag/${TagKey} ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcEndpoint	Grants permission to modify an attribute of a VPC endpoint	Write	vpc-endpoint*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceServiceRegion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcEndpointConnectionNotification	Grants permission to modify a connection notification for a VPC endpoint or VPC endpoint service	Write	vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			vpc-endpoint-service	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcEndpointServiceConfiguration	Grants permission to modify the attributes of a VPC endpoint service configuration	Write	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceServicePrivateDnsName ec2:VpceSupportedRegion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ModifyVpcEndpointServicePayerResponsibility	Grants permission to modify the payer responsibility for a VPC endpoint service	Write	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcEndpointServicePermissions	Grants permission to modify the permissions for a VPC endpoint service	Permissions management	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcPeeringConnectionOptions	Grants permission to modify the VPC peering connection options on one side of a VPC peering connection	Write	vpc-peering-connection*	aws:ResourceTag/${TagKey} ec2:AccepterVpc ec2:Attribute ec2:Attribute/${AttributeName} ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpcTenancy	Grants permission to modify the instance tenancy attribute of a VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpnConnection	Grants permission to modify the target gateway of a Site-to-Site VPN connection	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AuthenticationType ec2:DPDTimeoutSeconds ec2:GatewayType ec2:IKEVersions ec2:InsideTunnelCidr	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InsideTunnelIpv6Cidr ec2:Phase1DHGroup ec2:Phase1EncryptionAlgorithms ec2:Phase1IntegrityAlgorithms ec2:Phase1LifetimeSeconds ec2:Phase2DHGroup ec2:Phase2EncryptionAlgorithms ec2:Phase2IntegrityAlgorithms	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Phase2LifetimeSeconds ec2:RekeyFuzzPercentage ec2:RekeyMarginTimeSeconds ec2:ReplayWindowSizePackets ec2:ResourceTag/${TagKey} ec2:RoutingType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpnConnectionOptions	Grants permission to modify the connection options for your Site-to-Site VPN connection	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpnTunnelCertificate	Grants permission to modify the certificate for a Site-to-Site VPN connection	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVpnTunnelOptions	Grants permission to modify the options for a Site-to-Site VPN connection	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AuthenticationType ec2:DPDTimeoutSeconds ec2:GatewayType ec2:IKEVersions ec2:InsideTunnelCidr	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InsideTunnelIpv6Cidr ec2:Phase1DHGroup ec2:Phase1EncryptionAlgorithms ec2:Phase1IntegrityAlgorithms ec2:Phase1LifetimeSeconds ec2:Phase2DHGroup ec2:Phase2EncryptionAlgorithms ec2:Phase2IntegrityAlgorithms	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Phase2LifetimeSeconds ec2:RekeyFuzzPercentage ec2:RekeyMarginTimeSeconds ec2:ReplayWindowSizePackets ec2:ResourceTag/${TagKey} ec2:RoutingType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
MonitorInstances	Grants permission to enable detailed monitoring for a running instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
MoveAddressToVpc	Grants permission to move an Elastic IP address from the EC2-Classic platform to the EC2-VPC platform	Write		ec2:Region	
MoveByoipCidrToIpam	Grants permission to move a BYOIP IPv4 CIDR to Amazon VPC IP Address Manager (IPAM) from a public IPv4 pool	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
MoveCapacityReservationInstances	Grants permission to move available capacity from a source Capacity Reservation to a destination Capacity Reservation	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CapacityReservationFleet ec2:CreateDate ec2:DestinationCapacityReservationId ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:OutpostArn ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PauseVolumeIO [permission only]	Grants permission to temporarily pause I/O operations for a target Amazon EBS volume	Write	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
ProvisionByoipCidr	Grants permission to provision an address range for use in AWS through bring your own IP addresses (BYOIP), and to create a corresponding address pool	Write		ec2:Region	
ProvisionIpamByoasn	Grants permission to provision an Autonomous System Number (ASN) for use in an Amazon Web Services account	Write	ipam*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ProvisionIpamPoolCidr	Grants permission to provision a CIDR to an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipam-external-resource-verification-token	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ProvisionPublicIpv4PoolCidr	Grants permission to provision a CIDR to a public IPv4 pool	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv4pool-ec2*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
PurchaseCapacityBlock	Grants permission to purchase a Capacity Block offering	Write	capacity-reservation*	aws:RequestTag/${TagKey} aws:TagKeys ec2:CapacityReservationFleet	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PurchaseCapacityBlockExtension	Grants permission to purchase a Capacity Block extension	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:CapacityReservationFleet	
				ec2:Region	
PurchaseHostReservation	Grants permission to purchase a reservation with configurations that match those of a Dedicated Host	Write	dedicated-host*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
				ec2:Region	
PurchaseReservedInstancesOffering	Grants permission to purchase a Reserved Instance offering	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PurchaseScheduledInstances	Grants permission to purchase one or more Scheduled Instances with a specified schedule	Write		ec2:Region	
PutResourcePolicy [permission only]	Grants permission to attach an IAM policy that enables cross-account sharing to a resource	Permissions management	ipam-pool	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			verified-access-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RebootInstances	Grants permission to request a reboot of one or more instances	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
RegisterImage	Grants permission to register an Amazon Machine Image (AMI)	Write	image*	aws:RequestTag/${TagKey} aws:TagKeys ec2:ImageID ec2:Owner	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:ResourceTag/${TagKey} ec2:OutpostArn ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:SourceOutpostArn ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterInstanceEventNotificationAttributes	Grants permission to add tags to the set of tags to include in notifications about scheduled events for your instances	Write		ec2:Region	
RegisterTransitGatewayMulticastGroupMembers	Grants permission to register one or more network interfaces as a member of a group IP address in a transit gateway multicast domain	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterTransitGatewayMulticastGroupSources	Grants permission to register one or more network interfaces as a source of a group IP address in a transit gateway multicast domain	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectCapacityReservationBillingOwnership	Grants permission to reject a request to assign billing of the available capacity of a shared Capacity Reservation to your account	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:CapacityReservationFleet ec2:CreateDate ec2:DestinationCapacityReservationId ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:OutpostArn ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectTransitGatewayMulticastDomainAssociations	Grants permission to reject requests to associate cross-account subnets with a transit gateway multicast domain	Write	transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
			transit-gateway-multicast-domain	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectTransitGatewayPeeringAttachment	Grants permission to reject a transit gateway peering attachment request	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	
				ec2:Region	
RejectTransitGatewayVpcAttachment	Grants permission to reject a request to attach a VPC to a transit gateway	Write	transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
RejectVpcEndpointConnections	Grants permission to reject one or more VPC endpoint connection requests to a VPC endpoint service	Write	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectVpcPeeringConnection	Grants permission to reject a VPC peering connection request	Write	vpc-peering-connection*	aws:ResourceTag/${TagKey} ec2:AccepterVpc ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReleaseAddress	Grants permission to release an Elastic IP address	Write	elastic-ip	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	
				ec2:Region	
ReleaseHosts	Grants permission to release one or more On-Demand Dedicated Hosts	Write	dedicated-host*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ReleaseIpamPoolAllocation	Grants permission to release an allocation within an Amazon VPC IP Address Manager (IPAM) pool	Write	ipam-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReplaceIamInstanceProfileAssociation	Grants permission to replace an IAM instance profile for an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
ReplaceImageCriteriaInAllowedImagesSettings	Grants permission to replace image criteria in allowed images settings	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReplaceNetworkAclAssociation	Grants permission to change which network ACL a subnet is associated with	Write	network-acl*	aws:ResourceTag/${TagKey} ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReplaceNetworkAclEntry	Grants permission to replace an entry (rule) in a network ACL	Write	network-acl*	aws:ResourceTag/${TagKey} ec2:NetworkAclID ec2:ResourceTag/${TagKey} ec2:Vpc	
				ec2:Region	
ReplaceRoute	Grants permission to replace a route within a route table in a VPC	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ReplaceRouteTableAssociation	Grants permission to change the route table that is associated with a subnet	Write	route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc	
			internet-gateway	aws:ResourceTag/${TagKey} ec2:InternetGatewayID ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ipv4pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			ipv6pool-ec2	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ReplaceTransitGatewayRoute	Grants permission to replace a route in a transit gateway route table	Write	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
			transit-gateway-attachment	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ReplaceVpnTunnel	Grants permission to replace a VPN tunnel	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ReportInstanceStatus	Grants permission to submit feedback about the status of an instance	Write	instance*	ec2:AvailabilityZoneId ec2:InstanceBandwidthWeighting ec2:InstanceID	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RequestSpotFleet	Grants permission to create a Spot Fleet request	Write	spot-fleet-request*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			image	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			key-pair	aws:ResourceTag/${TagKey} ec2:KeyPairName ec2:KeyPairType ec2:ResourceTag/${TagKey}	
			launch-template	aws:ResourceTag/${TagKey} ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:ResourceTag/${TagKey} ec2:OutpostArn ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:SourceOutpostArn ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	
RequestSpotInstances	Grants permission to create a Spot Instance request	Write	spot-instances-request*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			key-pair	aws:ResourceTag/${TagKey} ec2:KeyPairName ec2:KeyPairType ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:ResourceTag/${TagKey} ec2:AuthorizedUser ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:Permission ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			placement-group	aws:ResourceTag/${TagKey} ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	
			security-group	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:ResourceTag/${TagKey} ec2:OutpostArn ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:SourceOutpostArn ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetAddressAttribute	Grants permission to reset the attribute of the specified IP address	Write	elastic-ip*	aws:ResourceTag/${TagKey} ec2:AllocationId ec2:Attribute ec2:Attribute/${AttributeName} ec2:Domain ec2:PublicIpAddress ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetEbsDefaultKmsKeyId	Grants permission to reset the default customer master key (CMK) for EBS encryption for your account to use the AWS-managed CMK for EBS	Write		ec2:Region	
ResetFpgaImageAttribute	Grants permission to reset an attribute of an Amazon FPGA Image (AFI) to its default value	Write	fpga-image*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:Owner ec2:Public ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetImageAttribute	Grants permission to reset an attribute of an Amazon Machine Image (AMI) to its default value	Write	image*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetInstanceAttribute	Grants permission to reset an attribute of an instance to its default value	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ProductCode	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetNetworkInterfaceAttribute	Grants permission to reset an attribute of a network interface	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetSnapshotAttribute	Grants permission to reset permission settings for a snapshot	Permissions management	snapshot*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
RestoreAddressToClassic	Grants permission to restore an Elastic IP address that was previously moved to the EC2-VPC platform back to the EC2-Classic platform	Write		ec2:Region	
RestoreImageFromRecycleBin	Grants permission to restore an Amazon Machine Image (AMI) from the Recycle Bin	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
RestoreManagedPrefixListVersion	Grants permission to restore the entries from a previous version of a managed prefix list to a new version of the prefix list	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreSnapshotFromRecycleBin	Grants permission to restore an Amazon EBS snapshot from the Recycle Bin	Write	snapshot*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreSnapshotTier	Grants permission to restore an archived Amazon EBS snapshot for use temporarily or permanently, or modify the restore period or restore type for a snapshot that was previously temporarily restored	Write	snapshot*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreVolumeFromRecycleBin	Grants permission to restore an EBS volume from Recycle Bin	Write	volume*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:ParentSnapshot ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeInitializationRate	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RevokeClientVpnIngress	Grants permission to remove an inbound authorization rule from a Client VPN endpoint	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
RevokeSecurityGroupEgress	Grants permission to remove one or more outbound rules from a VPC security group	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RevokeSecurityGroupIngress	Grants permission to remove one or more inbound rules from a security group	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RunInstances	Grants permission to launch one or more instances	Write	image*	aws:ResourceTag/${TagKey} ec2:ImageID ec2:ImageType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Owner ec2:Public ec2:ResourceTag/${TagKey} ec2:RootDeviceType	ec2:CreateTags iam:PassRole ssm:GetParameters

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPu	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:RootDeviceType ec2:Tenancy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface*	aws:RequestTag/${TagKey} aws:TagKeys ec2:AssociatePublicIpAddress ec2:AuthorizedService ec2:AvailabilityZone ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ManagedResourceOperator	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:NetworkInterfaceID ec2:Subnet ec2:Vpc	
			security-group*	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			capacity-reservation	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:LaunchTemplate	
			elastic-gpu	aws:ResourceTag/${TagKey} ec2:ElasticGpuType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			elastic-inference		
			group		
			key-pair	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:KeyPairName ec2:KeyPairType ec2:LaunchTemplate ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			launch-template	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	
			license-configuration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			placement-group	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot	aws:ResourceTag/${TagKey} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotID ec2:SnapshotTime ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume	aws:RequestTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ManagedResourceOperator ec2:ParentSnapshot	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeID ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: EC2-Classic-EBS		image* instance* security-group* volume* key-pair placement-group snapshot		
	SCENARIO: EC2-Classic-InstanceStore		image* instance* security-group* key-pair placement-group snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: EC2-VPC-EBS		image* instance* network-interface* security-group* volume* key-pair placement-group snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: EC2-VPC-EBS-Subnet		image* instance* network-interface* security-group* subnet* volume* key-pair placement-group snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: EC2-VPC-InstanceStore		image* instance* network-interface* security-group* key-pair placement-group snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: EC2-VPC-InstanceStore-Subnet		image* instance* network-interface* security-group* subnet* key-pair placement-group snapshot		
RunScheduledInstances	Grants permission to launch one or more Scheduled Instances	Write		ec2:Region	
SearchLocalGatewayRoutes	Grants permission to search for routes in a local gateway route table	List	local-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
SearchTransitGatewayMulticastGroups	Grants permission to search for groups, sources, and members in a transit gateway multicast domain	List	transit-gateway-multicast-domain*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchTransitGatewayRoutes	Grants permission to search for routes in a transit gateway route table	List	transit-gateway-route-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendDiagnosticInterrupt	Grants permission to send a diagnostic interrupt to an Amazon EC2 instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendSpotInstanceInterruptions [permission only]	Grants permission to interrupt a Spot Instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
StartDeclarativePoliciesReport	Grants permission to start a declarative policies report	Read		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartInstances	Grants permission to start a stopped instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ResourceTag/${TagKey} ec2:RootDeviceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Tenancy	
			license-configuration		
				ec2:Region	
StartNetworkInsightsAccessScopeAnalysis	Grants permission to start a Network Access Scope analysis	Write	network-insights-access-scope*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	ec2:CreateTags
			network-insights-access-scope-analysis*	aws:RequestTag/${TagKey} aws:TagKeys	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartNetworkInsightsAnalysis	Grants permission to start analyzing a specified path	Write	network-insights-analysis*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			network-insights-path*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartVpcEndpointServicePrivateDnsVerification	Grants permission to start the private DNS verification process for a VPC endpoint service	Write	vpc-endpoint-service*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceSupportedRegion	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopInstances	Grants permission to stop an Amazon EBS-backed instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Terminate ClientVpn Connections	Grants permission to terminate active Client VPN endpoint connections	Write	client-vpn-endpoint*	aws:ResourceTag/${TagKey} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Terminate Instances	Grants permission to shut down one or more instances	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UnassignIpv6Addresses	Grants permission to unassign one or more IPv6 addresses from a network interface	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UnassignPrivateIpAddresses	Grants permission to unassign one or more secondary private IP addresses from a network interface	Write	network-interface*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UnassignPrivateNatGatewayAddress	Grants permission to unassign secondary private IPv4 addresses from a private NAT gateway	Write	natgateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UnlockSnapshot	Grants permission to unlock a snapshot that is locked in governance mode or in compliance mode while still in the cooling-off period	Write	snapshot*	aws:ResourceTag/${TagKey} ec2:Encrypted ec2:Owner ec2:ParentVolume ec2:ResourceTag/${TagKey} ec2:SnapshotCoolOffPeriod ec2:SnapshotID ec2:SnapshotLockDuration ec2:SnapshotTime ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Unmonitor Instances	Grants permission to disable detailed monitoring for a running instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
UpdateCapacityManagerOrganizationsAccess	Grants permission to update the Organizations access setting for EC2 Capacity Manager	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateInterruptibleCapacityReservationAllocation	Grants permission to update the number of instances allocated to an interruptible reservation, allowing you to add more capacity or reclaim capacity to your source Capacity Reservation	Write	capacity-reservation*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CreateDate ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:InstanceCount ec2:InstanceMatchCriteria	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:InstancePlatform ec2:InstanceType ec2:InterruptibleCapacityReservationId ec2:InterruptionType ec2:IsInterruptible ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:TargetInstanceCount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Tenancy	
				ec2:Region	
UpdateSecurityGroupRuleDescriptionsEgress	Grants permission to update descriptions for one or more outbound rules in a VPC security group	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSecurityGroupRuleDescriptionsIngress	Grants permission to update descriptions for one or more inbound rules in a security group	Write	security-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc	
				ec2:Region	
WithdrawByoipCidr	Grants permission to stop advertising an address range that was provisioned for use in AWS through bring your own IP addresses (BYOIP)	Write		ec2:Region	

Resource types defined by Amazon EC2

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
elastic-ip	arn:${Partition}:ec2:${Region}:${Account}:elastic-ip/${AllocationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AllocationId ec2:Attribute ec2:Attribute/${AttributeName} ec2:Domain ec2:PublicIpAddress ec2:Region ec2:ResourceTag/${TagKey}
capacity-block	arn:${Partition}:ec2:${Region}:${Account}:capacity-block/${CapacityBlockId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region

Resource types	ARN	Condition keys
		ec2:ResourceTag/${TagKey}
capacity-manager-data-export	arn:${Partition}:ec2:${Region}:${Account}:capacity-manager-data-export/${CapacityManagerDataExportId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
capacity-reservation-fleet	arn:${Partition}:ec2:${Region}:${Account}:capacity-reservation-fleet/${CapacityReservationFleetId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
capacity-reservation	arn:${Partition}:ec2:${Region}:${Account}:capacity-reservation/${CapacityReservationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CapacityReservationFleet ec2:CommitmentDuration ec2:CreateDate ec2:DestinationCapacityReservationId ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:EphemeralStorage

Resource types	ARN	Condition keys
		ec2:InstanceCount ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:InterruptibleCapacityReservationId ec2:InterruptionType ec2:IsInterruptible ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:OutpostArn ec2:PlacementGroup ec2:Region ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId ec2:TargetInstanceCount ec2:Tenancy

Resource types	ARN	Condition keys
carrier-gateway	arn:${Partition}:ec2:${Region}:${Account}:carrier-gateway/${CarrierGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:Vpc
certificate	arn:${Partition}:acm:${Region}:${Account}:certificate/${CertificateId}	

Resource types	ARN	Condition keys
client-vpn-endpoint	arn:${Partition}:ec2:${Region}:${Account}:client-vpn-endpoint/${ClientVpnEndpointId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:ClientRootCertificateChainArn ec2:CloudwatchLogGroupArn ec2:CloudwatchLogStreamArn ec2:DirectoryArn ec2:Region ec2:ResourceTag/${TagKey} ec2:SamlProviderArn ec2:ServerCertificateArn

Resource types	ARN	Condition keys
customer-gateway	arn:${Partition}:ec2:${Region}:${Account}:customer-gateway/${CustomerGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
declarative-policies-report	arn:${Partition}:ec2:${Region}:${Account}:declarative-policies-report/${DeclarativePoliciesReportId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
dedicated-host	arn:${Partition}:ec2:${Region}:${Account}:dedicated-host/${DedicatedHostId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AutoPlacement ec2:AvailabilityZone ec2:HostRecovery ec2:InstanceType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Quantity ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
dhcp-options	arn:${Partition}:ec2:${Region}:${Account}:dhcp-options/${DhcpOptionsId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:DhcpOptionsID ec2:Region ec2:ResourceTag/${TagKey}
egress-only-internet-gateway	arn:${Partition}:ec2:${Region}:${Account}:egress-only-internet-gateway/${EgressOnlyInternetGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
elastic-gpu	arn:${Partition}:ec2:${Region}:${Account}:elastic-gpu/${ElasticGpuId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:ElasticGpuType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/${TagKey}
elastic-inference	arn:${Partition}:elastic-inference:${Region}:${Account}:elastic-inference-accelerator/${AcceleratorId}	
export-image-task	arn:${Partition}:ec2:${Region}:${Account}:export-image-task/${ExportImageTaskId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
export-instance-task	arn:${Partition}:ec2:${Region}:${Account}:export-instance-task/${ExportTaskId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
fleet	arn:${Partition}:ec2:${Region}:${Account}:fleet/${FleetId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
fpga-image	arn:${Partition}:ec2:${Region}:${Account}:fpga-image/${FpgaImageId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Owner ec2:Public ec2:Region ec2:ResourceTag/${TagKey}
host-reservation	arn:${Partition}:ec2:${Region}:${Account}:host-reservation/${HostReservationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
image	arn:${Partition}:ec2:${Region}::image/${ImageId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:ImageID ec2:ImageType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Owner ec2:Public ec2:Region ec2:ResourceTag/${TagKey} ec2:RootDeviceType

Resource types	ARN	Condition keys
image-usage-report	arn:${Partition}:ec2:${Region}:${Account}:image-usage-report/${ImageUsageReportId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
import-image-task	arn:${Partition}:ec2:${Region}:${Account}:import-image-task/${ImportImageTaskId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
import-snapshot-task	arn:${Partition}:ec2:${Region}:${Account}:import-snapshot-task/${ImportSnapshotTaskId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
instance-connect-endpoint	arn:${Partition}:ec2:${Region}:${Account}:instance-connect-endpoint/${InstanceConnectEndpointId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:SubnetID
instance-event-window	arn:${Partition}:ec2:${Region}:${Account}:instance-event-window/${InstanceEventWindowId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
instance	arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile

Resource types	ARN	Condition keys
		ec2:InstanceType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:NewInstanceProfile ec2:PlacementGroup ec2:ProductCode ec2:Region ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy

Resource types	ARN	Condition keys
internet-gateway	arn:${Partition}:ec2:${Region}:${Account}:internet-gateway/${InternetGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:InternetGatewayID ec2:Region ec2:ResourceTag/${TagKey}
ipam-external-resource-verification-token	arn:${Partition}:ec2::${Account}:ipam-external-resource-verification-token/${IpamExternalResourceVerificationTokenId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
ipam	arn:${Partition}:ec2::${Account}:ipam/${IpamId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
ipam-policy	arn:${Partition}:ec2::${Account}:ipam-policy/${IpamPolicyId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
ipam-pool	arn:${Partition}:ec2::${Account}:ipam-pool/${IpamPoolId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
ipam-prefix-list-resolver	arn:${Partition}:ec2::${Account}:ipam-prefix-list-resolver/${IpamPrefixListResolverId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
ipam-prefix-list-resolver-target	arn:${Partition}:ec2::${Account}:ipam-prefix-list-resolver-target/${IpamPrefixListResolverTargetId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
ipam-resource-discovery-association	arn:${Partition}:ec2::${Account}:ipam-resource-discovery-association/${IpamResourceDiscoveryAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
ipam-resource-discovery	arn:${Partition}:ec2::${Account}:ipam-resource-discovery/${IpamResourceDiscoveryId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
ipam-scope	arn:${Partition}:ec2::${Account}:ipam-scope/${IpamScopeId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
coip-pool	arn:${Partition}:ec2:${Region}:${Account}:coip-pool/${Ipv4PoolCoipId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
ipv4pool-ec2	arn:${Partition}:ec2:${Region}:${Account}:ipv4pool-ec2/${Ipv4PoolEc2Id}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
ipv6pool-ec2	arn:${Partition}:ec2:${Region}:${Account}:ipv6pool-ec2/${Ipv6PoolEc2Id}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
key-pair	arn:${Partition}:ec2:${Region}:${Account}:key-pair/${KeyPairName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:IsLaunchTemplateResource ec2:KeyPairName ec2:KeyPairType ec2:LaunchTemplate ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
launch-template	arn:${Partition}:ec2:${Region}:${Account}:launch-template/${LaunchTemplateId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ManagedResourceOperator ec2:Region ec2:ResourceTag/${TagKey}
license-configuration	arn:${Partition}:license-manager:${Region}:${Account}:license-configuration:${LicenseConfigurationId}	

Resource types	ARN	Condition keys
local-gateway	arn:${Partition}:ec2:${Region}:${Account}:local-gateway/${LocalGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
local-gateway-route-table-virtual-interface-group-association	arn:${Partition}:ec2:${Region}:${Account}:local-gateway-route-table-virtual-interface-group-association/${LocalGatewayRouteTableVirtualInterfaceGroupAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
local-gateway-route-table-vpc-association	arn:${Partition}:ec2:${Region}:${Account}:local-gateway-route-table-vpc-association/${LocalGatewayRouteTableVpcAssociationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
local-gateway-route-table	arn:${Partition}:ec2:${Region}:${Account}:local-gateway-route-table/${LocalGatewayRoutetableId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
local-gateway-virtual-interface-group	arn:${Partition}:ec2:${Region}:${Account}:local-gateway-virtual-interface-group/${LocalGatewayVirtualInterfaceGroupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
local-gateway-virtual-interface	arn:${Partition}:ec2:${Region}:${Account}:local-gateway-virtual-interface/${LocalGatewayVirtualInterfaceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
mac-modification-task	arn:${Partition}:ec2:${Region}:${Account}:mac-modification-task/${MacModificationTaskId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
natgateway	arn:${Partition}:ec2:${Region}:${Account}:natgateway/${NatGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:Vpc
network-acl	arn:${Partition}:ec2:${Region}:${Account}:network-acl/${NaclId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:NetworkAclID ec2:Region ec2:ResourceTag/${TagKey} ec2:Vpc

Resource types	ARN	Condition keys
network-insights-access-scope-analysis	arn:${Partition}:ec2:${Region}:${Account}:network-insights-access-scope-analysis/${NetworkInsightsAccessScopeAnalysisId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
network-insights-access-scope	arn:${Partition}:ec2:${Region}:${Account}:network-insights-access-scope/${NetworkInsightsAccessScopeId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
network-insights-analysis	arn:${Partition}:ec2:${Region}:${Account}:network-insights-analysis/${NetworkInsightsAnalysisId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
network-insights-path	arn:${Partition}:ec2:${Region}:${Account}:network-insights-path/${NetworkInsightsPathId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
network-interface	arn:${Partition}:ec2:${Region}:${Account}:network-interface/${NetworkInterfaceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AssociatePublicIpAddress ec2:Attribute ec2:Attribute/${AttributeName} ec2:AuthorizedService ec2:AuthorizedUser ec2:AvailabilityZone ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ManagedResourceOperator ec2:NetworkInterfaceID ec2:Permission ec2:Region

Resource types	ARN	Condition keys
		ec2:ResourceTag/${TagKey} ec2:Subnet ec2:Vpc
outpost-lag	arn:${Partition}:ec2:${Region}:${Account}:outpost-lag/${OutpostLagId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
placement-group	arn:${Partition}:ec2:${Region}:${Account}:placement-group/${PlacementGroupName}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:PlacementGroupName ec2:PlacementGroupStrategy ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
prefix-list	arn:${Partition}:ec2:${Region}:${Account}:prefix-list/${PrefixListId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:IpamPrefixListResolverTargetId ec2:Region ec2:ResourceTag/${TagKey}
replace-root-volume-task	arn:${Partition}:ec2:${Region}:${Account}:replace-root-volume-task/${ReplaceRootVolumeTaskId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
reserved-instances	arn:${Partition}:ec2:${Region}:${Account}:reserved-instances/${ReservationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:InstanceType ec2:Region ec2:ReservedInstancesOfferingType ec2:ResourceTag/${TagKey} ec2:Tenancy
group	arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}	
role	arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}	

Resource types	ARN	Condition keys
route-server-endpoint	arn:${Partition}:ec2:${Region}:${Account}:route-server-endpoint/${RouteServerEndpointId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:Region ec2:ResourceTag/${TagKey}
route-server	arn:${Partition}:ec2:${Region}:${Account}:route-server/${RouteServerId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
route-server-peer	arn:${Partition}:ec2:${Region}:${Account}:route-server-peer/${RouteServerPeerId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AvailabilityZone ec2:Region ec2:ResourceTag/${TagKey}
route-table	arn:${Partition}:ec2:${Region}:${Account}:route-table/${RouteTableId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:RouteTableID ec2:Vpc

Resource types	ARN	Condition keys
security-group	arn:${Partition}:ec2:${Region}:${Account}:security-group/${SecurityGroupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc
security-group-rule	arn:${Partition}:ec2:${Region}:${Account}:security-group-rule/${SecurityGroupRuleId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
snapshot	arn:${Partition}:ec2:${Region}::snapshot/${SnapshotId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Add/group ec2:Add/userId ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:Encrypted ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Location ec2:OutpostArn ec2:Owner ec2:ParentSnapshot ec2:ParentVolume ec2:ProductCode ec2:Region

Resource types	ARN	Condition keys
		ec2:Remove/group ec2:Remove/userId ec2:ResourceTag/${TagKey} ec2:SnapshotCoolOffPeriod ec2:SnapshotID ec2:SnapshotLockDuration ec2:SnapshotTime ec2:SourceAvailabilityZone ec2:SourceOutpostArn ec2:VolumeSize

Resource types	ARN	Condition keys
spot-fleet-request	arn:${Partition}:ec2:${Region}:${Account}:spot-fleet-request/${SpotFleetRequestId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
spot-instances-request	arn:${Partition}:ec2:${Region}:${Account}:spot-instances-request/${SpotInstanceRequestId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
subnet-cidr-reservation	arn:${Partition}:ec2:${Region}:${Account}:subnet-cidr-reservation/${SubnetCidrReservationId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
subnet	arn:${Partition}:ec2:${Region}:${Account}:subnet/${SubnetId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc

Resource types	ARN	Condition keys
traffic-mirror-filter	arn:${Partition}:ec2:${Region}:${Account}:traffic-mirror-filter/${TrafficMirrorFilterId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
traffic-mirror-filter-rule	arn:${Partition}:ec2:${Region}:${Account}:traffic-mirror-filter-rule/${TrafficMirrorFilterRuleId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
traffic-mirror-session	arn:${Partition}:ec2:${Region}:${Account}:traffic-mirror-session/${TrafficMirrorSessionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
traffic-mirror-target	arn:${Partition}:ec2:${Region}:${Account}:traffic-mirror-target/${TrafficMirrorTargetId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
transit-gateway-attachment	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-attachment/${TransitGatewayAttachmentId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId
transit-gateway-connect-peer	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-connect-peer/${TransitGatewayConnectPeerId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayConnectPeerId

Resource types	ARN	Condition keys
transit-gateway	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway/${TransitGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayId
transit-gateway-metering-policy	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-metering-policy/${TransitGatewayMeteringPolicyId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayMeteringPolicyId

Resource types	ARN	Condition keys
transit-gateway-multicast-domain	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-multicast-domain/${TransitGatewayMulticastDomainId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayMulticastDomainId
transit-gateway-policy-table	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-policy-table/${TransitGatewayPolicyTableId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId

Resource types	ARN	Condition keys
transit-gateway-route-table-announcement	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-route-table-announcement/${TransitGatewayRouteTableAnnouncementId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableAnnouncementId
transit-gateway-route-table	arn:${Partition}:ec2:${Region}:${Account}:transit-gateway-route-table/${TransitGatewayRouteTableId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:transitGatewayRouteTableId

Resource types	ARN	Condition keys
verified-access-endpoint	arn:${Partition}:ec2:${Region}:${Account}:verified-access-endpoint/${VerifiedAccessEndpointId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
verified-access-endpoint-target	arn:${Partition}:ec2:${Region}:${Account}:verified-access-endpoint-target/${VerifiedAccessEndpointTargetId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
verified-access-group	arn:${Partition}:ec2:${Region}:${Account}:verified-access-group/${VerifiedAccessGroupId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
verified-access-instance	arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
verified-access-policy	arn:${Partition}:ec2:${Region}:${Account}:verified-access-policy/${VerifiedAccessPolicyId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
verified-access-trust-provider	arn:${Partition}:ec2:${Region}:${Account}:verified-access-trust-provider/${VerifiedAccessTrustProviderId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
volume	arn:${Partition}:ec2:${Region}:${Account}:volume/${VolumeId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:AvailabilityZoneId ec2:Encrypted ec2:IsLaunchTemplateResource ec2:KmsKeyId ec2:LaunchTemplate ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ParentVolume ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
		ec2:VolumeID ec2:VolumeInitializationRate ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType
vpc-block-public-access-exclusion	arn:${Partition}:ec2:${Region}:${Account}:vpc-block-public-access-exclusion/${VpcBlockPublicAccessExclusionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
vpc-encryption-control	arn:${Partition}:ec2:${Region}:${Account}:vpc-encryption-control/${VpcEncryptionControlId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}
vpc-endpoint-connection	arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint-connection/${VpcEndpointConnectionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
vpc-endpoint	arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint/${VpcEndpointId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpcePrivateDnsPreference ec2:VpcePrivateDnsSpecifiedDomains ec2:VpceServiceName ec2:VpceServiceOwner ec2:VpceServiceRegion

Resource types	ARN	Condition keys
vpc-endpoint-service	arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint-service/${VpcEndpointServiceId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey} ec2:VpceMultiRegion ec2:VpceServicePrivateDnsName ec2:VpceServiceRegion ec2:VpceSupportedRegion

Resource types	ARN	Condition keys
vpc-endpoint-service-permission	arn:${Partition}:ec2:${Region}:${Account}:vpc-endpoint-service-permission/${VpcEndpointServicePermissionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
vpc-flow-log	arn:${Partition}:ec2:${Region}:${Account}:vpc-flow-log/${VpcFlowLogId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
vpc	arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Ipv4IpamPoolId ec2:Ipv6IpamPoolId ec2:Region ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID

Resource types	ARN	Condition keys
vpc-peering-connection	arn:${Partition}:ec2:${Region}:${Account}:vpc-peering-connection/${VpcPeeringConnectionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:AccepterVpc ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:RequesterVpc ec2:ResourceTag/${TagKey} ec2:VpcPeeringConnectionID
vpn-concentrator	arn:${Partition}:ec2:${Region}:${Account}:vpn-concentrator/${VpnConcentratorId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
vpn-connection-device-type	arn:${Partition}:ec2:${Region}:${Account}:vpn-connection-device-type/${VpnConnectionDeviceTypeId}	ec2:Region

Resource types	ARN	Condition keys
vpn-connection	arn:${Partition}:ec2:${Region}:${Account}:vpn-connection/${VpnConnectionId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:AuthenticationType ec2:DPDTimeoutSeconds ec2:GatewayType ec2:IKEVersions ec2:InsideTunnelCidr ec2:InsideTunnelIpv6Cidr ec2:Phase1DHGroup ec2:Phase1EncryptionAlgorithms ec2:Phase1IntegrityAlgorithms ec2:Phase1LifetimeSeconds

Resource types	ARN	Condition keys
		ec2:Phase2DHGroup ec2:Phase2EncryptionAlgorithms ec2:Phase2IntegrityAlgorithms ec2:Phase2LifetimeSeconds ec2:Region ec2:RekeyFuzzPercentage ec2:RekeyMarginTimeSeconds ec2:ReplayWindowSizePackets ec2:ResourceTag/${TagKey} ec2:RoutingType

Resource types	ARN	Condition keys
vpn-gateway	arn:${Partition}:ec2:${Region}:${Account}:vpn-gateway/${VpnGatewayId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Condition keys for Amazon EC2

Amazon EC2 defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString
ec2:AccepterVpc	Filters access by the ARN of an accepter VPC in a VPC peering connection	ARN

Condition keys	Description	Type
ec2:Add/group	Filters access by the group being added to a snapshot	String
ec2:Add/userId	Filters access by the account id being added to a snapshot	String
ec2:AllocationId	Filters access by the allocation ID of the Elastic IP address	String
ec2:AssociatePublicIpAddress	Filters access by whether the user wants to associate a public IP address with the instance	Bool
ec2:Attribute	Filters access by an attribute of a resource	String
ec2:Attribute/${AttributeName}	Filters access by an attribute being set on a resource	String
ec2:AuthenticationType	Filters access by the authentication type for the VPN tunnel endpoints	String
ec2:AuthorizedService	Filters access by the AWS service that has permission to use a resource	String
ec2:AuthorizedUser	Filters access by an IAM principal that has permission to use a resource	String
ec2:AutoPlacement	Filters access by the Auto Placement properties of a Dedicated Host	String
ec2:AvailabilityZone	Filters access by the name of an Availability Zone in an AWS Region	String
ec2:AvailabilityZoneId	Filters access by the ID of an Availability Zone in an AWS Region	String

Condition keys	Description	Type
ec2:CapacityReservationFleet	Filters access by the ARN of the Capacity Reservation Fleet	ARN
ec2:ClientRootCertificateChainArn	Filters access by the ARN of the client root certificate chain	ARN
ec2:CloudwatchLogGroupArn	Filters access by the ARN of the CloudWatch Logs log group	ARN
ec2:CloudwatchLogStreamArn	Filters access by the ARN of the CloudWatch Logs log stream	ARN
ec2:CommitmentDuration	Filters access by commitment duration of the Capacity Reservation	Numeric
ec2:CpuOptionsAmdSevSnp	Filters access by the state of AMD SEV-SNP CPU Options. Currently, only US East (Ohio) and Europe (Ireland) are supported	String
ec2:CreateAction	Filters access by the name of a resource-creating API action	String
ec2:CreateDate	Filters access by the date and time at which the Capacity Reservation was created	Date
ec2:DPDTimeoutSeconds	Filters access by the duration after which DPD timeout occurs on a VPN tunnel	Numeric
ec2:DestinationCapacityReservationId	Filters access by the ID of the Capacity Reservation that you want to move capacity into	ARN

Condition keys	Description	Type
ec2:DhcpOptionsID	Filters access by the ID of a dynamic host configuration protocol (DHCP) options set	String
ec2:DirectoryArn	Filters access by the ARN of the directory	ARN
ec2:Domain	Filters access by the domain of the Elastic IP address	String
ec2:EbsOptimized	Filters access by whether the instance is enabled for EBS optimization	Bool
ec2:ElasticGpuType	Filters access by the type of Elastic Graphics accelerator	String
ec2:Encrypted	Filters access by whether the EBS volume is encrypted	Bool
ec2:EndDate	Filters access by the date and time at which the Capacity Reservation ends	Date
ec2:EndDateType	Filters access by the way in which the Capacity Reservation ends	String
ec2:EphemeralStorage	Filters access by whether the instance is enabled for ephemeral storage	Bool
ec2:FisActionId	Filters access by the ID of an AWS FIS action	String
ec2:FisTargetArns	Filters access by the ARN of an AWS FIS target	ArrayOfARN
ec2:GatewayType	Filters access by the gateway type for a VPN endpoint on the AWS side of a VPN connection	String
ec2:HostRecovery	Filters access by whether host recovery is enabled for a Dedicated Host	String
ec2:IKEVersions	Filters access by the internet key exchange (IKE) versions that are permitted for a VPN tunnel	ArrayOfString

Condition keys	Description	Type
ec2:ImageID	Filters access by the ID of an image	String
ec2:ImageType	Filters access by the type of image (machine, aki, or ari)	String
ec2:InsideTunnelCidr	Filters access by the range of inside IP addresses for a VPN tunnel	String
ec2:InsideTunnelIpv6Cidr	Filters access by a range of inside IPv6 addresses for a VPN tunnel	String
ec2:InstanceAutoRecovery	Filters access by whether the instance type supports auto recovery	String
ec2:InstanceBandwidthWeighting	Filters access by the bandwidth weighting of an instance	String
ec2:InstanceCount	Filters access by the number of instances	Numeric
ec2:InstanceID	Filters access by the ID of an instance	String
ec2:InstanceMarketType	Filters access by the market or purchasing option of an instance (capacity-block, on-demand, or spot)	String
ec2:InstanceMatchCriteria	Filters access by the type of instance launches that the Capacity Reservation accepts	String
ec2:InstanceMetadataTags	Filters access by whether the instance allows access to instance tags from the instance metadata	String
ec2:InstancePlatform	Filters access by the type of operating system for which the Capacity Reservation reserves capacity	ARN
ec2:InstanceProfile	Filters access by the ARN of an instance profile	ARN

Condition keys	Description	Type
ec2:InstanceType	Filters access by the type of instance	String
ec2:InternetGatewayID	Filters access by the ID of an internet gateway	String
ec2:InterruptibleCapacityReservationId	Filters access by the ID of an interruptible Capacity Reservation	String
ec2:InterruptionType	Filters access by the type of interruption	String
ec2:IpamPrefixListResolverTargetId	Filters access by the IPAM prefix list resolver target ID that is syncing CIDRs to a managed prefix list	String
ec2:Ipv4IpamPoolId	Filters access by the ID of an IPAM pool provided for IPv4 CIDR block allocation	String
ec2:Ipv6IpamPoolId	Filters access by the ID of an IPAM pool provided for IPv6 CIDR block allocation	String
ec2:IsInterruptible	Filters access by whether Capacity Reservations are interruptible	Bool
ec2:IsLaunchTemplateResource	Filters access by whether users are able to override resources that are specified in the launch template	Bool
ec2:KeyPairName	Filters access by the name of a key pair	String
ec2:KeyPairType	Filters access by the type of a key pair	String

Condition keys	Description	Type
ec2:KmsKeyId	Filters access by the ID of an AWS KMS key provided in the request	String
ec2:LaunchTemplate	Filters access by the ARN of a launch template	ARN
ec2:Location	Filters access by the destination for the snapshot copy	String
ec2:ManagedResourceOperator	Filters access by the presence of an EC2 operator provisioning a managed resource	String
ec2:MetadataHttpEndpoint	Filters access by whether the HTTP endpoint is enabled for the instance metadata service	String
ec2:MetadataHttpPutResponseHopLimit	Filters access by the allowed number of hops when calling the instance metadata service	Numeric
ec2:MetadataHttpTokens	Filters access by whether tokens are required when calling the instance metadata service (optional or required)	String
ec2:NetworkAclID	Filters access by the ID of a network access control list (ACL)	String
ec2:NetworkInterfaceID	Filters access by the ID of an elastic network interface	String
ec2:NewInstanceProfile	Filters access by the ARN of the instance profile being attached	ARN
ec2:OutpostArn	Filters access by the ARN of the Outpost	ARN
ec2:Owner	Filters access by the owner of the resource (amazon, aws-marketplace, or an AWS account ID)	String

Condition keys	Description	Type
ec2:ParentSnapshot	Filters access by the ARN of the parent snapshot	ARN
ec2:ParentVolume	Filters access by the ARN of the parent volume from which the snapshot was created	ARN
ec2:Permission	Filters access by the type of permission for a resource (INSTANCE-ATTACH or EIP-ASSOCIATE)	String
ec2:Phase1DHGroup	Filters access by the Diffie-Hellman group numbers that are permitted for a VPN tunnel for the phase 1 IKE negotiations	ArrayOfString
ec2:Phase1EncryptionAlgorithms	Filters access by the encryption algorithms that are permitted for a VPN tunnel for the phase 1 IKE negotiations	ArrayOfString
ec2:Phase1IntegrityAlgorithms	Filters access by the integrity algorithms that are permitted for a VPN tunnel for the phase 1 IKE negotiations	ArrayOfString
ec2:Phase1LifetimeSeconds	Filters access by the lifetime in seconds for phase 1 of the IKE negotiations for a VPN tunnel	Numeric
ec2:Phase2DHGroup	Filters access by the Diffie-Hellman group numbers that are permitted for a VPN tunnel for the phase 2 IKE negotiations	ArrayOfString
ec2:Phase2EncryptionAlgorithms	Filters access by the encryption algorithms that are permitted for a VPN tunnel for the phase 2 IKE negotiations	ArrayOfString
ec2:Phase2IntegrityAlgorithms	Filters access by the integrity algorithms that are permitted for a VPN tunnel for the phase 2 IKE negotiations	ArrayOfString

Condition keys	Description	Type
ec2:Phase2LifetimeSeconds	Filters access by the lifetime in seconds for phase 2 of the IKE negotiations for a VPN tunnel	Numeric
ec2:PlacementGroup	Filters access by the ARN of the placement group	ARN
ec2:PlacementGroupName	Filters access by the name of a placement group	String
ec2:PlacementGroupStrategy	Filters access by the instance placement strategy used by the placement group (cluster, spread, or partition)	String
ec2:ProductCode	Filters access by the product code that is associated with the AMI	String
ec2:Public	Filters access by whether the image has public launch permissions	Bool
ec2:PublicIpAddress	Filters access by a public IP address	String
ec2:Quantity	Filters access by the number of Dedicated Hosts in a request	Numeric
ec2:Region	Filters access by the name of the AWS Region	String
ec2:RekeyFuzzPercentage	Filters access by the percentage of increase of the rekey window (determined by the rekey margin time) within which the rekey time is randomly selected for a VPN tunnel	Numeric
ec2:RekeyMarginTimeSeconds	Filters access by the margin time before the phase 2 lifetime expires for a VPN tunnel	Numeric

Condition keys	Description	Type
ec2:Remove/group	Filters access by the group being removed from a snapshot	String
ec2:Remove/userId	Filters access by the account id being removed from a snapshot	String
ec2:ReplayWindowSizePackets	Filters access by the number of packets in an IKE replay window	String
ec2:RequesterVpc	Filters access by the ARN of a requester VPC in a VPC peering connection	ARN
ec2:ReservedInstancesOfferingType	Filters access by the payment option of the Reserved Instance offering (No Upfront, Partial Upfront, or All Upfront)	String
ec2:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
ec2:RoleDelivery	Filters access by the version of the instance metadata service for retrieving IAM role credentials for EC2	Numeric
ec2:RootDeviceType	Filters access by the root device type of the instance (ebs or instance-store)	String
ec2:RouteTableID	Filters access by the ID of a route table	String
ec2:RoutingType	Filters access by the routing type for the VPN connection	String
ec2:SamlProviderArn	Filters access by the ARN of the IAM SAML identity provider	ARN

Condition keys	Description	Type
ec2:SecurityGroupID	Filters access by the ID of a security group	String
ec2:ServerCertificateArn	Filters access by the ARN of the server certificate	ARN
ec2:SnapshotCoolOffPeriod	Filters access by the compliance mode cooling-off period	Numeric
ec2:SnapshotID	Filters access by the ID of a snapshot	String
ec2:SnapshotLockDuration	Filters access by the snapshot lock duration	Numeric
ec2:SnapshotTime	Filters access by the initiation time of a snapshot	String
ec2:SourceAvailabilityZone	Filters access by the name of the Availability Zone from which the request originated	String
ec2:SourceCapacityReservationId	Filters access by the ID of the Capacity Reservation from which you want to move capacity	ARN
ec2:SourceInstanceARN	Filters access by the ARN of the instance from which the request originated	ARN
ec2:SourceOutpostArn	Filters access by the ARN of the Outpost from which the request originated	ARN
ec2:Subnet	Filters access by the ARN of the subnet	ARN
ec2:SubnetID	Filters access by the ID of a subnet	String
ec2:TargetInstanceCount	Filters access by the number of instances the interruptible Capacity Reservation is assigned	Numeric

Condition keys	Description	Type
ec2:Tenancy	Filters access by the tenancy of the VPC or instance (default, dedicated, or host)	String
ec2:VolumeID	Filters access by the ID of a volume	String
ec2:VolumeInitializationRate	Filters access by the initialization rate of the volume, in MiBps	Numeric
ec2:VolumeIops	Filters access by the the number of input/output operations per second (IOPS) provisioned for the volume	Numeric
ec2:VolumeSize	Filters access by the size of the volume, in GiB	Numeric
ec2:VolumeThroughput	Filters access by the throughput of the volume, in MiBps	Numeric
ec2:VolumeType	Filters access by the type of volume (gp2, gp3, io1, io2, st1, sc1, or standard)	String
ec2:Vpc	Filters access by the ARN of the VPC	ARN
ec2:VpcID	Filters access by the ID of a virtual private cloud (VPC)	String
ec2:VpcPeeringConnectionID	Filters access by the ID of a VPC peering connection	String
ec2:VpceMultiRegion	Filters access by multi region of the VPC endpoint service	String
ec2:VpcePrivateDnsPreference	Filters access by the private DNS preference	String

Condition keys	Description	Type
ec2:VpcePrivateDnsSpecifiedDomains	Filters access by the private DNS domains	ArrayOfString
ec2:VpceServiceName	Filters access by the name of the VPC endpoint service	String
ec2:VpceServiceOwner	Filters access by the service owner of the VPC endpoint service (amazon, aws-marketplace, or an AWS account ID)	String
ec2:VpceServicePrivateDnsName	Filters access by the private DNS name of the VPC endpoint service	String
ec2:VpceServiceRegion	Filters access by the region of the VPC endpoint service	String
ec2:VpceSupportedRegion	Filters access by the supported region of the VPC endpoint service	String
ec2:transitGatewayAttachmentId	Filters access by the ID of a transit gateway attachment	String
ec2:transitGatewayConnectPeerId	Filters access by the ID of a transit gateway connect peer	String
ec2:transitGatewayId	Filters access by the ID of a transit gateway	String
ec2:transitGatewayMeteringPolicyId	Filters access by the ID of a metering policy id	String

Condition keys	Description	Type
ec2:transitGatewayMulticastDomainId	Filters access by the ID of a transit gateway multicast domain	String
ec2:transitGatewayPolicyTableId	Filters access by the ID of a transit gateway policy table	String
ec2:transitGatewayRouteTableAnnouncementId	Filters access by the ID of a transit gateway route table announcement	String
ec2:transitGatewayRouteTableId	Filters access by the ID of a transit gateway route table	String

Actions, resources, and condition keys for Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling (service prefix: `autoscaling`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon EC2 Auto Scaling
- Resource types defined by Amazon EC2 Auto Scaling
- Condition keys for Amazon EC2 Auto Scaling

Actions defined by Amazon EC2 Auto Scaling

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachInstances	Grants permission to attach one or more EC2 instances to the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
AttachLoadBalancerTargetGroups	Grants permission to attach one or more target groups to the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TargetGroupARNs	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachLoadBalancers	Grants permission to attach one or more load balancers to the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:LoadBalancerNames	
AttachTrafficSources	Grants permission to attach one or more traffic sources to an Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TrafficSourceIdentifiers	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDeleteScheduledAction	Grants permission to delete the specified scheduled actions	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
BatchPutScheduledUpdateGroupAction	Grants permission to create or update multiple scheduled scaling actions for an Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CancelInstanceRefresh	Grants permission to cancel an instance refresh operation in progress	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CompleteLifecycleAction	Grants permission to complete the lifecycle action for the specified token or instance with the specified result	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateAutoScalingGroup	Grants permission to create an Auto Scaling group with the specified name and attributes	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:CreateServiceLinkedRole iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				autoscaling:ImageId autoscaling:CapacityReservationIds autoscaling:CapacityReservationResourceGroupArns autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified autoscaling:LoadBa	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				lancerNames autoscaling:MaxSize autoscaling:MinSize autoscaling:TargetGroupARNs autoscaling:TrafficSourceIdentifiers autoscaling:VPCZoneIdentifiers aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLaunchConfiguration	Grants permission to create a launch configuration	Write	launchConfiguration*		
				autoscaling:ImageId	
				autoscaling:InstanceType	
				autoscaling:SpotPrice	
				autoscaling:MetadataHttpTokens	
				autoscaling:MetadataHttpPutResponseHopLimit	
				autoscaling:MetadataHttpEndpoint	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateOrUpdateTags	Grants permission to create or update tags for the specified Auto Scaling group	Tagging	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAutoScalingGroup	Grants permission to delete the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ForceDelete autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLaunchConfiguration	Grants permission to delete the specified launch configuration	Write	launchConfiguration*		
DeleteLifecycleHook	Grants permission to deletes the specified lifecycle hook	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteNotificationConfiguration	Grants permission to delete the specified notification	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePolicy	Grants permission to delete the specified Auto Scaling policy	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteScheduledAction	Grants permission to delete the specified scheduled action	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteTags	Grants permission to delete the specified tags	Tagging	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteWarmPool	Grants permission to delete the warm pool associated with the Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DescribeAccountLimits	Grants permission to describe the current Auto Scaling resource limits for your AWS account	List			
DescribeAccountSettings	Grants permission to describe the current Amazon EC2 Auto Scaling account settings for your account	List			
DescribeAdjustmentTypes	Grants permission to describe the policy adjustment types for use with PutScalingPolicy	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAutoScalingGroups	Grants permission to describe one or more Auto Scaling groups. If a list of names is not provided, the call describes all Auto Scaling groups	List			
DescribeAutoScalingInstances	Grants permission to describe one or more Auto Scaling instances. If a list is not provided, the call describes all instances	List			
DescribeAutoScalingNotificationTypes	Grants permission to describe the notification types that are supported by Auto Scaling	List			
DescribeInstanceRefreshes	Grants permission to describe one or more instance refreshes for an Auto Scaling group	List			
DescribeLaunchConfigurations	Grants permission to describe one or more launch configurations. If you omit the list of names, then the call describes all launch configurations	List			
DescribeLifecycleHookTypes	Grants permission to describe the available types of lifecycle hooks	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLifecycleHooks	Grants permission to describe the lifecycle hooks for the specified Auto Scaling group	List			
DescribeLoadBalancerTargetGroups	Grants permission to describe the target groups for the specified Auto Scaling group	List			
DescribeLoadBalancers	Grants permission to describe the load balancers for the specified Auto Scaling group	List			
DescribeMetricCollectionTypes	Grants permission to describe the available CloudWatch metrics for Auto Scaling	List			
DescribeNotificationConfigurations	Grants permission to describe the notification actions associated with the specified Auto Scaling group	List			
DescribePolicies	Grants permission to describe the policies for the specified Auto Scaling group	List			
DescribeScalingActivities	Grants permission to describe one or more scaling activities for the specified Auto Scaling group	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeScalingProcessTypes	Grants permission to describe the scaling process types for use with ResumeProcesses and SuspendProcesses	List			
DescribeScheduledActions	Grants permission to describe the actions scheduled for your Auto Scaling group that haven't run	List			
DescribeTags	Grants permission to describe the specified tags	Read			
DescribeTerminationPolicyTypes	Grants permission to describe the termination policies supported by Auto Scaling	List			
DescribeTrafficSources	Grants permission to describe the target groups for the specified Auto Scaling group	List			
DescribeWarmPool	Grants permission to describe the warm pool associated with the Auto Scaling group	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachInstances	Grants permission to remove one or more instances from the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DetachLoadBalancerTargetGroups	Grants permission to detach one or more target groups from the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TargetGroupARNs	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachLoadBalancers	Grants permission to remove one or more load balancers from the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:LoadBalancerNames	
DetachTrafficSources	Grants permission to detach one or more traffic sources from an Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
				autoscaling:TrafficSourceIdentifiers	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableMetricsCollection	Grants permission to disable monitoring of the specified metrics for the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
EnableMetricsCollection	Grants permission to enable monitoring of the specified metrics for the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
EnterStandby	Grants permission to move the specified instances into Standby mode	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExecutePolicy	Grants permission to execute the specified policy	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
ExitStandby	Grants permission to move the specified instances out of Standby mode	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
GetPredictiveScalingForecast	Grants permission to retrieve the forecast data for a predictive scaling policy	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
LaunchInstances	Grants permission to launch one or more EC2 instances in the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutAccountSetting	Grants permission to modify an account setting for your account	Write			
PutLifecycleHook	Grants permission to create or update a lifecycle hook for the specified Auto Scaling Group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutNotificationConfiguration	Grants permission to configure an Auto Scaling group to send notifications when specified events take place	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutScalingPolicy	Grants permission to create or update a policy for an Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
PutScheduledUpdateGroupAction	Grants permission to create or update a scheduled scaling action for an Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				autoscaling:MaxSize autoscaling:MinSize	
PutWarmPool	Grants permission to create or update the warm pool associated with the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
RecordLifecycleActionHeartbeat	Grants permission to record a heartbeat for the lifecycle action associated with the specified token or instance	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResumeProcesses	Grants permission to resume the specified suspended Auto Scaling processes, or all suspended process, for the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
RollbackInstanceRefresh	Grants permission to rollback an instance refresh operation in progress	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SetDesiredCapacity	Grants permission to set the size of the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetInstanceHealth	Grants permission to set the health status of the specified instance	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
SetInstanceProtection	Grants permission to update the instance protection settings of the specified instances	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
StartInstanceRefresh	Grants permission to start a new instance refresh operation	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				autoscaling:ImageId	
SuspendProcesses	Grants permission to suspend the specified Auto Scaling processes, or all processes, for the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
TerminateInstanceInAutoScalingGroup	Grants permission to terminate the specified instance and optionally adjust the desired group size	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAutoScalingGroup	Grants permission to update the configuration for the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				autoscaling:ImageId autoscaling:CapacityReservationIds autoscaling:CapacityReservationResourceGroupArns autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				autoscaling:MaxSize autoscaling:MinSize autoscaling:VPCZoneIdentifiers	

Resource types defined by Amazon EC2 Auto Scaling

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
autoScalingGroup	`arn:${Partition}:autoscaling:${Region}:${Account}:autoScalingGroup:${GroupId}:autoScalingGroupName/${GroupFriendlyName}`	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}
launchConfiguration	`arn:${Partition}:autoscaling:${Region}:${Account}:launchConfiguration:${`	

Resource types	ARN	Condition keys
	`Id}:launchConfigurationName/${Launch ConfigurationName}`	

Condition keys for Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
autoscaling:CapacityReservationIds	Filters access based on the Capacity Reservation IDs	ArrayOfString
autoscaling:CapacityReservationResourceGroupArns	Filters access based on the ARN of a Capacity Reservation resource group	ArrayOfString
autoscaling:ForceDelete	Filters access based on whether the force delete option is specified when deleting an Auto Scaling group	Bool
autoscaling:ImageId	Filters access based on the AMI ID for the launch configuration	String
autoscaling:InstanceType	Filters access based on the instance type for the launch configuration	String

Condition keys	Description	Type
autoscaling:InstanceTypes	Filters access based on the instance types present as overrides to a launch template for a mixed instances policy. Use it to qualify which instance types can be explicitly defined in the policy	String
autoscaling:LaunchConfigurationName	Filters access based on the name of a launch configuration	String
autoscaling:LaunchTemplateVersionSpecified	Filters access based on whether users can specify any version of a launch template or only the Latest or Default version	Bool
autoscaling:LoadBalancerNames	Filters access based on the name of the load balancer	ArrayOfString
autoscaling:MaxSize	Filters access based on the maximum scaling size in the request	Numeric
autoscaling:MetadataHttpEndpoint	Filters access based on whether the HTTP endpoint is enabled for the instance metadata service	String
autoscaling:MetadataHttpPutResponseHopLimit	Filters access based on the allowed number of hops when calling the instance metadata service	Numeric
autoscaling:MetadataHttpTokens	Filters access based on whether tokens are required when calling the instance metadata service (optional or required)	String

Condition keys	Description	Type
autoscaling:MinSize	Filters access based on the minimum scaling size in the request	Numeric
autoscaling:ResourceTag/${TagKey}	Filters access based on the tags associated with the resource	String
autoscaling:SpotPrice	Filters access based on the price for Spot Instances for the launch configuration	Numeric
autoscaling:TargetGroupARNs	Filters access based on the ARN of a target group	ArrayOfARN
autoscaling:TrafficSourceIdentifiers	Filters access based on the identifiers of the traffic sources	ArrayOfString
autoscaling:VPCZoneIdentifiers	Filters access based on the identifier of a VPC zone	ArrayOfString
aws:RequestTag/${TagKey}	Filters access based on the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access based on the tags associated with the resource	String
aws:TagKeys	Filters access based on the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon EC2 Image Builder

Amazon EC2 Image Builder (service prefix: `imagebuilder`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon EC2 Image Builder
- Resource types defined by Amazon EC2 Image Builder
- Condition keys for Amazon EC2 Image Builder

Actions defined by Amazon EC2 Image Builder

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelImageCreation	Grants permission to cancel an image creation	Write	image*		
CancelLifecycleExecution	Grants permission to cancel a lifecycle execution	Write	lifecycleExecution*		
CreateComponent	Grants permission to create a new component	Write	component*		imagebuilder:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateContainerRecipe	Grants permission to create a new Container Recipe	Write	containerRecipe*		ec2:DescribeImages ecr:DescribeImages ecr:DescribeRepositories imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:GetObject s3:ListBucket ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDistributionConfiguration	Grants permission to create a new distribution configuration	Write	distributionConfiguration*		ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplates ec2:ModifyLaunchTemplate imagebuilder:TagResource s3:ListBucket ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateImage	Grants permission to create a new image	Write	image*		ecr:BatchGetRepositoryScanningConfiguration ecr:DescribeRepositories iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetIn

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					frastructureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource inspector2:BatchGetAccountStatus
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateImagePipeline	Grants permission to create a new image pipeline	Write	imagePipeline*		ecr:BatchGetRepositoryScanningConfiguration ecr:DescribeRepositories iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetIn

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					frastructureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource inspector2:BatchGetAccountStatus
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateImageRecipe	Grants permission to create a new Image Recipe	Write	imageRecipe*		ec2:DescribeImages imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInfrastructureConfiguration	Grants permission to create a new infrastructure configuration	Write	infrastructureConfiguration*		ec2:DescribeAvailabilityZones ec2:DescribeHosts iam:PassRole imagebuilder:TagResource resource-groups:GetGroup sns:Publish

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/${TagKey} imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLifecyclePolicy	Grants permission to create a new lifecycle policy	Write	lifecyclePolicy*		iam:PassRole imagebuilder:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:LifecyclePolicyResourceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateWorkflow	Grants permission to create a new workflow	Write	workflow*		imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComponent	Grants permission to delete a component	Write	component*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteContainerRecipe	Grants permission to delete a container recipe	Write	containerRecipe*		
DeleteDistributionConfiguration	Grants permission to delete a distribution configuration	Write	distributionConfiguration*		
DeleteImage	Grants permission to delete an image	Write	image*		
DeleteImagePipeline	Grants permission to delete an image pipeline	Write	imagePipeline*		
DeleteImageRecipe	Grants permission to delete an image recipe	Write	imageRecipe*		
DeleteInfrastructureConfiguration	Grants permission to delete an infrastructure configuration	Write	infrastructureConfiguration*		
DeleteLifecyclePolicy	Grants permission to delete a lifecycle policy	Write	lifecyclePolicy*		
DeleteWorkflow	Grants permission to delete a workflow	Write	workflow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DistributeImage	Grants permission to distribute an image	Write	image*		ec2:DescribeImages iam:PassRole imagebuilder:GetDistributionConfiguration imagebuilder:GetImage imagebuilder:TagResource ssm:GetParameter
				aws:RequestTag/${TagKey} aws:TagKeys	
GetComponent	Grants permission to view details about a component	Read	component*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetComponentPolicy	Grants permission to view the resource policy associated with a component	Read	component*		
GetContainerRecipe	Grants permission to view details about a container recipe	Read	containerRecipe*		
GetContainerRecipePolicy	Grants permission to view the resource policy associated with a container recipe	Read	containerRecipe*		
GetDistributionConfiguration	Grants permission to view details about a distribution configuration	Read	distributionConfiguration*		
GetImage	Grants permission to view details about an image	Read	image*		
GetImagePipeline	Grants permission to view details about an image pipeline	Read	imagePipeline*		
GetImagePolicy	Grants permission to view the resource policy associated with an image	Read	image*		
GetImageRecipe	Grants permission to view details about an image recipe	Read	imageRecipe*		
GetImageRecipePolicy	Grants permission to view the resource policy associated with an image recipe	Read	imageRecipe*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInfrastructureConfiguration	Grants permission to view details about an infrastructure configuration	Read	infrastructureConfiguration*		
GetLifecycleExecution	Grants permission to view details about a lifecycle execution	Read	lifecycleExecution*		
GetLifecyclePolicy	Grants permission to view details about a lifecycle policy	Read	lifecyclePolicy*		
GetMarketplaceResource	Grants permission to retrieve Marketplace provided resource	Read	component*		
GetWorkflow	Grants permission to view details about a workflow	Read	workflow*		kms:Decrypt
GetWorkflowExecution	Grants permission to view details about a workflow execution	Read	workflowExecution*		
GetWorkflowStepExecution	Grants permission to view details about a workflow step execution	Read	workflowStepExecution*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportComponent	Grants permission to import a new component	Write	component *		imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportDiskImage	Grants permission to import a disk image	Write	imageVersion*		iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource s3:GetObject s3:ListBucket
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportVmImage	Grants permission to import an image	Write	imageVersion*		ec2:DescribeImages ec2:DescribeImportImageTasks iam:CreateServiceLinkedRole imagebuilder:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
ListComponentBuildVersions	Grants permission to list the component build versions in your account	List	allComponentBuildVersions*		
ListComponents	Grants permission to list the component versions owned by or shared with your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListContainerRecipes	Grants permission to list the container recipes owned by or shared with your account	List			
ListDistributionConfigurations	Grants permission to list the distribution configurations in your account	List			
ListImageBuildVersions	Grants permission to list the image build versions in your account	List	allImageBuildVersions*		
ListImagePackages	Grants permission to return a list of packages installed on the specified image	List	image*		
ListImagePipelineImages	Grants permission to return a list of images created by the specified pipeline	List	imagePipeline*		
ListImagePipelines	Grants permission to list the image pipelines in your account	List			
ListImageRecipes	Grants permission to list the image recipes owned by or shared with your account	List			
ListImageScanFindingAggregations	Grants permission to list aggregations on the image scan findings in your account	List	image imagePipeline		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListImageScanFindings	Grants permission to list the image scan findings for the images in your account	List	image		inspector2:ListFindings
			imagePipeline		
ListImages	Grants permission to list the image versions owned by or shared with your account	List			
ListInfrastructureConfigurations	Grants permission to list the infrastructure configurations in your account	List			
ListLifecycleExecutionResources	Grants permission to list resources for the specified lifecycle execution	List	lifecycleExecution*		
ListLifecycleExecutions	Grants permission to list lifecycle executions for the specified resource	List	image		
			lifecyclePolicy		
ListLifecyclePolicies	Grants permission to list the lifecycle policies in your account	List			
ListTagsForResource	Grants permission to list tags for an Image Builder resource	Read	component		
			containerRecipe		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			distributionConfiguration		
			image		
			imagePipeline		
			imageRecipe		
			infrastructureConfiguration		
			lifecyclePolicy		
			workflow		
ListWaitingWorkflowSteps	Grants permission to list waiting workflow steps for the caller account	List			
ListWorkflowBuildVersions	Grants permission to list the workflow build versions in your account	List	allWorkflowBuildVersions*		
ListWorkflowExecutions	Grants permission to list workflow executions for the specified image	List	image*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListWorkflowStepExecutions	Grants permission to list workflow step executions for the specified workflow	List	workflowExecution*		kms:Decrypt
ListWorkflows	Grants permission to list the workflow versions owned by or shared with your account	List			
PutComponentPolicy	Grants permission to set the resource policy associated with a component	Permissions management	component*		
PutContainerRecipePolicy	Grants permission to set the resource policy associated with a container recipe	Permissions management	containerRecipe*		
PutImagePolicy	Grants permission to set the resource policy associated with an image	Permissions management	image*		
PutImageRecipePolicy	Grants permission to set the resource policy associated with an image recipe	Permissions management	imageRecipe*		
RetryImage	Grants permission to retry an image creation	Write	image*		
SendWorkflowStepAction	Grants permission to send an action to a workflow step	Write	image*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			workflowStepExecution*		
StartImagePipelineExecution	Grants permission to create a new image from a pipeline	Write	imagePipeline*		iam:CreateServiceLinkedRole imagebuilder:GetImagePipeline imagebuilder:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
StartResourceStateUpdate	Grants permission to start a state update for the specified resource	Write	image*		
TagResource	Grants permission to tag an Image Builder resource	Tagging	component		
			containerRecipe		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			distributionConfiguration		
			image		
			imagePipeline		
			imageRecipe		
			infrastructureConfiguration		
			lifecyclePolicy		
			workflow		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag an Image Builder resource	Tagging	component		
			containerRecipe		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			distributionConfiguration		
			image		
			imagePipeline		
			imageRecipe		
			infrastructureConfiguration		
			lifecyclePolicy		
			workflow		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDistributionConfiguration	Grants permission to update an existing distribution configuration	Write	distributionConfiguration*		ec2:CreateLaunchTemplateVersion ec2:DescribeLaunchTemplates ec2:ModifyLaunchTemplate s3:ListBucket ssm:GetParameter

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateImagePipeline	Grants permission to update an existing image pipeline	Write	imagePipeline*		ecr:BatchGetRepositoryScanningConfiguration ecr:DescribeRepositories iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetIn

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					frastructureConfiguration imagebuilder:GetWorkflow inspector2:BatchGetAccountStatus
UpdateInfrastructureConfiguration	Grants permission to update an existing infrastructure configuration	Write	infrastructureConfiguration*		ec2:DescribeAvailabilityZones ec2:DescribeHosts iam:PassRole resource-groups:GetGroup sns:Publish

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/${TagKey} imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	
UpdateLifecyclePolicy	Grants permission to update an existing lifecycle policy	Write	lifecyclePolicy*		iam:PassRole
				imagebuilder:LifecyclePolicyResourceType	

Resource types defined by Amazon EC2 Image Builder

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
component	arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}/${ComponentBuildVersion}	aws:ResourceTag/${TagKey}
distributionConfiguration	arn:${Partition}:imagebuilder:${Region}:${Account}:distribution-configuration/${DistributionConfigurationName}	aws:ResourceTag/${TagKey}
image	arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}/${ImageBuildVersion}	aws:ResourceTag/${TagKey}
imageVersion	arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}	aws:ResourceTag/${TagKey}
imageRecipe	arn:${Partition}:imagebuilder:${Region}:${Account}:image-recipe/${ImageRecipeName}/${ImageRecipeVersion}	aws:ResourceTag/${TagKey}
containerRecipe	arn:${Partition}:imagebuilder:${Region}:${Account}:container-recipe/${ContainerRecipeName}/${ContainerRecipeVersion}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
imagePipeline	arn:${Partition}:imagebuilder:${Region}:${Account}:image-pipeline/${ImagePipelineName}	aws:ResourceTag/${TagKey}
infrastructureConfiguration	arn:${Partition}:imagebuilder:${Region}:${Account}:infrastructure-configuration/${ResourceId}	aws:ResourceTag/${TagKey}
lifecycleExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-execution/${LifecycleExecutionId}	
lifecyclePolicy	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-policy/${LifecyclePolicyName}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}/${WorkflowBuildVersion}	aws:ResourceTag/${TagKey}
workflowExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-execution/${WorkflowExecutionId}	
workflowStepExecution	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-step-execution/${WorkflowStepExecutionId}	
allComponentBuildVersions	arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}/*	

Resource types	ARN	Condition keys
allImageBuildVersions	arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}/*	
allWorkflowBuildVersions	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}/*	

Condition keys for Amazon EC2 Image Builder

Amazon EC2 Image Builder defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
imagebuilder:CreatedResourceTag/${TagKey}	Filters access by the tag key-value pairs attached to the resource created by Image Builder	String

Condition keys	Description	Type
imagebuilder:CreatedResourceTagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
imagebuilder:Ec2MetadataHttpTokens	Filters access by the EC2 Instance Metadata HTTP Token Requirement specified in the request	String
imagebuilder:LifecyclePolicyResourceType	Filters access by the Lifecycle Policy Resource Type specified in the request	String
imagebuilder:StatusTopicArn	Filters access by the SNS Topic Arn in the request to which terminal state notifications will be published	ARN

Actions, resources, and condition keys for Amazon Elastic Block Store

Amazon Elastic Block Store (service prefix: ebs) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Elastic Block Store
- Resource types defined by Amazon Elastic Block Store
- Condition keys for Amazon Elastic Block Store

Actions defined by Amazon Elastic Block Store

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CompleteSnapshot	Grants permission to seal and complete the snapshot after all of the required blocks of data have been written to it	Write	snapshot*		
				aws:ResourceTag/${TagKey}	
GetSnapshotBlock	Grants permission to return the data of a block in an Amazon Elastic Block Store (EBS) snapshot	Read	snapshot*		
				aws:ResourceTag/${TagKey}	
ListChangedBlocks	Grants permission to list the blocks that are different between two Amazon Elastic Block Store (EBS) snapshots of the same volume/snapshot lineage	Read	snapshot*		
				aws:ResourceTag/${TagKey}	
ListSnapshotBlocks	Grants permission to list the blocks in an Amazon Elastic Block Store (EBS) snapshot	Read	snapshot*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutSnapshotBlock	Grants permission to write a block of data to a snapshot created by the StartSnapshot operation	Write	snapshot*		
				aws:ResourceTag/${TagKey}	
StartSnapshot	Grants permission to create a new EBS snapshot	Write	snapshot		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ebs:Description ebs:ParentSnapshot ebs:VolumeSize	

Resource types defined by Amazon Elastic Block Store

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
snapshot	`arn:${Partition}:ec2:${Region}::snapshot/${SnapshotId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ebs:Description ebs:ParentSnapshot ebs:VolumeSize

Condition keys for Amazon Elastic Block Store

Amazon Elastic Block Store defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString
ebs:Description	Filters access by the description of the snapshot being created	String
ebs:ParentSnapshot	Filters access by the ARN of the parent snapshot	ARN
ebs:VolumeSize	Filters access by the size of the volume for the snapshot being created, in GiB	Numeric

Actions, resources, and condition keys for Amazon Elastic Container Registry

Amazon Elastic Container Registry (service prefix: `ecr`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Elastic Container Registry
- Resource types defined by Amazon Elastic Container Registry

- Condition keys for Amazon Elastic Container Registry

Actions defined by Amazon Elastic Container Registry

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchCheckLayerAvailability	Grants permission to check the availability of multiple image layers in a specified registry and repository	Read	repository*		
BatchDeleteImage	Grants permission to delete a list of specified images within a specified repository	Write	repository*		
BatchGetImage	Grants permission to get detailed information for specified images within a specified repository	Read	repository*		
BatchGetRepositoryScanningConfiguration	Grants permission to retrieve repository scanning configuration for a list of repositories	Read	repository*		
BatchImportUpstreamImage	Grants permission to retrieve the image from the upstream registry and import it to your private registry	Write	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
CompleteLayerUpload	Grants permission to inform Amazon ECR that the image layer upload for a specified registry, repository name, and upload ID, has completed	Write	repository*		
CreatePullThroughCacheRule	Grants permission to create new pull-through cache rule	Write			iam:CreateServiceLinkedRole
CreateRepository	Grants permission to create an image repository	Write	repository*		ecr:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRepositoryCreationTemplate	Grants permission to create the repository creation template	Write			ecr:CreateRepository ecr:PutLifecyclePolicy ecr:SetRepositoryPolicy iam:CreateServiceLinkedRole iam:PassRole
DeleteLifecyclePolicy	Grants permission to delete the specified lifecycle policy	Write	repository*		
DeletePullThroughCacheRule	Grants permission to delete the pull-through cache rule	Write			
DeleteRegistryPolicy	Grants permission to delete the registry policy	Permissions management			
DeleteRepository	Grants permission to delete an existing image repository	Write	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRepositoryCreationTemplate	Grants permission to delete the repository creation template	Write			
DeleteRepositoryPolicy	Grants permission to delete the repository policy from a specified repository	Permissions management	repository*		
DeleteSigningConfiguration	Grants permission to delete the signing configuration for the registry	Write			
DeregisterPullTimeUpdateExclusion	Grants permission to deregister a pull time update exclusion	Write			
DescribeImageReplicationStatus	Grants permission to retrieve replication status about an image in a registry, including failure reason if replication fails	Read	repository*		
DescribeImageScanFindings	Grants permission to describe the image scan findings for the specified image	Read	repository*		
DescribeImageSigningStatus	Grants permission to retrieve signing status about an image in a specified registry	Read	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeImages	Grants permission to get metadata about the images in a repository, including image size, image tags, and creation date	List	repository*		
DescribePullThroughCacheRules	Grants permission to describe the pull-through cache rules	List			
DescribeRegistry	Grants permission to describe the registry settings	Read			
DescribeRepositories	Grants permission to describe image repositories in a registry	Read	repository*		
DescribeRepositoryCreationTemplates	Grants permission to describe the repository creation template	Read			
GetAccountSetting	Grants permission to retrieve account settings	Read		ecr:AccountSetting	
GetAuthorizationToken	Grants permission to retrieve a token that is valid for a specified registry for 12 hours	Read			
GetDownloadUrlForLayer	Grants permission to retrieve the download URL corresponding to an image layer	Read	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetImageCopyStatus [permission only]	Grants permission to retrieve the status about an image copy	Read	repository*		
GetLifecyclePolicy	Grants permission to retrieve the specified lifecycle policy	Read	repository*		
GetLifecyclePolicyPreview	Grants permission to retrieve the results of the specified lifecycle policy preview request	Read	repository*		
GetRegistryPolicy	Grants permission to retrieve the registry policy	Read			
GetRegistryScanningConfiguration	Grants permission to retrieve registry scanning configuration	Read			
GetRepositoryPolicy	Grants permission to retrieve the repository policy for a specified repository	Read	repository*		
GetSigningConfiguration	Grants permission to retrieve the signing configuration for the registry	Read			
InitiateLayerUpload	Grants permission to notify Amazon ECR that you intend to upload an image layer	Write	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListImages	Grants permission to list all the image IDs for a given repository	List	repository*		
ListPullTimeUpdateExclusions	Grants permission to list pull time update exclusions for the registry	List			
ListTagsForResource	Grants permission to list the tags for an Amazon ECR resource	Read	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutAccountSetting	Grants permission to update account settings	Write		ecr:AccountSetting	
PutImage	Grants permission to create or update the image manifest associated with an image	Write	repository*		
PutImageScanningConfiguration	Grants permission to update the image scanning configuration for a repository	Write	repository*		
PutImageTagMutability	Grants permission to update the image tag mutability settings for a repository	Write	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutLifecyclePolicy	Grants permission to create or update a lifecycle policy	Write	repository*		
PutRegistryPolicy	Grants permission to update the registry policy	Permissions management			
PutRegistryScanningConfiguration	Grants permission to update registry scanning configuration	Write			
PutReplicationConfiguration	Grants permission to update the replication configuration for the registry	Write			iam:CreateServiceLinkedRole
PutSigningConfiguration	Grants permission to update the signing configuration for the registry	Write			
RegisterPullTimeUpdateExclusion	Grants permission to register a pull time update exclusion	Write			
ReplicateImage [permission only]	Grants permission to replicate images to the destination registry	Write	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetRepositoryPolicy	Grants permission to apply a repository policy on a specified repository to control access permissions	Permissions management	repository*		
StartImageScan	Grants permission to start an image scan	Write	repository*		
StartLifecyclePolicyPreview	Grants permission to start a preview of the specified lifecycle policy	Write	repository*		
TagResource	Grants permission to tag an Amazon ECR resource	Tagging	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag an Amazon ECR resource	Tagging	repository*		
				aws:TagKeys	
UpdateImageStorageClass	Grants permission to get update the storage class of a specified image within a specified repository	Write	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePullThroughCacheRule	Grants permission to update the pull-through cache rule	Write			
UpdateRepositoryCreationTemplate	Grants permission to update the repository creation template	Write			ecr:CreateRepository ecr:PutLifecyclePolicy ecr:SetRepositoryPolicy iam:CreateServiceLinkedRole iam:PassRole
UploadLayerPart	Grants permission to upload an image layer part to Amazon ECR	Write	repository*		
ValidatePullThroughCacheRule	Grants permission to validate the pull-through cache rule	Read			

Resource types defined by Amazon Elastic Container Registry

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
repository	`arn:${Partition}:ecr:${Region}:${Account}:repository/${RepositoryName}`	aws:ResourceTag/${TagKey} ecr:ResourceTag/${TagKey}

Condition keys for Amazon Elastic Container Registry

Amazon Elastic Container Registry defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tags in the request	ArrayOfString

Condition keys	Description	Type
ecr:AccountSetting	Filters access by the ECR account setting name	String
ecr:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String

Actions, resources, and condition keys for Amazon Elastic File System

Amazon Elastic File System (service prefix: `elasticfilesystem`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Elastic File System
- Resource types defined by Amazon Elastic File System
- Condition keys for Amazon Elastic File System

Actions defined by Amazon Elastic File System

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Backup [permission only]	Grants permission to start a backup job for an existing file system	Write	file-system*		
ClientMount [permission only]	Grants permission to allow an NFS client read-access to a file system	Read	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	
ClientRootAccess [permission only]	Grants permission to allow an NFS client root-access to a file system	Write	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ClientWrite [permission only]	Grants permission to allow an NFS client write-access to a file system	Write	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	
CreateAccessPoint	Grants permission to create an access point for the specified file system	Write	file-system*		elasticfilesystem:TagResource
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFileSystem	Grants permission to create a new, empty file system	Write		aws:RequestTag/${TagKey} aws:TagKeys elasticfilesystem:Encrypted	elasticfilesystem:TagResource
CreateMountTarget	Grants permission to create a mount target for a file system	Write	file-system*		
CreateReplicationConfiguration	Grants permission to create a new replication configuration	Write	file-system*		
CreateTags	Grants permission to create or overwrite tags associated with a file system; deprecated, see TagResource	Tagging	file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessPoint	Grants permission to delete the specified access point	Write	access-point*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFileSystem	Grants permission to delete a file system, permanently severing access to its contents	Write	file-system*		
DeleteFileSystemPolicy	Grants permission to delete the resource-level policy for a file system	Permissions management	file-system*		
DeleteMountTarget	Grants permission to delete the specified mount target	Write	file-system*		
DeleteReplicationConfiguration	Grants permission to delete a replication configuration	Write	file-system*		
DeleteTags	Grants permission to delete the specified tags from a file system; deprecated, see UntagResource	Tagging	file-system*		
				aws:TagKeys	
DescribeAccessPoints	Grants permission to view the descriptions of Amazon EFS access points	List	access-point		
			file-system		
DescribeAccountPreferences	Grants permission to view the account preferences in effect for an account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeBackupPolicy	Grants permission to view the BackupPolicy object for an Amazon EFS file system	Read	file-system*		
DescribeFileSystemPolicy	Grants permission to view the resource-level policy for an Amazon EFS file system	Read	file-system		
DescribeFileSystems	Grants permission to view the description of an Amazon EFS file system specified by file system CreationToken or FileSystemId; or to view the description of all file systems owned by the caller's AWS account in the AWS region of the endpoint that is being called	List	file-system		
DescribeLifecycleConfiguration	Grants permission to view the LifecycleConfiguration object for an Amazon EFS file system	Read	file-system*		
DescribeMountTargetSecurityGroups	Grants permission to view the security groups in effect for a mount target	Read	file-system*		
DescribeMountTargets	Grants permission to view the descriptions of all mount targets, or a specific mount target, for a file system	Read	file-system*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			access-point		
DescribeReplicationConfigurations	Grants permission to view the description of an Amazon EFS replication configuration specified by FileSystemId; or to view the description of all replication configurations owned by the caller's AWS account in the AWS region of the endpoint that is being called	List	file-system		
DescribeTags	Grants permission to view the tags associated with a file system	Read	file-system*		
ListTagsForResource	Grants permission to view the tags associated with the specified Amazon EFS resource	Read	access-point		
			file-system		
ModifyMountTargetSecurityGroups	Grants permission to modify the set of security groups in effect for a mount target	Write	file-system*		
PutAccountPreferences	Grants permission to set the account preferences of an account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutBackupPolicy	Grants permission to enable or disable automatic backups with AWS Backup by creating a new BackupPolicy object	Write	file-system*		
PutFileSystemPolicy	Grants permission to apply a resource-level policy that defines the actions allowed or denied from given actors for the specified file system	Permissions management	file-system*		
PutLifecycleConfiguration	Grants permission to enable lifecycle management by creating a new Lifecycle Configuration object	Write	file-system*		
ReplicationRead [permission only]	Grants permission to read file system data for replication	Read	file-system*		
ReplicationWrite [permission only]	Grants permission to replicate data to a file system	Write	file-system*		
Restore [permission only]	Grants permission to start a restore job for a backup of a file system	Write	file-system*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to create or overwrite tags associated with the specified Amazon EFS resource	Tagging	access-point		
			file-system		
				aws:RequestTag/${TagKey} aws:TagKeys elasticfilesystem:CreateAction	
UntagResource	Grants permission to delete the specified tags from an Amazon EFS resource	Tagging	access-point		
			file-system		
				aws:TagKeys	
UpdateFileSystem	Grants permission to update the throughput mode or the amount of provisioned throughput of an existing file system	Write	file-system*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFileSystemProtection	Grants permission to update the file system protection of an existing file system	Write	file-system*		

Resource types defined by Amazon Elastic File System

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
file-system	`arn:${Partition}:elasticfilesystem:${Region}:${Account}:file-system/${FileSystemId}`	aws:ResourceTag/${TagKey}
access-point	`arn:${Partition}:elasticfilesystem:${Region}:${Account}:access-point/${AccessPointId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Elastic File System

Amazon Elastic File System defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString
elasticfilesystem:AccessPointArn	Filters access by the ARN of the access point used to mount the file system	ARN
elasticfilesystem:AccessedViaMountTarget	Filters access by whether the file system is accessed via mount targets	Bool
elasticfilesystem:CreateAction	Filters access by the name of a resource-creating API action	String
elasticfilesystem:Encrypted	Filters access by whether users can create only encrypted or unencrypted file systems	Bool

Actions, resources, and condition keys for Amazon Elastic Kubernetes Service

Amazon Elastic Kubernetes Service (service prefix: eks) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Elastic Kubernetes Service
- Resource types defined by Amazon Elastic Kubernetes Service
- Condition keys for Amazon Elastic Kubernetes Service

Actions defined by Amazon Elastic Kubernetes Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AccessKubernetesApi [permission only]	Grants permission to view Kubernetes objects via AWS EKS console	Read	cluster*		
AssociateAccessPolicy	Grants permission to associate an Amazon EKS access policy to an Amazon EKS access entry	Write	access-entry*		
				eks:policyArn eks:namespaces	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				eks:accessScope	
AssociateEncryptionConfig	Grants permission to associate encryption configuration to a cluster	Write	cluster*		
AssociateIdentityProviderConfig	Grants permission to associate an identity provider configuration to a cluster	Write	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys eks:clientId eks:issuerUrl	
CreateAccessEntry	Grants permission to create an Amazon EKS access entry	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys eks:principalArn eks:kubernetesGroups eks:username eks:accessEntryType	
CreateAddon	Grants permission to create an Amazon EKS add-on	Write	cluster*		
			podidentityassociation		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCapability	Grants permission to create a capability for an Amazon EKS cluster	Write	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCluster	Grants permission to create an Amazon EKS cluster	Write		aws:RequestTag/${TagKey} aws:TagKeys eks:bootstrapClusterCreatorAdminPermissions eks:bootstrapSelfManagedAddons eks:authenticationMode eks:supportType eks:computeConfigEnabled eks:elasticLoadBalancingEnabled	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				eks:blockStorageEnabled eks:loggingType/${type}	
CreateEksAnywhereSubscription	Grants permission to create an EKS Anywhere subscription	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFargateProfile	Grants permission to create an AWS Fargate profile	Write	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNodegroup	Grants permission to create an Amazon EKS Nodegroup	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePodIdentityAssociation	Grants permission to create an EKS Pod Identity association	Write	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessEntry	Grants permission to delete an Amazon EKS access entry	Write	access-entry*		
DeleteAddon	Grants permission to delete an Amazon EKS add-on	Write	addon*		
			podidentityassociation		
DeleteCapability	Grants permission to delete a capability from an Amazon EKS cluster	Write	capability*		
DeleteCluster	Grants permission to delete an Amazon EKS cluster	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEksAnywhereSubscription	Grants permission to describe an EKS Anywhere subscription	Write	eks-anywhere-subscription*		
DeleteFargateProfile	Grants permission to delete an AWS Fargate profile	Write	fargateprofile*		
DeleteNodegroup	Grants permission to delete an Amazon EKS Nodegroup	Write	nodegroup*		
DeletePodIdentityAssociation	Grants permission to delete an EKS Pod Identity association	Write	podidentityassociation*		
DeregisterCluster	Grants permission to deregister an External cluster	Write	cluster*		
DescribeAccessEntry	Grants permission to describe an Amazon EKS access entry	Read	access-entry*		
DescribeAddon	Grants permission to retrieve descriptive information about an Amazon EKS add-on	Read	addon*		
DescribeAddonConfiguration	Grants permission to list configuration options about an Amazon EKS add-on	Read			
DescribeAddonVersions	Grants permission to retrieve descriptive version information about the add-ons that Amazon EKS Add-ons supports	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCapability	Grants permission to describe a capability for an Amazon EKS cluster	Read	capability*		
DescribeCluster	Grants permission to retrieve descriptive information about an Amazon EKS cluster	Read	cluster*		
DescribeClusterVersions	Grants permission to retrieve descriptive information about Kubernetes versions that Amazon EKS clusters support	Read			
DescribeEksAnywhereSubscription	Grants permission to describe an EKS Anywhere subscription	Read	eks-anywhere-subscription*		
DescribeFargateProfile	Grants permission to retrieve descriptive information about an AWS Fargate profile associated with a cluster	Read	fargateprofile*		
DescribeIdentityProviderConfig	Grants permission to retrieve descriptive information about an Idp config associated with a cluster	Read	identityproviderconfig*		
DescribeInsight	Grants permission to retrieve descriptive information of a detected insight for a specified cluster	Read	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInsightsRefresh	Grants permission to retrieve the status of the latest on-demand cluster insights refresh operation	Read	cluster*		
DescribeNodegroup	Grants permission to retrieve descriptive information about an Amazon EKS nodegroup	Read	nodegroup*		
DescribePodIdentityAssociation	Grants permission to describe an EKS Pod Identity association	Read	podidentityassociation*		
DescribeUpdate	Grants permission to retrieve a given update for a given Amazon EKS cluster/nodegroup/add-on (in the specified or default region)	Read	cluster*		
			addon		
			capability		
			nodegroup		
DisassociateAccessPolicy	Grants permission to disassociate an Amazon EKS access policy from an Amazon EKS acces entry	Write	access-entry*		
				eks:policyArn eks:namespaces eks:accessScope	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateIdentityProviderConfig	Grants permission to delete an asssociated Idp config	Write	identityproviderconfig*		
ListAccessEntries	Grants permission to list all Amazon EKS access entries	List	cluster*		
ListAccessPolicies	Grants permission to list Amazon EKS access policies	List			
ListAddons	Grants permission to list the Amazon EKS add-ons in your AWS account (in the specified or default region) for a given cluster	List	cluster*		
ListAssociatedAccessPolicies	Grants permission to list associated access policy on and Amazon EKS access entry	List	access-entry*		
ListCapabilities	Grants permission to list capabilities for an Amazon EKS cluster	List	cluster*		
ListClusters	Grants permission to list the Amazon EKS clusters in your AWS account (in the specified or default region)	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDashboardData	Grants permission to list dashboard data. The Amazon EKS Dashboard aggregates information about cluster resources across multiple accounts and regions. The dashboard includes information about EC2 Instances and EKS Cluster versions	Read	dashboard*		
ListDashboardResources	Grants permission to list dashboard resources. The Amazon EKS Dashboard aggregates information about cluster resources across multiple accounts and regions. The dashboard includes information about EC2 Instances and EKS Cluster versions	Read	dashboard*		
ListEksAnywhereSubscriptions	Grants permission to list EKS Anywhere subscriptions	List			
ListFargateProfiles	Grants permission to list the AWS Fargate profiles in your AWS account (in the specified or default region) associated with a given cluster	List	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListIdentityProviderConfigs	Grants permission to list the Idp configs in your AWS account (in the specified or default region) associated with a given cluster	List	cluster*		
ListInsights	Grants permission to list all detected insights for a specified cluster	List	cluster*		
ListNodegroups	Grants permission to list the Amazon EKS nodegroups in your AWS account (in the specified or default region) attached to given cluster	List	cluster*		
ListPodIdentityAssociations	Grants permission to list EKS Pod Identity associations	List	cluster*		
ListTagsForResource	Grants permission to list tags for the specified resource	Read	addon		
			capability		
			cluster		
			dashboard		
			eks-anywhere-subscription		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			fargateprofile		
			identityproviderconfig		
			nodegroup		
ListUpdates	Grants permission to list the updates for a given Amazon EKS cluster/nodegroup/add-on (in the specified or default region)	List	cluster*		
			addon		
			capability		
			nodegroup		
MutateViaKubernetesApi [permission only]	Grants permission to modify Kubernetes objects via AWS console	Write	cluster*		eks:AccessKubernetesApi
RegisterCluster	Grants permission to register an External cluster	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartInsightsRefresh	Grants permission to initiate an on-demand refresh operation for cluster insights, getting the latest analysis outside of the standard refresh schedule	Write	cluster*		
TagResource	Grants permission to tag the specified resource	Tagging	access-entry		
			addon		
			capability		
			cluster		
			dashboard		
			eks-anywhere-subscription		
			fargateprofile		
			identityproviderconfig		
			nodegroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			podidentityassociation		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag the specified resource	Tagging	access-entry		
			addon		
			capability		
			cluster		
			dashboard		
			eks-anywhere-subscription		
			fargateprofile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			identityproviderconfig		
			nodegroup		
			podidentityassociation		
				aws:TagKeys	
UpdateAccessEntry	Grants permission to update an Amazon EKS access entry	Write	access-entry*		
UpdateAddon	Grants permission to update Amazon EKS add-on configurations, such as the VPC-CNI version	Write	addon*		
			podidentityassociation		
UpdateCapability	Grants permission to update a capability for an Amazon EKS cluster	Write	capability*		
UpdateClusterConfig	Grants permission to update Amazon EKS cluster configurations (eg: API server endpoint access)	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				eks:authenticationMode eks:supportType eks:computeConfigEnabled eks:elasticLoadBalancingEnabled eks:blockStorageEnabled eks:loggingType/${type}	
UpdateClusterVersion	Grants permission to update the Kubernetes version of an Amazon EKS cluster	Write	cluster*		
UpdateEksAnywhereSubscription	Grants permission to update an EKS Anywhere subscription	Write	eks-anywhere-subscription*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateNodegroupConfig	Grants permission to update Amazon EKS nodegroup configurations (eg: min/max/desired capacity or labels)	Write	nodegroup*		
UpdateNodegroupVersion	Grants permission to update the Kubernetes version of an Amazon EKS nodegroup	Write	nodegroup*		
UpdatePodIdentityAssociation	Grants permission to update an EKS Pod Identity association	Write	podidentityassociation*		

Resource types defined by Amazon Elastic Kubernetes Service

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
cluster	`arn:${Partition}:eks:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey}
nodegroup	`arn:${Partition}:eks:${Region}:${Account}:nodegroup/${ClusterName}/${NodegroupName}/${UUID}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
addon	arn:${Partition}:eks:${Region}:${Account}:addon/${ClusterName}/${AddonName}/${UUID}	aws:ResourceTag/${TagKey}
fargateprofile	arn:${Partition}:eks:${Region}:${Account}:fargateprofile/${ClusterName}/${FargateProfileName}/${UUID}	aws:ResourceTag/${TagKey}
identityproviderconfig	arn:${Partition}:eks:${Region}:${Account}:identityproviderconfig/${ClusterName}/${IdentityProviderType}/${IdentityProviderConfigName}/${UUID}	aws:ResourceTag/${TagKey}
eks-anywhere-subscription	arn:${Partition}:eks:${Region}:${Account}:eks-anywhere-subscription/${UUID}	aws:ResourceTag/${TagKey}
podidentityassociation	arn:${Partition}:eks:${Region}:${Account}:podidentityassociation/${ClusterName}/${UUID}	aws:ResourceTag/${TagKey}
access-entry	arn:${Partition}:eks:${Region}:${Account}:access-entry/${ClusterName}/${IamIdentityType}/${IamIdentityAccountID}/${IamIdentityName}/${UUID}	aws:ResourceTag/${TagKey} eks:accessEntryType eks:clusterName eks:kubernetesGroups eks:principalArn eks:username

Resource types	ARN	Condition keys
access-policy	arn:${Partition}:eks::aws:cluster-access-policy/${AccessPolicyName}	
dashboard	arn:${Partition}:eks:${Region}:${Account}:dashboard/${DashboardName}	aws:ResourceTag/${TagKey}
capability	arn:${Partition}:eks:${Region}:${Account}:capability/${ClusterName}/${CapabilityType}/${CapabilityName}/${UUID}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Elastic Kubernetes Service

Amazon Elastic Kubernetes Service defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a key that is present in the request the user makes to the EKS service	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair	String
aws:TagKeys	Filters access by the list of all the tag key names present in the request the user makes to the EKS service	ArrayOfString
eks:accessEntryType	Filters access by the access entry type present in the access entry requests the user makes to the EKS service	String

Condition keys	Description	Type
eks:accessScope	Filters access by the accessScope present in the associate / disassociate access policy requests the user makes to the EKS service	String
eks:authenticationMode	Filters access by the authenticationMode present in the create / update cluster request	String
eks:blockStorageEnabled	Filters access by the block storage enabled parameter in the create / update cluster request	Bool
eks:bootstrapClusterCreatorAdminPermissions	Filters access by the bootstrapClusterCreatorAdminPermissions present in the create cluster request	Bool
eks:bootstrapSelfManagedAddons	Filters access by the bootstrapSelfManagedAddons present in the create cluster request	Bool
eks:clientId	Filters access by the clientId present in the associate IdentityProviderConfig request the user makes to the EKS service	String
eks:clusterName	Filters access by the clusterName present in the access entry requests the user makes to the EKS service	String
eks:computeConfigEnabled	Filters access by the compute config enabled parameter in the create / update cluster request	Bool
eks:elasticLoadBalancingEnabled	Filters access by the elastic load balancing enabled parameter in the create / update cluster request	Bool
eks:issuerUrl	Filters access by the issuerUrl present in the associate IdentityProviderConfig request the user makes to the EKS service	String

Condition keys	Description	Type
eks:kubernetesGroups	Filters access by the kubernetesGroups present in the access entry requests the user makes to the EKS service	ArrayOfString
eks:loggingType/${type}	Filters access by the cluster logging enabled and type parameter in the create / update cluster request	Bool
eks:namespaces	Filters access by the namespaces present in the associate / disassociate access policy requests the user makes to the EKS service	ArrayOfString
eks:policyArn	Filters access by the policyArn present in the access entry requests the user makes to the EKS service	ARN
eks:principalArn	Filters access by the principalArn present in the access entry requests requests the user makes to the EKS service	ARN
eks:supportType	Filters access by the supportType present in the create / update cluster request	String
eks:username	Filters access by the Kubernetes username present in the access entry requests the user makes to the EKS service	String

Actions, resources, and condition keys for AWS Elastic Load Balancing

AWS Elastic Load Balancing (service prefix: `elasticloadbalancing`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Elastic Load Balancing

- Resource types defined by AWS Elastic Load Balancing
- Condition keys for AWS Elastic Load Balancing

Actions defined by AWS Elastic Load Balancing

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddTags	Grants permission to add the specified tags to the specified load balancer. Each load balancer can have a maximum of 10 tags	Tagging	loadbalancer*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				elasticloadbalancing:CreateAction	
ApplySecurityGroupsToLoadBalancer	Grants permission to associate one or more security groups with your load balancer in a virtual private cloud (VPC)	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup	
AttachLoadBalancerToSubnets	Grants permission to add one or more subnets to the set of configured subnets for the specified load balancer	Write	loadbalancer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:Subnet	
Configure HealthCheck	Grants permission to specify the health check settings to use when evaluating the health state of your back-end instances	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAppCookieStickinessPolicy	Grants permission to generate a stickiness policy with sticky session lifetimes that follow that of an application-generated cookie	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateLBCookieStickinessPolicy	Grants permission to generate a stickiness policy with sticky session lifetimes controlled by the lifetime of the browser (user-agent) or a specified expiration period	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLoadBalancer	Grants permission to create a load balancer	Write	loadbalancer		elasticloadbalancing:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup elasticloadbalancing:Subnet elasticloadbalancing:Scheme	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				elasticloadbalancing:ListenerProtocol	
CreateLoadBalancerListeners	Grants permission to create one or more listeners for the specified load balancer	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:ListenerProtocol	
CreateLoadBalancerPolicy	Grants permission to create a policy with the specified attributes for the specified load balancer	Write	loadbalancer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy	
DeleteLoadBalancer	Grants permission to delete the specified load balancer	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLoadBalancerListeners	Grants permission to delete the specified listeners from the specified load balancer	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteLoadBalancerPolicy	Grants permission to delete the specified policy from the specified load balancer. This policy must not be enabled for any listeners	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterInstancesFromLoadBalancer	Grants permission to deregister the specified instances from the specified load balancer	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DescribeInstanceHealth	Grants permission to describe the state of the specified instances with respect to the specified load balancer	Read			
DescribeLoadBalancerAttributes	Grants permission to describe the attributes for the specified load balancer	Read			
DescribeLoadBalancerPolicies	Grants permission to describe the specified policies	Read			
DescribeLoadBalancerPolicyTypes	Grants permission to describe the specified load balancer policy types	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLoadBalancers	Grants permission to describe the specified the load balancers. If no load balancers are specified, the call describes all of your load balancers	List			
DescribeTags	Grants permission to describe the tags associated with the specified load balancers	Read			
DetachLoadBalancerFromSubnets	Grants permission to remove the specified subnets from the set of configured subnets for the load balancer	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableAvailabilityZonesForLoadBalancer	Grants permission to remove the specified Availability Zones from the set of Availability Zones for the specified load balancer	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
EnableAvailabilityZonesForLoadBalancer	Grants permission to add the specified Availability Zones to the set of Availability Zones for the specified load balancer	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyLoadBalancerAttributes	Grants permission to modify the attributes of the specified load balancer	Write	loadbalancer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RegisterInstancesWithLoadBalancer	Grants permission to add the specified instances to the specified load balancer	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTags	Grants permission to remove one or more tags from the specified load balancer	Tagging	loadbalancer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetLoadBalancerListenerSSLCertificate	Grants permission to set the certificate that terminates the specified listener's SSL connections	Write	loadbalancer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetLoadBalancerPoliciesForBackendServer	Grants permission to replace the set of policies associated with the specified port on which the back-end server is listening with a new set of policies	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetLoadBalancerPoliciesOfListener	Grants permission to replace the current set of policies for the specified load balancer port with the specified set of policies	Write	loadbalancer*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy	

Resource types defined by AWS Elastic Load Balancing

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
loadbalancer	`arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/${LoadBalancerName}`	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Condition keys for AWS Elastic Load Balancing

AWS Elastic Load Balancing defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString
elasticloadbalancing:CreateAction	Filters access by the name of a resource-creating API action	String
elasticloadbalanci	Filters access by the listener protocols that are allowed in the request	ArrayOfString

Condition keys	Description	Type
ng:ListenerProtocol		
elasticloadbalancing:ResourceTag/	Filters access by the preface string for a tag key and value pair that are attached to a resource	String
elasticloadbalancing:ResourceTag/${TagKey}	Filters access by the preface string for a tag key and value pair that are attached to a resource	String
elasticloadbalancing:Scheme	Filters access by the load balancer scheme that are allowed in the request	String
elasticloadbalancing:SecurityGroup	Filters access by the security-group IDs that are allowed in the request	ArrayOfString
elasticloadbalancing:SecurityPolicy	Filters access by the SSL Security Policies that are allowed in the request	ArrayOfString
elasticloadbalancing:Subnet	Filters access by the subnet IDs that are allowed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Elastic Load Balancing V2

AWS Elastic Load Balancing V2 (service prefix: `elasticloadbalancing`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Elastic Load Balancing V2
- Resource types defined by AWS Elastic Load Balancing V2
- Condition keys for AWS Elastic Load Balancing V2

Actions defined by AWS Elastic Load Balancing V2

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddListenerCertificates	Grants permission to add the specified certificates to the specified secure listener	Write	listener/app*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:Resour	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ceTag/${TagKey}	
AddTags	Grants permission to add the specified tags to the specified load balancer. Each load balancer can have a maximum of 10 tags	Tagging	listener-rule/app		
			listener-rule/net		
			listener/app		
			listener/gwy		
			listener/net		
			loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
			targetgroup		
			truststore		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:CreateAction	
AddTrustStoreRevocations	Grants permission to add revocations to a trust store	Write	truststore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
AllowVendedLogDeliveryForResource [permission only]	Grants permission to configure vended log delivery for load balancers	Permissions management			
CreateListener	Grants permission to create a listener for the specified Application Load Balancer	Write	loadbalancer/app/		elasticloadbalancing:AddTags
			loadbalancer/gwy/		
			loadbalancer/net/		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy elasticloadbalancing:ListenerProtocol	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLoadBalancer	Grants permission to create a load balancer	Write	loadbalancer/app/		elasticloadbalancing:AddTags
			loadbalancer/gwy/		
			loadbalancer/net/		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup elasticloadbalancing:Subnet elasticloadbalancing:Scheme	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRule	Grants permission to create a rule for the specified listener	Write	listener/app*		elasticloadbalancing:AddTags
			listener/net*		
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateTargetGroup	Grants permission to create a target group	Write	targetgroup*		elasticloadbalancing:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
CreateTrustStore	Grants permission to create a trust store	Write	truststore		elasticloadbalancing:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteListener	Grants permission to delete the specified listener	Write	listener/app*		
			listener/gwy*		
			listener/net*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteLoadBalancer	Grants permission to delete the specified load balancer	Write	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRule	Grants permission to delete the specified rule	Write	listener-rule/app*		
			listener-rule/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteSharedTrustStoreAssociation	Grants permission to delete the specified shared trust store association	Write	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTargetGroup	Grants permission to delete the specified target group	Write	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DeleteTrustStore	Grants permission to delete the specified trust store	Write	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterTargets	Grants permission to deregister the specified targets from the specified target group	Write	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
DescribeAccountLimits	Grants permission to describe the Elastic Load Balancing resource limits for the AWS account	Read			
DescribeCapacityReservation	Grants permission to describe the capacity reservation for a load balancer	Read			
DescribeListenerAttributes	Grants permission to describe the attributes for the specified listener	Read			
DescribeListenerCertificates	Grants permission to describe the certificates for the specified secure listener	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeListeners	Grants permission to describe the specified listeners or the listeners for the specified Application Load Balancer	Read			
DescribeLoadBalancerAttributes	Grants permission to describe the attributes for the specified load balancer	Read			
DescribeLoadBalancers	Grants permission to describe the specified the load balancers. If no load balancers are specified, the call describes all of your load balancers	List			
DescribeRules	Grants permission to describe the specified rules or the rules for the specified listener	Read			
DescribeSSLPolicies	Grants permission to describe the specified policies or all policies used for SSL negotiation	Read			
DescribeTags	Grants permission to describe the tags associated with the specified resource	Read			
DescribeTargetGroupAttributes	Grants permission to describe the attributes for the specified target group	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTargetGroups	Grants permission to describe the specified target groups or all of your target groups	Read			
DescribeTargetHealth	Grants permission to describe the health of the specified targets or all of your targets	Read			
DescribeTrustStoreAssociations	Grants permission to describe the associations with a trust store	Read			
DescribeTrustStoreRevocations	Grants permission to describe the specified trust stores revocations or all of your revocations related to a trust store	Read			
DescribeTrustStores	Grants permission to describe the specified trust stores or all of your trust stores	Read			
GetResourcePolicy	Grants permission to retrieve the resource policy associated with the resource	Read	truststore		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetTrustStoreCaCertificatesBundle	Grants permission to retrieve a trust store CA certificates bundle	Read	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
GetTrustStoreRevocationContent	Grants permission to retrieve a trust store revocation content	Read	truststore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyCapacityReservation	Grants permission to modify the capacity reservation for a load balancer	Write	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyIpPools	Grants permission to modify the ip pools for a load balancer	Write	loadbalancer/app/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyListener	Grants permission to modify the specified properties of the specified listener	Write	listener/app*		
			listener/gwy*		
			listener/net*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityPolicy elasticloadbalancing:ListenerProtocol	
ModifyListenerAttributes	Grants permission to modify the attributes of the specified listener	Write	listener/app*		
			listener/gwy*		
			listener/net*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyLoadBalancerAttributes	Grants permission to modify the attributes of the specified load balancer	Write	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyRule	Grants permission to modify the specified rule	Write	listener-rule/app*		
			listener-rule/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTargetGroup	Grants permission to modify the health checks used when evaluating the health state of the targets in the specified target group	Write	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyTargetGroupAttributes	Grants permission to modify the specified attributes of the specified target group	Write	targetgroup*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
ModifyTrustStore	Grants permission to modify the specified trust store	Write	truststore*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RegisterTargets	Grants permission to register the specified targets with the specified target group	Write	targetgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveListenerCertificates	Grants permission to remove the specified certificates of the specified secure listener	Write	listener/app*		
			listener/net*		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTags	Grants permission to remove one or more tags from the specified load balancer	Tagging	listener-rule/app		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			listener-rule/net		
			listener/app		
			listener/gwy		
			listener/net		
			loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
			targetgroup		
			truststore		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
RemoveTrustStoreRevocations	Grants permission to remove revocations from a trust store	Write	truststore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	
SetIpAddressType	Grants permission to set the type of IP addresses used by the subnets of the specified load balancer	Write	loadbalancer/app/		
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetRulePriorities	Grants permission to set the priorities of the specified rules	Write	listener-rule/app*		
			listener-rule/net*		
SetSecurityGroups	Grants permission to associate the specified security groups with the specified load balancer	Write	loadbalancer/app/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:SecurityGroup	
SetSubnets	Grants permission to enable the Availability Zone for the specified subnets for the specified load balancer	Write	loadbalancer/app/		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			loadbalancer/gwy/		
			loadbalancer/net/		
				aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey} elasticloadbalancing:Subnet	
SetWebAcl [permission only]	Grants permission to give WebAcl permission to WAF	Write			

Resource types defined by AWS Elastic Load Balancing V2

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
listener/gwy	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/gwy/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener/app	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/app/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener-rule/app	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener-rule/app/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}/${ListenerRuleId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener/net	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener/net/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
listener-rule/net	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:listener-rule/net/${LoadBalancerName}/${LoadBalancerId}/${ListenerId}/${ListenerRuleId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
loadbalancer/gwy/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/gwy/${LoadBalancerName}/${LoadBalancerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
loadbalancer/app/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
loadbalancer/net/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/net/${LoadBalancerName}/${LoadBalancerId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
targetgroup	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:targetgroup/${TargetGroupName}/${TargetGroupId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}
truststore	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:truststore/${TrustStoreName}/${TrustStoreId}	aws:ResourceTag/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}

Condition keys for AWS Elastic Load Balancing V2

AWS Elastic Load Balancing V2 defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString
elasticloadbalancing:CreateAction	Filters access by the name of a resource-creating API action	String
elasticloadbalancing:ListenerProtocol	Filters access by the listener protocol that is allowed in the request	String
elasticloadbalancing:ResourceTag/${TagKey}	Filters access by the preface string for a tag key and value pair that are attached to a resource	String
elasticloadbalancing:Scheme	Filters access by the load balancer scheme that is allowed in the request	String

Condition keys	Description	Type
elasticloadbalancing:SecurityGroup	Filters access by the security-group IDs that are allowed in the request	ArrayOfString
elasticloadbalancing:SecurityPolicy	Filters access by the SSL Security Policies that are allowed in the request	ArrayOfString
elasticloadbalancing:Subnet	Filters access by the subnet IDs that are allowed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Elastic MapReduce

Amazon Elastic MapReduce (service prefix: `elasticmapreduce`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Elastic MapReduce
- Resource types defined by Amazon Elastic MapReduce
- Condition keys for Amazon Elastic MapReduce

Actions defined by Amazon Elastic MapReduce

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy,

you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Note

The DescribeJobFlows API is deprecated and will eventually be removed. We recommend you use ListClusters, DescribeCluster, ListSteps, ListInstanceGroups and ListBootstrapActions instead

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AccessAllEventLogs	Grants permission to view all event logs in a persistent application history server	Write	cluster*		
AddInstanceFleet	Grants permission to add an instance fleet to a running cluster	Write	cluster*		
AddInstanceGroups	Grants permission to add instance groups to a running cluster	Write	cluster*		
AddJobFlowSteps	Grants permission to add new steps to a running cluster	Write	cluster*		
				elasticmapreduce:ExecutionRoleArn	
AddTags	Grants permission to add tags to an Amazon EMR resource	Tagging	cluster		
			editor		
			notebook-execution		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			studio		
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
AttachEditor [permission only]	Grants permission to attach an EMR notebook to a compute engine	Write	editor*		
CancelSteps	Grants permission to cancel a pending step or steps in a running cluster	Write	cluster*		
CreateEditor [permission only]	Grants permission to create an EMR notebook	Write	cluster		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
CreatePersistentAppUI	Grants permission to create a persistent application history server	Write	cluster*		
CreateRepository [permission only]	Grants permission to create an EMR notebook repository	Write			
CreateSecurityConfiguration	Grants permission to create a security configuration	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateStudio	Grants permission to create an EMR Studio	Write		aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
CreateStudioPresignedUrl	Grants permission to launch an EMR Studio using IAM authentication mode	Write	studio*		
CreateStudioSessionMapping	Grants permission to create an EMR Studio session mapping	Write	studio*		
DeleteEditor [permission only]	Grants permission to delete an EMR notebook	Write	editor*		
DeleteRepository [permission only]	Grants permission to delete an EMR notebook repository	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSecurityConfiguration	Grants permission to delete a security configuration	Write			
DeleteStudio	Grants permission to delete an EMR Studio	Write	studio*		
DeleteStudioSessionMapping	Grants permission to delete an EMR Studio session mapping	Write	studio*		
DeleteWorkspaceAccess [permission only]	Grants permission to block an identity from opening a collaborative workspace	Permissions management	editor*		
DescribeCluster	Grants permission to get details about a cluster, including status, hardware and software configuration, VPC settings, and so on	Read	cluster*		
DescribeEditor [permission only]	Grants permission to view information about a notebook, including status, user, role, tags, location, and more	Read	editor*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeJobFlows	Grants permission to describe details of clusters (job flows). This API is deprecated and will eventually be removed. We recommend you use ListClusters, DescribeCluster, ListSteps, ListInstanceGroups and ListBootstrapActions instead	Read	cluster*		
DescribeNotebookExecution	Grants permission to view information about a notebook execution	Read	notebook-execution*		
DescribePersistentAppUI	Grants permission to describe a persistent application history server	Read	cluster*		
DescribeReleaseLabel	Grants permission to view information about an EMR release, such as which applications are supported	Read			
DescribeRepository [permission only]	Grants permission to describe an EMR notebook repository	Read			
DescribeSecurityConfiguration	Grants permission to get details of a security configuration	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStep	Grants permission to get details about a cluster step	Read	cluster*		
DescribeStudio	Grants permission to view information about an EMR Studio	Read	studio*		
DetachEditor [permission only]	Grants permission to detach an EMR notebook from a compute engine	Write	editor*		
GetAutoTerminationPolicy	Grants permission to retrieve the auto-termination policy associated with a cluster	Read	cluster*		
GetBlockPublicAccessConfiguration	Grants permission to retrieve the EMR block public access configuration for the AWS account in the Region	Read			
GetClusterSessionCredentials	Grants permission to retrieve HTTP basic credentials associated with a given execution IAM Role for a fine-grained access control enabled EMR Cluster	Write	cluster*		
				elasticmapreduce:ExecutionRoleArn	
GetManagedScalingPolicy	Grants permission to retrieve the managed scaling policy associated with a cluster	Read	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetOnClusterAppUIPresignedURL	Grants permission to get a presigned URL for an application history server running on the cluster	Write	cluster*		
GetPersistentAppUIPresignedURL	Grants permission to get a presigned URL for a persistent application history server	Write	cluster*		
				elasticmapreduce:ExecutionRoleArn	
GetStudioSessionMapping	Grants permission to view information about an EMR Studio session mapping	Read	studio*		
LinkRepository [permission only]	Grants permission to link an EMR notebook repository to EMR notebooks	Write			
ListBootstrapActions	Grants permission to get details about the bootstrap actions associated with a cluster	Read	cluster*		
ListClusters	Grants permission to get the status of accessible clusters	List			
ListEditors [permission only]	Grants permission to list summary information for accessible EMR notebooks	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListInstanceFleets	Grants permission to get details of instance fleets in a cluster	Read	cluster*		
ListInstanceGroups	Grants permission to get details of instance groups in a cluster	Read	cluster*		
ListInstances	Grants permission to get details about the Amazon EC2 instances in a cluster	Read	cluster*		
ListNotebookExecutions	Grants permission to list summary information for notebook executions	List			
ListReleaseLabels	Grants permission to list and filter the available EMR releases in the current region	List			
ListRepositories [permission only]	Grants permission to list existing EMR notebook repositories	List			
ListSecurityConfigurations	Grants permission to list available security configurations in this account by name, along with creation dates and times	List			
ListSteps	Grants permission to list steps associated with a cluster	Read	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListStudioSessionMappings	Grants permission to list summary information about EMR Studio session mappings	List			
ListStudios	Grants permission to list summary information about EMR Studios	List			
ListSupportedInstanceTypes	Grants permission to list the Amazon EC2 instance types that an Amazon EMR release supports	List			
ListWorkspaceAccessIdentities [permission only]	Grants permission to list identities that are granted access to a workspace	List	editor*		
ModifyCluster	Grants permission to change cluster settings such as number of steps that can be executed concurrently for a cluster	Write	cluster*		
ModifyInstanceFleet	Grants permission to change the target On-Demand and target Spot capacities for a instance fleet	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceGroups	Grants permission to change the number and configuration of EC2 instances for an instance group	Write	cluster		
OpenEditorInConsole [permission only]	Grants permission to launch the Jupyter notebook editor for an EMR notebook from within the console	Write	editor*		
			cluster		
PutAutoScalingPolicy	Grants permission to create or update an automatic scaling policy for a core instance group or task instance group	Write	cluster*		
PutAutoTerminationPolicy	Grants permission to create or update the auto-termination policy associated with a cluster	Write	cluster*		
PutBlockPublicAccessConfiguration	Grants permission to create or update the EMR block public access configuration for the AWS account in the Region	Permissions management			
PutManagedScalingPolicy	Grants permission to create or update the managed scaling policy associated with a cluster	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutWorkspaceAccess [permission only]	Grants permission to allow an identity to open a collaborative workspace	Permissions management	editor*		
RemoveAutoScalingPolicy	Grants permission to remove an automatic scaling policy from an instance group	Write	cluster*		
RemoveAutoTerminationPolicy	Grants permission to remove the auto-termination policy associated with a cluster	Write	cluster*		
RemoveManagedScalingPolicy	Grants permission to remove the managed scaling policy associated with a cluster	Write	cluster*		
RemoveTags	Grants permission to remove tags from an Amazon EMR resource	Tagging	cluster		
			editor		
			notebook-execution		
			studio		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RunJobFlow	Grants permission to create and launch a cluster (job flow)	Write		aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	iam:PassRole
SetKeepJobFlowAliveWhenNoSteps	Grants permission to add and remove auto terminate after step execution for a cluster	Write	cluster*		
SetTerminationProtection	Grants permission to add and remove termination protection for a cluster	Write	cluster*		
SetUnhealthyNodeReplacement	Grants permission to enable or disable unhealthy node replacement for a cluster	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetVisibleToAllUsers	Grants permission to set whether all AWS Identity and Access Management (IAM) users in the AWS account can view a cluster. This API is deprecated and your cluster may be visible to all users in your account. To restrict cluster access using an IAM policy, see AWS Identity and Access Management for Amazon EMR (https://docs.aws.amazon.com/emr/latest/ManagementGuide/emr-plan-access-iam.html)	Write	cluster*		
StartEditor [permission only]	Grants permission to start an EMR notebook	Write	editor* cluster		
StartNotebookExecution	Grants permission to start an EMR notebook execution	Write	cluster* editor*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${TagKey}	
StopEditor [permission only]	Grants permission to shut down an EMR notebook	Write	editor*		
StopNotebookExecution	Grants permission to stop notebook execution	Write	notebook-execution*		
TerminateJobFlows	Grants permission to terminate a cluster (job flow)	Write	cluster*		
UnlinkRepository [permission only]	Grants permission to unlink an EMR notebook repository from EMR notebooks	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEditor [permission only]	Grants permission to update an EMR notebook	Write	editor*		
UpdateRepository [permission only]	Grants permission to update an EMR notebook repository	Write			
UpdateStudio	Grants permission to update information about an EMR Studio	Write	studio*		
UpdateStudioSessionMapping	Grants permission to update an EMR Studio session mapping	Write	studio*		
ViewEventsFromAllClustersInConsole [permission only]	Grants permission to use the EMR console to view events from all clusters	List			

Resource types defined by Amazon Elastic MapReduce

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
cluster	arn:${Partition}:elasticmapreduce:${Region}:${Account}:cluster/${ClusterId}	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
editor	arn:${Partition}:elasticmapreduce:${Region}:${Account}:editor/${EditorId}	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
notebook-execution	arn:${Partition}:elasticmapreduce:${Region}:${Account}:notebook-execution/${NotebookExecutionId}	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}
studio	arn:${Partition}:elasticmapreduce:${Region}:${Account}:studio/${StudioId}	aws:ResourceTag/${TagKey} elasticmapreduce:ResourceTag/${TagKey}

Condition keys for Amazon Elastic MapReduce

Amazon Elastic MapReduce defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by whether the tag and value pair is provided with the action	String
aws:ResourceTag/${TagKey}	Filters access by the tag and value pair associated with an Amazon EMR resource	String
aws:TagKeys	Filters access by whether the tag keys are provided with the action regardless of tag value	ArrayOfString
elasticmapreduce:ExecutionRoleArn	Filters access by whether the execution role ARN is provided with the action	ARN
elasticmapreduce:RequestTag/${TagKey}	Filters access by whether the tag and value pair is provided with the action	String
elasticmapreduce:ResourceTag/${TagKey}	Filters access by the tag and value pair associated with an Amazon EMR resource	String

Actions, resources, and condition keys for Amazon EventBridge

Amazon EventBridge (service prefix: `events`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.

- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon EventBridge
- Resource types defined by Amazon EventBridge
- Condition keys for Amazon EventBridge

Actions defined by Amazon EventBridge

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ActivateEventSource	Grants permission to activate partner event sources	Write	event-source*		
AllowVendedLogDeliveryForResource [permission only]	Grants permission to configure vended log delivery for EventBridge	Write	event-bus*		
CancelReplay	Grants permission to cancel a replay	Write	replay*		
CreateApiDestination	Grants permission to create a new api destination	Write	api-destination*		
			connection*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateArchive	Grants permission to create a new archive	Write	archive*		
			event-bus*		
			alias		
			key		
CreateConnection	Grants permission to create a new connection	Write	connection*		
CreateEndpoint	Grants permission to create an endpoint	Write	endpoint*		
				events:EventBusArn	
CreateEventBus	Grants permission to create event buses	Write	event-bus*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePartnerEventSource	Grants permission to create partner event sources	Write	event-source*		
DeactivateEventSource	Grants permission to deactivate event sources	Write	event-source*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeauthorizeConnection	Grants permission to deauthorize a connection, deleting its stored authorization secrets	Write	connection*		
DeleteApiDestination	Grants permission to delete an api destination	Write	api-destination*		
DeleteArchive	Grants permission to delete an archive	Write	archive*		
DeleteConnection	Grants permission to delete a connection	Write	connection*		
DeleteEndpoint	Grants permission to delete an endpoint	Write	endpoint*		
DeleteEventBus	Grants permission to delete event buses	Write	event-bus*		
DeletePartnerEventSource	Grants permission to delete partner event sources	Write	event-source*		
DeleteRule	Grants permission to delete rules	Write	rule-on-custom-event-bus		
			rule-on-default-event-bus		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				events:creatorAccount events:ManagedBy	
DescribeApiDestination	Grants permission to retrieve details about an api destination	Read	api-destination*		
			connection*		
DescribeArchive	Grants permission to retrieve details about an archive	Read	archive*		
DescribeConnection	Grants permission to retrieve details about a conection	Read	connection*		
DescribeEndpoint	Grants permission to retrieve details about an endpoint	Read	endpoint*		
DescribeEventBus	Grants permission to retrieve details about event buses	Read	event-bus		
DescribeEventSource	Grants permission to retrieve details about event sources	Read	event-source*		
DescribePartnerEventSource	Grants permission to retrieve details about partner event sources	Read	event-source*		
DescribeReplay	Grants permission to retrieve the details of a replay	Read	replay*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeRule	Grants permission to retrieve details about rules	Read	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount	
DisableRule	Grants permission to disable rules	Write	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	
EnableRule	Grants permission to enable rules	Write	rule-on-custom-event-bus		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			rule-on-default-event-bus		
				events:creatorAccount events:ManagedBy	
InvokeApiDestination [permission only]	Grants permission to invoke an api destination	Write	api-destination*		
ListApiDestinations	Grants permission to retrieve a list of api destinations	List			
ListArchives	Grants permission to retrieve a list of archives	List			
ListConnections	Grants permission to retrieve a list of connections	List			
ListEndpoints	Grants permission to retrieve a list of endpoints	List			
ListEventBuses	Grants permission to retrieve a list of the event buses in your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEventSources	Grants permission to to retrieve a list of event sources shared with this account	List			
ListPartnerEventSourceAccounts	Grants permission to retrieve a list of AWS account IDs associated with an event source	List	event-source*		
ListPartnerEventSources	Grants permission to retrieve a list partner event sources	List			
ListReplays	Grants permission to retrieve a list of replays	List			
ListRuleNamesByTarget	Grants permission to retrieve a list of the names of the rules associated with a target	List			
ListRules	Grants permission to retrieve a list of the Amazon EventBridge rules in the account	List			
ListTagsForResource	Grants permission to retrieve a list of tags associated with an Amazon EventBridge resource	List	event-bus		
			rule-on-custom-event-bus		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			rule-on-default-event-bus		
				events:creatorAccount	
ListTargetsByRule	Grants permission to retrieve a list of targets defined for a rule	List	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:creatorAccount	
PutEvents	Grants permission to send custom events to Amazon EventBridge	Write	event-bus*		
				events:detail-type events:source events:eventBusInvocation	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutPartnerEvents	Grants permission to sends custom events to Amazon EventBridge	Write			
PutPermission	Grants permission to use the PutPermission action to grants permission to another AWS account to put events to your default event bus	Permissions management			
PutRule	Grants permission to create or updates rules	Write	rule-on-custom-event-bus		
			rule-on-default-event-bus		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				events:detail.userIdentity.principalId events:detail-type events:source events:detail.service events:detail.eventTypeCode aws:RequestTag/${TagKey} aws:TagKeys events:creatorAccount events:ManagedBy	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutTargets	Grants permission to add targets to a rule	Write	rule-on-custom-event-bus		
			rule-on-default-event-bus		
				events:TargetArn events:creatorAccount events:ManagedBy	
RemovePermission	Grants permission to revoke the permission of another AWS account to put events to your default event bus	Permissions management			
RemoveTargets	Grants permission to removes targets from a rule	Write	rule-on-custom-event-bus		
			rule-on-default-event-bus		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				events:creatorAccount events:ManagedBy	
RetrieveConnectionCredentials [permission only]	Grants permission to retrieve credentials from a connection	Write	connection*		
StartReplay	Grants permission to start a replay of an archive	Write	archive*		
			event-bus*		
			replay*		
TagResource	Grants permission to add a tag to an Amazon EventBridge resource	Tagging	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} events:creatorAccount	
TestEventPattern	Grants permission to test whether an event pattern matches the provided event	Read			
UntagResource	Grants permission to remove a tag from an Amazon EventBridge resource	Tagging	event-bus		
			rule-on-custom-event-bus		
			rule-on-default-event-bus		
				aws:TagKeys events:creatorAccount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateApiDestination	Grants permission to update an api destination	Write	api-destination*		
UpdateArchive	Grants permission to update an archive	Write	archive*		
			alias		
			key		
UpdateConnection	Grants permission to update a connection	Write	connection*		
UpdateEndpoint	Grants permission to update an endpoint	Write	endpoint*		
				events:EventBusArn	
UpdateEventBus	Grants permission to update event buses	Write	event-bus*		

Resource types defined by Amazon EventBridge

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
event-source	`arn:${Partition}:events:${Region}::event-source/${EventSourceName}`	

Resource types	ARN	Condition keys
event-bus	arn:${Partition}:events:${Region}:${Account}:event-bus/${EventBusName}	aws:ResourceTag/${TagKey}
rule-on-default-event-bus	arn:${Partition}:events:${Region}:${Account}:rule/${RuleName}	aws:ResourceTag/${TagKey}
rule-on-custom-event-bus	arn:${Partition}:events:${Region}:${Account}:rule/${EventBusName}/${RuleName}	aws:ResourceTag/${TagKey}
archive	arn:${Partition}:events:${Region}:${Account}:archive/${ArchiveName}	
replay	arn:${Partition}:events:${Region}:${Account}:replay/${ReplayName}	
connection	arn:${Partition}:events:${Region}:${Account}:connection/${ConnectionName}	
api-destination	arn:${Partition}:events:${Region}:${Account}:api-destination/${ApiDestinationName}	
endpoint	arn:${Partition}:events:${Region}:${Account}:endpoint/${EndpointName}	
create-snapshot	arn:${Partition}:events:${Region}:${Account}:target/create-snapshot	
reboot-instance	arn:${Partition}:events:${Region}:${Account}:target/reboot-instance	
stop-instance	arn:${Partition}:events:${Region}:${Account}:target/stop-instance	

Resource types	ARN	Condition keys
terminate-instance	arn:${Partition}:events:${Region}:${Account}:target/terminate-instance	
alias	arn:${Partition}:kms:${Region}:${Account}:alias/${Alias}	
key	arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}	

Condition keys for Amazon EventBridge

Amazon EventBridge defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for each of the tags to event bus and rule actions	String
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource to event bus and rule actions	String
aws:TagKeys	Filters access by the tags in the request to event bus and rule actions	ArrayOfString
events:EventBusArn	Filters access by the ARN of the event buses that can be associated with an endpoint to CreateEndpoint and UpdateEndpoint actions	ArrayOfARN

Condition keys	Description	Type
events:ManagedBy	Filters access by AWS services. If a rule is created by an AWS service on your behalf, the value is the principal name of the service that created the rule	String
events:TargetArn	Filters access by the ARN of a target that can be put to a rule to PutTargets actions. TargetARN doesn't include DeadLetterConfigArn	ArrayOfARN
events:creatorAccount	Filters access by the account the rule was created in to rule actions	String
events:detail-type	Filters access by the literal string of the detail-type of the event to PutEvents and PutRule actions	ArrayOfString
events:detail.eventTypeCode	Filters access by the literal string for the detail.eventTypeCode field of the event to PutRule actions	String
events:detail.service	Filters access by the literal string for the detail.service field of the event to PutRule actions	String
events:detail.userIdentity.principalId	Filters access by the literal string for the detail.useridentity.principalid field of the event to PutRule actions	String
events:eventBusInvocation	Filters access by whether the event was generated via API or cross-account bus invocation to PutEvents actions	String
events:source	Filters access by the AWS service or AWS partner event source that generated the event to PutEvents and PutRule actions. Matches the literal string of the source field of the event	ArrayOfString

Actions, resources, and condition keys for Amazon EventBridge Scheduler

Amazon EventBridge Scheduler (service prefix: `scheduler`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon EventBridge Scheduler
- Resource types defined by Amazon EventBridge Scheduler
- Condition keys for Amazon EventBridge Scheduler

Actions defined by Amazon EventBridge Scheduler

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit

resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSchedule	Grants permission to create an Amazon EventBridge Scheduler schedule	Write	schedule*		iam:PassRole
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateScheduleGroup	Grants permission to create an Amazon EventBridge Scheduler schedule group	Write	schedule-group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSchedule	Grants permission to delete an Amazon EventBridge Scheduler schedule	Write	schedule*		
				aws:ResourceTag/${TagKey}	
DeleteScheduleGroup	Grants permission to delete an Amazon EventBridge Scheduler schedule group	Write	schedule-group*		scheduler:DeleteSchedule
				aws:ResourceTag/${TagKey}	
GetSchedule	Grants permission to view details about an Amazon EventBridge Scheduler schedule	Read	schedule*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetScheduleGroup	Grants permission to view details about an Amazon EventBridge Scheduler schedule group	Read	schedule-group*		
				aws:ResourceTag/${TagKey}	
ListScheduleGroups	Grants permission to list the Amazon EventBridge Scheduler schedule groups in your account	List			
ListSchedules	Grants permission to list the Amazon EventBridge Scheduler schedules in your account	List			
ListTagsForResource	Grants permission to lists tag for an Amazon EventBridge Scheduler resource	Read	schedule-group		
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to tag an Amazon EventBridge Scheduler resource	Tagging	schedule-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag an Amazon EventBridge Scheduler resource	Tagging	schedule-group*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateSchedule	Grants permission to modify an Amazon EventBridge Scheduler schedule	Write	schedule*		iam:PassRole
				aws:ResourceTag/${TagKey}	

Resource types defined by Amazon EventBridge Scheduler

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
schedule-group	`arn:${Partition}:scheduler:${Region}:${Account}:schedule-group/${GroupName}`	aws:ResourceTag/${TagKey}
schedule	`arn:${Partition}:scheduler:${Region}:${Account}:schedule/${GroupName}/${ScheduleName}`	

Condition keys for Amazon EventBridge Scheduler

Amazon EventBridge Scheduler defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon FSx

Amazon FSx (service prefix: `fsx`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon FSx
- Resource types defined by Amazon FSx
- Condition keys for Amazon FSx

Actions defined by Amazon FSx

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a

resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate FileGateway [permission only]	Grants permission to associate a File Gateway instance with an Amazon FSx for Windows File Server file system	Write	file-system*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateFileSystemAliases	Grants permission to associate DNS aliases with an Amazon FSx for Windows File Server file system	Write	file-system*		
BypassSnaplockEnterpriseRetention [permission only]	Grants permission to allow deletion of an FSx for ONTAP SnapLock Enterprise volume that contains WORM (write once, read many) files with active retention periods	Permissions management	volume*		
CancelDataRepositoryTask	Grants permission to cancel a data repository task	Write	task*		
CopyBackup	Grants permission to copy a backup	Write	backup*		fsx:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CopySnapshotAndUpdateVolume	Grants permission to update an existing volume by using a snapshot from another Amazon FSx for OpenZFS file system	Write	snapshot*		
			volume*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAndAttachS3AccessPoint	Grants permission to create and attach a S3 Access Point to a FSx File System	Write	volume		s3:CreateAccessPoint s3:GetAccessPoint s3:PutAccessPointPolicy
CreateBackup	Grants permission to create a new backup of an Amazon FSx file system or an Amazon FSx volume	Write	backup*		fsx:TagResource
			file-system		
			volume		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDataRepositoryAssociation	Grants permission to create a new data respository association for an Amazon FSx for Lustre file system	Write	association*	fsx:NfsDataRepositoryAuthenticationEnabled fsx:NfsDataRepositoryEncryptionInTransitEnabled	fsx:TagResource
			file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataRepositoryTask	Grants permission to create a new data respository task for an Amazon FSx for Lustre file system	Write	file-system*		fsx:TagResource
			task*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFileCache	Grants permission to create a new, empty, Amazon file cache	Write	file-cache*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs ec2:GetSecurityGroupsForVpc fsx:CreateDataRepositoryAssociation fsx:TagResource logs:CreateLogGroup logs:CreateLogStream logs:PutLogEvents

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:ListBucket
			association	fsx:NfsDataRepositoryEncryptionInTransitEnabled fsx:NfsDataRepositoryAuthenticationEnabled	
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFileSystem	Grants permission to create a new, empty, Amazon FSx file system	Write	file-system*		ec2:GetSecurityGroupsForVpc fsx:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFileSystemFromBackup	Grants permission to create a new Amazon FSx file system from an existing backup	Write	backup*		ec2:GetSecurityGroupsForVpc fsx:TagResource
			file-system*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	Grants permission to create a new snapshot on a volume	Write	snapshot*		fsx:TagResource
			volume*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorageVirtualMachine	Grants permission to create a new storage virtual machine in an Amazon FSx for Ontap file system	Write	file-system*		fsx:TagResource
			storage-virtual-machine*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVolume	Grants permission to create a new volume	Write	volume*		fsx:TagResource
			snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId fsx:ParentVolumeId	
CreateVolumeFromBackup	Grants permission to create a new volume from backup	Write	backup*		fsx:TagResource
			storage-virtual-machine*		
			volume*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId	
DeleteBackup	Grants permission to delete a backup, deleting its contents. After deletion, the backup no longer exists, and its data is no longer available	Write	backup*		
DeleteDataRepositoryAssociation	Grants permission to delete a data repository association	Write	association*		
DeleteFileCache	Grants permission to delete a file cache, deleting its contents	Write	file-cache*		fsx:DeleteDataRepositoryAssociation
			association		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFileSystem	Grants permission to delete a file system, deleting its contents and any existing automatic backups of the file system	Write	file-system*		fsx:CreateBackup fsx:TagResource
			backup		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteResourcePolicy [permission only]	Grants permission to manage cross-account sharing of FSx volumes through AWS Resource Access Manager (RAM). PutResourcePolicy and GetResourcePolicy are also required	Permissions management	volume*		
DeleteSnapshot	Grants permission to delete a snapshot on a volume	Write	snapshot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteStorageVirtualMachine	Grants permission to delete a storage virtual machine, deleting its contents	Write	storage-virtual-machine*		
DeleteVolume	Grants permission to delete a volume, deleting its contents and any existing automatic backups of the volume	Write	volume*		fsx:TagResource
			backup		
				aws:RequestTag/${TagKey} aws:TagKeys fsx:StorageVirtualMachineId fsx:ParentVolumeId	
DescribeAssociatedFileGateways [permission only]	Grants permission to describe the File Gateway instances associated with an Amazon FSx for Windows File Server file system	Read	file-system*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeBackups	Grants permission to return the descriptions of all backups owned by your AWS account in the AWS Region of the endpoint that you're calling	Read			
DescribeDataRepositoryAssociations	Grants permission to return the descriptions of all data repository associations owned by your AWS account in the AWS Region of the endpoint that you're calling	Read			
DescribeDataRepositoryTasks	Grants permission to return the descriptions of all data repository tasks owned by your AWS account in the AWS Region of the endpoint that you're calling	Read			
DescribeFileCaches	Grants permission to return the descriptions of all file caches owned by your AWS account in the AWS Region of the endpoint that you're calling	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFileSystemAliases	Grants permission to return the description of all DNS aliases owned by your Amazon FSx for Windows File Server file system	Read	file-system*		
DescribeFileSystems	Grants permission to return the descriptions of all file systems owned by your AWS account in the AWS Region of the endpoint that you're calling	Read			
DescribeS3AccessPointAttachments	Grants permission to return the descriptions of S3 Access Point Attachments	Read			
DescribeSharedVpcConfiguration	Grants permission to return the descriptions of whether FSx route table updates from participant accounts are allowed in your account	Read			
DescribeSnapshots	Grants permission to return the descriptions of all snapshots owned by your AWS account in the AWS Region of the endpoint you're calling	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStorageVirtualMachines	Grants permission to return the descriptions of all storage virtual machines owned by your AWS account in the AWS Region of the endpoint that you're calling	Read			
DescribeVolumes	Grants permission to return the descriptions of all volumes owned by your AWS account in the AWS Region of the endpoint that you're calling	Read			
DetachAndDeleteS3AccessPoint	Grants permission to detach an S3 Access Point from an Amazon FSx File System and delete the S3 Access Point	Write	volume		s3:DeleteAccessPoint
DisassociateFileGateway [permission only]	Grants permission to disassociate a File Gateway instance from an Amazon FSx for Windows File Server file system	Write	file-system*		
DisassociateFileSystemAliases	Grants permission to disassociate file system aliases with an Amazon FSx for Windows File Server file system	Write	file-system*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResourcePolicy [permission only]	Grants permission to manage cross-account sharing of FSx volumes through AWS Resource Access Manager (RAM). PutResourcePolicy and DeleteResourcePolicy are also required	Permissions management	volume*		
ListTagsForResource	Grants permission to list tags for an Amazon FSx resource	Read	association		
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ManageBackupPrincipalAssociations [permission only]	Grants permission to manage backup principal associations through AWS Backup	Permissions management	backup*		
PutResourcePolicy [permission only]	Grants permission to manage cross-account sharing of FSx volumes through AWS Resource Access Manager (RAM). DeleteResourcePolicy and GetResourcePolicy are also required	Permissions management	volume*		
ReleaseFileSystemNfsV3Locks	Grants permission to release file system NFS V3 locks	Write	file-system*		
RestoreVolumeFromSnapshot	Grants permission to restore volume state from a snapshot	Write	snapshot* volume*		
StartMisconfiguredStateRecovery	Grants permission to start misconfigured state recovery	Write	file-system*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag an Amazon FSx resource	Tagging	association	fsx:NfsDataRepositoryAuthenticationEnabled fsx:NfsDataRepositoryEncryptionInTransitEnabled	
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume	fsx:ParentVolumeId fsx:StorageVirtualMachineId	
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove a tag from an Amazon FSx resource	Tagging	association		
			backup		
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume		
				aws:TagKeys	
UpdateDataRepositoryAssociation	Grants permission to update data repository association configuration	Write	association*		
UpdateFileCache	Grants permission to update file cache configuration	Write	file-cache*		
UpdateFileSystem	Grants permission to update file system configuration	Write	file-system*		
UpdateSharedVpcConfiguration	Grants permission to enable or disable FSx route table updates from participant accounts in your account	Write			
UpdateSnapshot	Grants permission to update snapshot configuration	Write	snapshot*		
UpdateStorageVirtualMachine	Grants permission to update storage virtual machine configuration	Write	storage-virtual-machine*		
UpdateVolume	Grants permission to update volume configuration	Write	volume*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				fsx:StorageVirtualMachineId fsx:ParentVolumeId	

Resource types defined by Amazon FSx

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

> **Note**
>
> Amazon FSx for Windows File Server, Lustre, and Ontap share some of the same resource types, with the same ARN format for each.

Resource types	ARN	Condition keys
file-system	`arn:${Partition}:fsx:${Region}:${Account}:file-system/${FileSystemId}`	aws:ResourceTag/${TagKey}
file-cache	`arn:${Partition}:fsx:${Region}:${Account}:file-cache/${FileCacheId}`	aws:ResourceTag/${TagKey}
backup	`arn:${Partition}:fsx:${Region}:${Account}:backup/${BackupId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
storage-virtual-machine	arn:${Partition}:fsx:${Region}:${Account}:storage-virtual-machine/${FileSystemId}/${StorageVirtualMachineId}	aws:ResourceTag/${TagKey}
task	arn:${Partition}:fsx:${Region}:${Account}:task/${TaskId}	aws:ResourceTag/${TagKey}
association	arn:${Partition}:fsx:${Region}:${Account}:association/${FileSystemIdOrFileCacheId}/${DataRepositoryAssociationId}	aws:ResourceTag/${TagKey}
volume	arn:${Partition}:fsx:${Region}:${Account}:volume/${FileSystemId}/${VolumeId}	aws:ResourceTag/${TagKey}
snapshot	arn:${Partition}:fsx:${Region}:${Account}:snapshot/${VolumeId}/${SnapshotId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon FSx

Amazon FSx defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
fsx:IsBackupCopyDestination	Filters access by whether the backup is a destination backup for a CopyBackup operation	Bool
fsx:IsBackupCopySource	Filters access by whether the backup is a source backup for a CopyBackup operation	Bool
fsx:NfsDataRepositoryAuthenticationEnabled	Filters access by NFS data repositories which support authentication	Bool
fsx:NfsDataRepositoryEncryptionInTransitEnabled	Filters access by NFS data repositories which support encryption-in-transit	Bool
fsx:ParentVolumeId	Filters access by the containing parent volume for mutating volume operations	String
fsx:StorageVirtualMachineId	Filters access by the containing storage virtual machine for a volume for mutating volume operations	String

Actions, resources, and condition keys for AWS Health APIs and Notifications

AWS Health APIs and Notifications (service prefix: `health`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Health APIs and Notifications
- Resource types defined by AWS Health APIs and Notifications
- Condition keys for AWS Health APIs and Notifications

Actions defined by AWS Health APIs and Notifications

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAffectedAccountsForOrganization	Grants permission to retrieve a list of accounts that have been affected by the specified events in organization	Read			organizations:ListAccounts
DescribeAffectedEntities	Grants permission to retrieve a list of entities that have been affected by the specified events	Read	event*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				health:eventTypeCode health:service	
DescribeAffectedEntitiesForOrganization	Grants permission to retrieve a list of entities that have been affected by the specified events and accounts in organization	Read			organizations:ListAccounts
DescribeEntityAggregates	Grants permission to retrieve the number of entities that are affected by each of the specified events	Read			
DescribeEntityAggregatesForOrganization	Grants permission to retrieve the number of entities that are affected by each of the specified events in an organization	Read			organizations:ListAccounts
DescribeEventAggregates	Grants permission to retrieve the number of events of each event type (issue, scheduled change, and account notification)	Read			
DescribeEventDetails	Grants permission to retrieve detailed information about one or more specified events	Read	event*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				health:eventTypeCode health:service	
DescribeEventDetailsForOrganization	Grants permission to retrieve detailed information about one or more specified events for provided accounts in organization	Read			organizations:ListAccounts
DescribeEventTypes	Grants permission to retrieve the event types that meet the specified filter criteria	Read			
DescribeEvents	Grants permission to retrieve information about events that meet the specified filter criteria	Read			
DescribeEventsForOrganization	Grants permission to retrieve information about events that meet the specified filter criteria in organization	Read			organizations:ListAccounts
DescribeHealthServiceStatusForOrganization	Grants permission to retrieve the status of enabling or disabling the Organizational View feature	Read			organizations:ListAccounts

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableHealthServiceAccessForOrganization	Grants permission to disable the Organizational View feature	Permissions management			organizations:DisableAWSServiceAccess organizations:ListAccounts
EnableHealthServiceAccessForOrganization	Grants permission to enable the Organizational View feature	Permissions management			iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess organizations:ListAccounts

Resource types defined by AWS Health APIs and Notifications

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
event	`arn:${Partition}:health:*::event/${Service}/${EventTypeCode}/*`	

Condition keys for AWS Health APIs and Notifications

AWS Health APIs and Notifications defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
health:eventTypeCode	Filters access by event type	String
health:service	Filters access by impacted service	String

Actions, resources, and condition keys for AWS IAM Identity Center directory

AWS IAM Identity Center directory (service prefix: `sso-directory`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS IAM Identity Center directory
- Resource types defined by AWS IAM Identity Center directory
- Condition keys for AWS IAM Identity Center directory

Actions defined by AWS IAM Identity Center directory

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddMemberToGroup	Grants permission to add a member to a group in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
CompleteVirtualMfaDeviceRegistration	Grants permission to complete the creation process of a virtual MFA device	Write			
CompleteWebAuthnDeviceRegistration	Grants permission to complete the registration process of a WebAuthn device	Write			
CreateAlias	Grants permission to create an alias for the directory that AWS IAM Identity Center provides by default	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBearerToken	Grants permission to create a bearer token for a given provisioning tenant	Write			kms:Decrypt
CreateExternalIdPConfigurationForDirectory	Grants permission to create an External Identity Provider configuration for the directory	Write			
CreateGroup	Grants permission to create a group in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
CreateProvisioningTenant	Grants permission to create a provisioning tenant for a given directory	Write			kms:Decrypt
CreateUser	Grants permission to create a user in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
DeleteBearerToken	Grants permission to delete a bearer token	Write			kms:Decrypt
DeleteExternalIdPCertificate	Grants permission to delete the given external IdP certificate	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteExternalIdPConfigurationForDirectory	Grants permission to delete an External Identity Provider configuration associated with the directory	Write			
DeleteGroup	Grants permission to delete a group from the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
DeleteMfaDeviceForUser	Grants permission to delete a MFA device by device name for a given user	Write			
DeleteProvisioningTenant	Grants permission to delete the provisioning tenant	Write			kms:Decrypt
DeleteUser	Grants permission to delete a user from the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
DescribeDirectory	Grants permission to retrieve information about the directory that AWS IAM Identity Center provides by default	Read			
DescribeGroup	Grants permission to query the group data, not including user and group members	Read			kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeGroups	Grants permission to retrieve information about groups from the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
DescribeProvisioningTenant	Grants permission to describes the provisioning tenant	Read			kms:Decrypt
DescribeUser	Grants permission to retrieve information about a user from the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
DescribeUserByUniqueAttribute	Grants permission to describe user with a valid unique attribute represented for the user	Read			kms:Decrypt
DescribeUsers	Grants permission to retrieve information about user from the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
DisableExternalIdPConfigurationForDirectory	Grants permission to disable authentication of end users with an External Identity Provider	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableUser	Grants permission to deactivate a user in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
EnableExternalIdPConfigurationForDirectory	Grants permission to enable authentication of end users with an External Identity Provider	Write			
EnableUser	Grants permission to activate user in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
GetAWSSPConfigurationForDirectory	Grants permission to retrieve the AWS IAM Identity Center Service Provider configurations for the directory	Read			
GetGroupId	Grants permission to retrieve ID information about group from the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
GetUserId	Grants permission to retrieve ID information about user from the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUserPoolInfo	(Deprecated) Grants permission to get UserPool Info	Read			
ImportExternalIdPCertificate	Grants permission to import the IdP certificate used for verifying external IdP responses	Write			
IsMemberInGroup	Grants permission to check if a member is a part of the group in the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
IsMemberInGroups	Grants permission to check if a member is a part of multiple groups in the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
ListBearerTokens	Grants permission to list bearer tokens for a given provisioning tenant	Read			kms:Decrypt
ListExternalIdPCertificates	Grants permission to list the external IdP certificates of a given directory and IdP	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListExternalIdPConfigurationsForDirectory	Grants permission to list all the External Identity Provider configurations created for the directory	Read			
ListGroups	Grants permission to list groups from the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
ListGroupsForMember	Grants permission to list groups of the target member	Read			kms:Decrypt
ListGroupsForUser	Grants permission to list groups for a user from the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
ListMembersInGroup	Grants permission to retrieve all members that are part of a group in the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
ListMfaDevicesForUser	Grants permission to list all active MFA devices and their MFA device metadata for a user	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListProvisioningTenants	Grants permission to list provisioning tenants for a given directory	Read			kms:Decrypt
ListUsers	Grants permission to list users from the directory that AWS IAM Identity Center provides by default	Read			kms:Decrypt
RemoveMemberFromGroup	Grants permission to remove a member that is part of a group in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
SearchGroups	Grants permission to search for groups within the associated directory	Read			kms:Decrypt
SearchUsers	Grants permission to search for users within the associated directory	Read			kms:Decrypt
StartVirtualMfaDeviceRegistration	Grants permission to begin the creation process of virtual mfa device	Write			
StartWebAuthnDeviceRegistration	Grants permission to begin the registration process of a WebAuthn device	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateExternalIdPConfigurationForDirectory	Grants permission to update an External Identity Provider configuration associated with the directory	Write			
UpdateGroup	Grants permission to update information about a group in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
UpdateGroupDisplayName	Grants permission to update group display name update group display name response	Write			kms:Decrypt
UpdateMfaDeviceForUser	Grants permission to update MFA device information	Write			
UpdatePassword	Grants permission to update a password by sending password reset link via email or generating one time password for a user in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateUser	Grants permission to update user information in the directory that AWS IAM Identity Center provides by default	Write			kms:Decrypt
UpdateUserName	Grants permission to update user name update user name response	Write			kms:Decrypt
VerifyEmail	Grants permission to verify an email address of an User	Write			

Resource types defined by AWS IAM Identity Center directory

AWS IAM Identity Center directory does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS IAM Identity Center directory, specify `"Resource": "*"` in your policy.

Condition keys for AWS IAM Identity Center directory

IAM Identity Center directory has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) (service prefix: `iam`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Identity and Access Management (IAM)
- Resource types defined by AWS Identity and Access Management (IAM)
- Condition keys for AWS Identity and Access Management (IAM)

Actions defined by AWS Identity and Access Management (IAM)

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptDelegationRequest	Accepts a delegation request resource, granting the requested temporary access	Write	delegation-request*		
AddClientIDToOpenIDConnectProvider	Grants permission to add a new client ID (audience) to the list of registered IDs for the specified IAM OpenID Connect (OIDC) provider resource	Write	oidc-provider*		
AddRoleToInstanceProfile	Grants permission to add an IAM role to the specified instance profile	Write	instance-profile*		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddUserToGroup	Grants permission to add an IAM user to the specified IAM group	Write	group*		
AssociateDelegationRequest	Associates a delegation request resource with the calling identity	Write	delegation-request*		
AttachGroupPolicy	Grants permission to attach a managed policy to the specified IAM group	Permissions management	group*		
				iam:PolicyARN	
AttachRolePolicy	Grants permission to attach a managed policy to the specified IAM role	Permissions management	role*		
				iam:PolicyARN iam:PermissionsBoundary	
AttachUserPolicy	Grants permission to attach a managed policy to the specified IAM user	Permissions management	user*		
				iam:PolicyARN iam:PermissionsBoundary	
ChangePassword	Grants permission to an IAM user to change their own password	Write	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAccessKey	Grants permission to create access key and secret access key for the specified IAM user	Write	user*		
CreateAccountAlias	Grants permission to create an alias for your AWS account	Write			
CreateDelegationRequest	Creates an IAM delegation request resource for temporary access delegation	Write	delegation-request*		
				iam:DelegationDuration iam:NotificationChannel iam:TemplateArn	
CreateGroup	Grants permission to create a new group	Write	group*		
CreateInstanceProfile	Grants permission to create a new instance profile	Write	instance-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLoginProfile	Grants permission to create a password for the specified IAM user	Write	user*		
CreateOpenIDConnectProvider	Grants permission to create an IAM resource that describes an identity provider (IdP) that supports OpenID Connect (OIDC)	Write	oidc-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreatePolicy	Grants permission to create a new managed policy	Permissions management	policy*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePolicyVersion	Grants permission to create a new version of the specified managed policy	Permissions management	policy*		
CreateRole	Grants permission to create a new role	Write	role*		
				iam:PermissionsBoundary aws:TagKeys aws:RequestTag/${TagKey}	
CreateSAMLProvider	Grants permission to create an IAM resource that describes an identity provider (IdP) that supports SAML 2.0	Write	saml-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateServiceLinkedRole	Grants permission to create an IAM role that allows an AWS service to perform actions on your behalf	Write	role*		
				iam:AWSServiceName	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateServiceSpecificCredential	Grants permission to create a new service-specific credential for an IAM user	Write	user*		
				iam:ServiceSpecificCredentialAgeDays iam:ServiceSpecificCredentialServiceName	
CreateUser	Grants permission to create a new IAM user	Write	user*		
				iam:PermissionsBoundary aws:TagKeys aws:RequestTag/${TagKey}	
CreateVirtualMFADevice	Grants permission to create a new virtual MFA device	Write	mfa*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
DeactivateMFADevice	Grants permission to deactivate the specified MFA device and remove its association with the IAM user for which it was originally enabled	Write	user*		
DeleteAccessKey	Grants permission to delete the access key pair that is associated with the specified IAM user	Write	user*		
DeleteAccountAlias	Grants permission to delete the specified AWS account alias	Write			
DeleteAccountPasswordPolicy	Grants permission to delete the password policy for the AWS account	Permissions management			
DeleteCloudFrontPublicKey	Grants permission to delete an existing CloudFront public key	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteGroup	Grants permission to delete the specified IAM group	Write	group*		
DeleteGroupPolicy	Grants permission to delete the specified inline policy from its group	Permissions management	group*		
DeleteInstanceProfile	Grants permission to delete the specified instance profile	Write	instance-profile*		
DeleteLoginProfile	Grants permission to delete the password for the specified IAM user	Write	user*		
DeleteOpenIDConnectProvider	Grants permission to delete an OpenID Connect identity provider (IdP) resource object in IAM	Write	oidc-provider*		
DeletePolicy	Grants permission to delete the specified managed policy and remove it from any IAM entities (users, groups, or roles) to which it is attached	Permissions management	policy*		
DeletePolicyVersion	Grants permission to delete a version from the specified managed policy	Permissions management	policy*		
DeleteRole	Grants permission to delete the specified role	Write	role*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				iam:PermissionsBoundary	
DeleteRolePermissionsBoundary	Grants permission to remove the permissions boundary from a role	Permissions management	role*		
				iam:PermissionsBoundary	
DeleteRolePolicy	Grants permission to delete the specified inline policy from the specified role	Permissions management	role*		
				iam:PermissionsBoundary	
DeleteSAMLProvider	Grants permission to delete a SAML provider resource in IAM	Write	saml-provider*		
DeleteSSHPublicKey	Grants permission to delete the specified SSH public key	Write	user*		
DeleteServerCertificate	Grants permission to delete the specified server certificate	Write	server-certificate*		
DeleteServiceLinkedRole	Grants permission to delete an IAM role that is linked to a specific AWS service, if the service is no longer using it	Write	role*		
DeleteServiceSpecificCredential	Grants permission to delete the specified service-specific credential for an IAM user	Write	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				iam:ServiceSpecificCredentialServiceName	
DeleteSigningCertificate	Grants permission to delete a signing certificate that is associated with the specified IAM user	Write	user*		
DeleteUser	Grants permission to delete the specified IAM user	Write	user*		
DeleteUserPermissionsBoundary	Grants permission to remove the permissions boundary from the specified IAM user	Permissions management	user*		
				iam:PermissionsBoundary	
DeleteUserPolicy	Grants permission to delete the specified inline policy from an IAM user	Permissions management	user*		
				iam:PermissionsBoundary	
DeleteVirtualMFADevice	Grants permission to delete a virtual MFA device	Write	mfa		
			sms-mfa		
DetachGroupPolicy	Grants permission to detach a managed policy from the specified IAM group	Permissions management	group*		
				iam:PolicyARN	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachRolePolicy	Grants permission to detach a managed policy from the specified role	Permissions management	role*		
				iam:PolicyARN iam:PermissionsBoundary	
DetachUserPolicy	Grants permission to detach a managed policy from the specified IAM user	Permissions management	user*		
				iam:PolicyARN iam:PermissionsBoundary	
DisableOrganizationsRootCredentialsManagement	Grants permission to disable the management of member account root user credentials for an organization managed under the current account	Write			
DisableOrganizationsRootSessions	Grants permission to disable privileged root actions in member accounts for an organization managed under the current account	Write			
DisableOutboundWebIdentityFederation	Disables the outbound identity federation feature for the callers account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableMFADevice	Grants permission to enable an MFA device and associate it with the specified IAM user	Write	user*		
				iam:RegisterSecurityKey iam:FIDO-FIPS-140-2-certification iam:FIDO-FIPS-140-3-certification iam:FIDO-certification	
EnableOrganizationsRootCredentialsManagement	Grants permission to enable the management of member account root user credentials for an organization managed under the current account	Write			
EnableOrganizationsRootSessions	Grants permission to enable privileged root actions in member accounts for an organization managed under the current account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableOutboundWebIdentityFederation	Enables the outbound identity federation feature for the callers account	Write			
GenerateCredentialReport	Grants permission to generate a credential report for the AWS account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateOrganizationsAccessReport	Grants permission to generate an access report for an AWS Organizations entity	Read	access-report*		organizations:DescribePolicy organizations:ListChildren organizations:ListParents organizations:ListPoliciesForTarget organizations:ListRoots organizations:ListTargetsForPolicy
				iam:OrganizationsPolicyId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateServiceLastAccessedDetails	Grants permission to generate a service last accessed data report for an IAM resource	Read	group*		
			policy*		
			role*		
			user*		
GetAccessKeyLastUsed	Grants permission to retrieve information about when the specified access key was last used	Read	user*		
GetAccountAuthorizationDetails	Grants permission to retrieve information about all IAM users, groups, roles, and policies in your AWS account, including their relationships to one another	Read			
GetAccountEmailAddress	Grants permission to retrieve the email address that is associated with the account	Read			
GetAccountName	Grants permission to retrieve the account name that is associated with the account	Read			
GetAccountPasswordPolicy	Grants permission to retrieve the password policy for the AWS account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccountSummary	Grants permission to retrieve information about IAM entity usage and IAM quotas in the AWS account	List			
GetCloudFrontPublicKey	Grants permission to retrieve information about the specified CloudFront public key	Read			
GetContextKeysForCustomPolicy	Grants permission to retrieve a list of all of the context keys that are referenced in the specified policy	Read			
GetContextKeysForPrincipalPolicy	Grants permission to retrieve a list of all context keys that are referenced in all IAM policies that are attached to the specified IAM identity (user, group, or role)	Read	group role user		
GetCredentialReport	Grants permission to retrieve a credential report for the AWS account	Read			
GetDelegationRequest	Retrieves information about a specific delegation request	Read	delegation-request*		
GetGroup	Grants permission to retrieve a list of IAM users in the specified IAM group	Read	group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetGroupPolicy	Grants permission to retrieve an inline policy document that is embedded in the specified IAM group	Read	group*		
GetHumanReadableSummary	Retrieves a human readable summary for a given entity. At this time, only delegation request are supported	Read	delegation-request*		
GetInstanceProfile	Grants permission to retrieve information about the specified instance profile, including the instance profile's path, GUID, ARN, and role	Read	instance-profile*		
GetLoginProfile	Grants permission to retrieve the user name and password creation date for the specified IAM user	List	user*		
GetMFADevice	Grants permission to retrieve information about an MFA device for the specified user	Read	user*		
GetOpenIDConnectProvider	Grants permission to retrieve information about the specified OpenID Connect (OIDC) provider resource in IAM	Read	oidc-provider*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetOrganizationsAccessReport	Grants permission to retrieve an AWS Organizations access report	Read			
GetOutboundWebIdentityFederationInfo	Retrieves the configuration information for the outbound identity federation feature for the callers account	Read			
GetPolicy	Grants permission to retrieve information about the specified managed policy, including the policy's default version and the total number of identities to which the policy is attached	Read	policy*		
GetPolicyVersion	Grants permission to retrieve information about a version of the specified managed policy, including the policy document	Read	policy*		
GetRole	Grants permission to retrieve information about the specified role, including the role's path, GUID, ARN, and the role's trust policy	Read	role*		
				iam:PermissionsBoundary	
GetRolePolicy	Grants permission to retrieve an inline policy document that is embedded with the specified IAM role	Read	role*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSAMLProvider	Grants permission to retrieve the SAML provider metadocument that was uploaded when the IAM SAML provider resource was created or updated	Read	saml-provider*		
GetSSHPublicKey	Grants permission to retrieve the specified SSH public key, including metadata about the key	Read	user*		
GetServerCertificate	Grants permission to retrieve information about the specified server certificate stored in IAM	Read	server-certificate*		
GetServiceLastAccessedDetails	Grants permission to retrieve information about the service last accessed data report	Read			
GetServiceLastAccessedDetailsWithEntities	Grants permission to retrieve information about the entities from the service last accessed data report	Read			
GetServiceLinkedRoleDeletionStatus	Grants permission to retrieve an IAM service-linked role deletion status	Read	role*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUser	Grants permission to retrieve information about the specified IAM user, including the user's creation date, path, unique ID, and ARN	Read	user*		
GetUserPolicy	Grants permission to retrieve an inline policy document that is embedded in the specified IAM user	Read	user*		
ListAccessKeys	Grants permission to list information about the access key IDs that are associated with the specified IAM user	List	user*		
ListAccountAliases	Grants permission to list the account alias that is associated with the AWS account	List			
ListAttachedGroupPolicies	Grants permission to list all managed policies that are attached to the specified IAM group	List	group*		
ListAttachedRolePolicies	Grants permission to list all managed policies that are attached to the specified IAM role	List	role*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAttachedUserPolicies	Grants permission to list all managed policies that are attached to the specified IAM user	List	user*		
ListCloudFrontPublicKeys	Grants permission to list all current CloudFront public keys for the account	List			
ListDelegationRequests	Lists delegation requests based on the specified criteria	List		iam:DelegationRequestOwner	
ListEntitiesForPolicy	Grants permission to list all IAM identities to which the specified managed policy is attached	List	policy*		
ListGroupPolicies	Grants permission to list the names of the inline policies that are embedded in the specified IAM group	List	group*		
ListGroups	Grants permission to list the IAM groups that have the specified path prefix	List			
ListGroupsForUser	Grants permission to list the IAM groups that the specified IAM user belongs to	List	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListInstanceProfileTags	Grants permission to list the tags that are attached to the specified instance profile	List	instance-profile*		
ListInstanceProfiles	Grants permission to list the instance profiles that have the specified path prefix	List			
ListInstanceProfilesForRole	Grants permission to list the instance profiles that have the specified associated IAM role	List	role*		
ListMFADeviceTags	Grants permission to list the tags that are attached to the specified virtual mfa device	List	mfa*		
ListMFADevices	Grants permission to list the MFA devices for an IAM user	List	user		
ListOpenIDConnectProviderTags	Grants permission to list the tags that are attached to the specified OpenID Connect provider	List	oidc-provider*		
ListOpenIDConnectProviders	Grants permission to list information about the IAM OpenID Connect (OIDC) provider resource objects that are defined in the AWS account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListOrganizationsFeatures	Grants permission to list the centralized root access features enabled for your organization	List			
ListPolicies	Grants permission to list all managed policies	List			
ListPoliciesGrantingServiceAccess	Grants permission to list information about the policies that grant an entity access to a specific service	List	group*		
			role*		
			user*		
ListPolicyTags	Grants permission to list the tags that are attached to the specified managed policy	List	policy*		
ListPolicyVersions	Grants permission to list information about the versions of the specified managed policy, including the version that is currently set as the policy's default version	List	policy*		
ListRolePolicies	Grants permission to list the names of the inline policies that are embedded in the specified IAM role	List	role*		
ListRoleTags	Grants permission to list the tags that are attached to the specified IAM role	List	role*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRoles	Grants permission to list the IAM roles that have the specified path prefix	List			
ListSAMLProviderTags	Grants permission to list the tags that are attached to the specified SAML provider	List	saml-provider*		
ListSAMLProviders	Grants permission to list the SAML provider resources in IAM	List			
ListSSHPublicKeys	Grants permission to list information about the SSH public keys that are associated with the specified IAM user	List	user*		
ListSTSRegionalEndpointsStatus	Grants permission to list the status of all active STS regional endpoints	List			
ListServerCertificateTags	Grants permission to list the tags that are attached to the specified server certificate	List	server-certificate*		
ListServerCertificates	Grants permission to list the server certificates that have the specified path prefix	List			
ListServiceSpecificCredentials	Grants permission to list the service-specific credentials that are associated with the specified IAM user	List	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSigningCertificates	Grants permission to list information about the signing certificates that are associated with the specified IAM user	List	user*		
ListUserPolicies	Grants permission to list the names of the inline policies that are embedded in the specified IAM user	List	user*		
ListUserTags	Grants permission to list the tags that are attached to the specified IAM user	List	user*		
ListUsers	Grants permission to list the IAM users that have the specified path prefix	List			
ListVirtualMFADevices	Grants permission to list virtual MFA devices by assignment status	List			
PassRole [permission only]	Grants permission to pass a role to a service	Write	role*		
				iam:AssociatedResourceArn iam:PassedToService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutGroupPolicy	Grants permission to create or update an inline policy document that is embedded in the specified IAM group	Permissions management	group*		
PutRolePermissionsBoundary	Grants permission to set a managed policy as a permissions boundary for a role	Permissions management	role*		
				iam:PermissionsBoundary	
PutRolePolicy	Grants permission to create or update an inline policy document that is embedded in the specified IAM role	Permissions management	role*		
				iam:PermissionsBoundary	
PutUserPermissionsBoundary	Grants permission to set a managed policy as a permissions boundary for an IAM user	Permissions management	user*		
				iam:PermissionsBoundary	
PutUserPolicy	Grants permission to create or update an inline policy document that is embedded in the specified IAM user	Permissions management	user*		
				iam:PermissionsBoundary	
RejectDelegationRequest	Rejects a delegation request, denying the requested temporary access	Write	delegation-request*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveClientIDFromOpenIDConnectProvider	Grants permission to remove the client ID (audience) from the list of client IDs in the specified IAM OpenID Connect (OIDC) provider resource	Write	oidc-provider*		
RemoveRoleFromInstanceProfile	Grants permission to remove an IAM role from the specified EC2 instance profile	Write	instance-profile*		
RemoveUserFromGroup	Grants permission to remove an IAM user from the specified group	Write	group*		
ResetServiceSpecificCredential	Grants permission to reset the password for an existing service-specific credential for an IAM user	Write	user*		
				iam:ServiceSpecificCredentialServiceName	
ResyncMFADevice	Grants permission to synchronize the specified MFA device with its IAM entity (user or role)	Write	user*		
SendDelegationToken	Sends the exchange token for an accepted delegation request	Write	delegation-request*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetDefaultPolicyVersion	Grants permission to set the version of the specified policy as the policy's default version	Permissions management	policy*		
SetSTSRegionalEndpointStatus	Grants permission to activate or deactivate an STS regional endpoint	Write			
SetSecurityTokenServicePreferences	Grants permission to set the STS global endpoint token version	Write			
SimulateCustomPolicy	Grants permission to simulate whether an identity-based policy or resource-based policy provides permissions for specific API operations and resources	Read			
SimulatePrincipalPolicy	Grants permission to simulate whether an identity-based policy that is attached to a specified IAM entity (user or role) provides permissions for specific API operations and resources	Read	group role user		
TagInstanceProfile	Grants permission to add tags to an instance profile	Tagging	instance-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
TagMFADevice	Grants permission to add tags to a virtual mfa device	Tagging	mfa*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagOpenIDConnectProvider	Grants permission to add tags to an OpenID Connect provider	Tagging	oidc-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagPolicy	Grants permission to add tags to a managed policy	Tagging	policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
TagRole	Grants permission to add tags to an IAM role	Tagging	role*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagSAMLProvider	Grants permission to add tags to a SAML Provider	Tagging	saml-provider*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagServerCertificate	Grants permission to add tags to a server certificate	Tagging	server-certificate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
TagUser	Grants permission to add tags to an IAM user	Tagging	user*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagInstanceProfile	Grants permission to remove the specified tags from the instance profile	Tagging	instance-profile*		
				aws:TagKeys	
UntagMFADevice	Grants permission to remove the specified tags from the virtual mfa device	Tagging	mfa*		
				aws:TagKeys	
UntagOpenIDConnectProvider	Grants permission to remove the specified tags from the OpenID Connect provider	Tagging	oidc-provider*		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagPolicy	Grants permission to remove the specified tags from the managed policy	Tagging	policy*		
				aws:TagKeys	
UntagRole	Grants permission to remove the specified tags from the role	Tagging	role*		
				aws:TagKeys	
UntagSAMLProvider	Grants permission to remove the specified tags from the SAML Provider	Tagging	saml-provider*		
				aws:TagKeys	
UntagServerCertificate	Grants permission to remove the specified tags from the server certificate	Tagging	server-certificate*		
				aws:TagKeys	
UntagUser	Grants permission to remove the specified tags from the user	Tagging	user*		
				aws:TagKeys	
UpdateAccessKey	Grants permission to update the status of the specified access key as Active or Inactive	Write	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAccountEmailAddress	Grants permission to update the email address that is associated with the account	Write			
UpdateAccountName	Grants permission to update the account name that is associated with the account	Write			
UpdateAccountPasswordPolicy	Grants permission to update the password policy settings for the AWS account	Write			
UpdateAssumeRolePolicy	Grants permission to update the policy that grants an IAM entity permission to assume a role	Permissions management	role*		
				iam:PermissionsBoundary	
UpdateCloudFrontPublicKey	Grants permission to update an existing CloudFront public key	Write			
UpdateGroup	Grants permission to update the name or path of the specified IAM group	Write	group*		
UpdateLoginProfile	Grants permission to change the password for the specified IAM user	Write	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateOpenIDConnectProviderThumbprint	Grants permission to update the entire list of server certificate thumbprints that are associated with an OpenID Connect (OIDC) provider resource	Write	oidc-provider*		
UpdateRole	Grants permission to update the description or maximum session duration setting of a role	Write	role*		
				iam:PermissionsBoundary	
UpdateRoleDescription	Grants permission to update only the description of a role	Write	role*		
				iam:PermissionsBoundary	
UpdateSAMLProvider	Grants permission to update the metadata document for an existing SAML provider resource	Write	saml-provider*		
UpdateSSHPublicKey	Grants permission to update the status of an IAM user's SSH public key to active or inactive	Write	user*		
UpdateServerCertificate	Grants permission to update the name or the path of the specified server certificate stored in IAM	Write	server-certificate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateServiceSpecificCredential	Grants permission to update the status of a service-specific credential to active or inactive for an IAM user	Write	user*		
				iam:ServiceSpecificCredentialServiceName	
UpdateSigningCertificate	Grants permission to update the status of the specified user signing certificate to active or disabled	Write	user*		
UpdateUser	Grants permission to update the name or the path of the specified IAM user	Write	user*		
UploadCloudFrontPublicKey	Grants permission to upload a CloudFront public key	Write			
UploadSSHPublicKey	Grants permission to upload an SSH public key and associate it with the specified IAM user	Write	user*		
UploadServerCertificate	Grants permission to upload a server certificate entity for the AWS account	Write	server-certificate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UploadSigningCertificate	Grants permission to upload an X.509 signing certificate and associate it with the specified IAM user	Write	user*		

Resource types defined by AWS Identity and Access Management (IAM)

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
access-report	`arn:${Partition}:iam::${Account}:access-report/${EntityPath}`	
assumed-role	`arn:${Partition}:iam::${Account}:assumed-role/${RoleName}/${RoleSessionName}`	

Resource types	ARN	Condition keys
federated-user	arn:${Partition}:iam::${Account}:federated-user/${UserName}	
group	arn:${Partition}:iam::${Account}:group/${GroupNameWithPath}	
instance-profile	arn:${Partition}:iam::${Account}:instance-profile/${InstanceProfileNameWithPath}	aws:ResourceTag/${TagKey}
mfa	arn:${Partition}:iam::${Account}:mfa/${MfaTokenIdWithPath}	aws:ResourceTag/${TagKey}
oidc-provider	arn:${Partition}:iam::${Account}:oidc-provider/${OidcProviderName}	aws:ResourceTag/${TagKey}
policy	arn:${Partition}:iam::${Account}:policy/${PolicyNameWithPath}	aws:ResourceTag/${TagKey}
role	arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}	aws:ResourceTag/${TagKey} iam:ResourceTag/${TagKey}
saml-provider	arn:${Partition}:iam::${Account}:saml-provider/${SamlProviderName}	aws:ResourceTag/${TagKey}
server-certificate	arn:${Partition}:iam::${Account}:server-certificate/${CertificateNameWithPath}	aws:ResourceTag/${TagKey}
sms-mfa	arn:${Partition}:iam::${Account}:sms-mfa/${MfaTokenIdWithPath}	

Resource types	ARN	Condition keys
user	arn:${Partition}:iam::${Account}:user/${UserNameWithPath}	aws:ResourceTag/${TagKey} iam:ResourceTag/${TagKey}
delegation-request	arn:${Partition}:iam::${Account}:delegation-request/${DelegationRequestId}	iam:DelegationRequestOwner

Condition keys for AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access based on the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access based on the tags associated with the resource	String
aws:TagKeys	Filters access based on the tag keys that are passed in the request	ArrayOfString
iam:AWSServiceName	Filters access by the AWS service to which this role is attached	String

Condition keys	Description	Type
iam:AssociatedResourceArn	Filters access by the resource that the role will be used on behalf of	ARN
iam:DelegationDuration	Filters access based on the requested delegation duration	String
iam:DelegationRequestOwner	Filters access based on the delegation request owner	ARN
iam:FIDO-FIPS-140-2-certification	Filters access by the MFA device FIPS-140-2 validation certification level at the time of registration of a FIDO security key	String
iam:FIDO-FIPS-140-3-certification	Filters access by the MFA device FIPS-140-3 validation certification level at the time of registration of a FIDO security key	String
iam:FIDO-certification	Filters access by the MFA device FIDO certification level at the time of registration of a FIDO security key	String
iam:NotificationChannel	Filters access based on the requested notification channel	String
iam:OrganizationsPolicyId	Filters access by the ID of an AWS Organizations policy	String
iam:PassedToService	Filters access by the AWS service to which this role is passed	String
iam:PermissionsBoundary	Filters access if the specified policy is set as the permissions boundary on the IAM entity (user or role)	ARN
iam:PolicyARN	Filters access by the ARN of an IAM policy	ARN

Condition keys	Description	Type
iam:RegisterSecurityKey	Filters access by the current state of MFA device enablement	String
iam:ResourceTag/${TagKey}	Filters access by the tags attached to an IAM entity (user or role)	String
iam:ServiceSpecificCredentialAgeDays	Filters access by the duration until the credential's expiration	Numeric
iam:ServiceSpecificCredentialServiceName	Filters access by the service associated with the credential	String
iam:TemplateArn	Filters access based on the requested template ARN	ARN

Actions, resources, and condition keys for AWS Identity and Access Management Roles Anywhere

AWS Identity and Access Management Roles Anywhere (service prefix: `rolesanywhere`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Identity and Access Management Roles Anywhere

- Resource types defined by AWS Identity and Access Management Roles Anywhere
- Condition keys for AWS Identity and Access Management Roles Anywhere

Actions defined by AWS Identity and Access Management Roles Anywhere

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateProfile	Grants permission to create a profile	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateTrustAnchor	Grants permission to create a trust anchor	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAttributeMapping	Grants permission to delete a mapping rule from a profile	Write	profile*		
DeleteCrl	Grants permission to delete a certificate revocation list (crl)	Write	crl*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteProfile	Grants permission to delete a profile	Write	profile*		
DeleteTrustAnchor	Grants permission to delete a trust anchor	Write	trust-anchor*		
DisableCrl	Grants permission to disable a certificate revocation list (crl)	Write	crl*		
DisableProfile	Grants permission to disable a profile	Write	profile*		
DisableTrustAnchor	Grants permission to disable a trust anchor	Write	trust-anchor*		
EnableCrl	Grants permission to enable a certificate revocation list (crl)	Write	crl*		
EnableProfile	Grants permission to enable a profile	Write	profile*		iam:PassRole
EnableTrustAnchor	Grants permission to enable a trust anchor	Write	trust-anchor*		
GetCrl	Grants permission to get a certificate revocation list (crl)	Read	crl*		
GetProfile	Grants permission to get a profile	Read	profile*		
GetSubject	Grants permission to get a subject	Read	subject*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTrustAnchor	Grants permission to get a trust anchor	Read	trust-anchor*		
ImportCrl	Grants permission to import a certificate revocation list (crl)	Write		aws:RequestTag/${TagKey} aws:TagKeys	
ListCrls	Grants permission to list certificate revocation lists (crls)	List			
ListProfiles	Grants permission to list profiles	List			
ListSubjects	Grants permission to list subjects	List			
ListTagsForResource	Grants permission to list tags for a resource	List			
ListTrustAnchors	Grants permission to list trust anchors	List			
PutAttributeMapping	Grants permission to put a mapping rule into a profile	Write	profile*		
PutNotificationSettings	Grants permission to attach notification settings to a trust anchor	Write	trust-anchor*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetNotificationSettings	Grants permission to reset custom notification settings to IAM Roles Anywhere defined default state	Write	trust-anchor*		
TagResource	Grants permission to tag a resource	Tagging	crl		
			profile		
			subject		
			trust-anchor		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	crl		
			profile		
			subject		
			trust-anchor		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCrl	Grants permission to update a certificate revocation list (crl)	Write	crl*		
UpdateProfile	Grants permission to update a profile	Write	profile*		iam:PassRole
UpdateTrustAnchor	Grants permission to update a trust anchor	Write	trust-anchor*		

Resource types defined by AWS Identity and Access Management Roles Anywhere

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
trust-anchor	`arn:${Partition}:rolesanywhere:${Region}:${Account}:trust-anchor/${TrustAnchorId}`	aws:ResourceTag/${TagKey}
profile	`arn:${Partition}:rolesanywhere:${Region}:${Account}:profile/${ProfileId}`	aws:ResourceTag/${TagKey}
subject	`arn:${Partition}:rolesanywhere:${Region}:${Account}:subject/${SubjectId}`	aws:ResourceTag/${TagKey}
crl	`arn:${Partition}:rolesanywhere:${Region}:${Account}:crl/${CrlId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Identity and Access Management Roles Anywhere

AWS Identity and Access Management Roles Anywhere defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Identity Store

AWS Identity Store (service prefix: `identitystore`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Identity Store
- Resource types defined by AWS Identity Store
- Condition keys for AWS Identity Store

Actions defined by AWS Identity Store

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGroup	Grants permission to create a group in the specified IdentityStore	Write	Identitystore*		kms:Decrypt
				identitystore:PrimaryRegion identitystore:GroupExternalIdIssuers	
CreateGroupMembership	Grants permission to create a member to a group in the specified IdentityStore	Write	Group*		kms:Decrypt
			Identitystore*		
			User*		
				identitystore:PrimaryRegion	
CreateIdentityStore	Grants permission to create a new IdentityStore in an AWS account	Write			kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					kms:DescribeKey kms:Encrypt kms:GenerateDataKeyWithoutPlaintext
CreateUser	Grants permission to create a user in the specified IdentityStore	Write	Identitystore*		kms:Decrypt
				identitystore:PrimaryRegion identitystore:UserExternalIdIssuers identitystore:ReservedUserId	
DeleteGroup	Grants permission to delete a group in the specified IdentityStore	Write	Group*		kms:Decrypt
			Identitystore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				identitystore:PrimaryRegion identitystore:GroupExternalIdIssuers	
DeleteGroupMembership	Grants permission to remove a member that is part of a group in the specified IdentityStore	Write	Group*		kms:Decrypt
			GroupMembership*		
			Identitystore*		
			User*		
				identitystore:PrimaryRegion	
DeleteIdentityStore	Grants permission to delete an IdentityStore	Write			
DeleteUser	Grants permission to delete a user in the specified IdentityStore	Write	Identitystore*		kms:Decrypt
			User*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				identitystore:PrimaryRegion identitystore:UserExternalIdIssuers	
DescribeGroup	Grants permission to retrieve information about a group in the specified IdentityStore	Read	Group*		kms:Decrypt
			Identitystore*		
				identitystore:PrimaryRegion identitystore:GroupExternalIdIssuers	
DescribeGroupMembership	Grants permission to retrieve information about a member that is part of a group in the specified IdentityStore	Read	Group*		kms:Decrypt
			GroupMembership*		
			Identitystore*		
			User*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				identitystore:PrimaryRegion	
DescribeUser	Grants permission to retrieve information about user in the specified IdentityStore	Read	Identitystore*		kms:Decrypt
			User*		
				identitystore:PrimaryRegion identitystore:UserExternalIdIssuers	
GetGroupId	Grants permission to retrieve ID information about group in the specified IdentityStore	Read	Group*		kms:Decrypt
			Identitystore*		
				identitystore:PrimaryRegion	
GetGroupMembershipId	Grants permission to retrieve ID information of a member which is part of a group in the specified IdentityStore	Read	Group*		kms:Decrypt
			GroupMembership*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Identitystore*		
			User*		
				identitystore:PrimaryRegion	
GetUserId	Grants permission to retrieves ID information about user in the specified IdentityStore	Read	Identitystore*		kms:Decrypt
			User*		
				identitystore:PrimaryRegion	
IsMemberInGroups	Grants permission to check if a member is a part of groups in the specified IdentityStore	Read	AllGroupMemberships*		kms:Decrypt
			Group*		
			Identitystore*		
			User*		
				identitystore:PrimaryRegion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListGroupMemberships	Grants permission to retrieve all members that are part of a group in the specified IdentityStore	List	AllGroupMemberships*		kms:Decrypt
			Group*		
			Identitystore*		
				identitystore:PrimaryRegion	
ListGroupMembershipsForMember	Grants permission to list groups of the target member in the specified IdentityStore	List	AllGroupMemberships*		kms:Decrypt
			Identitystore*		
			User*		
				identitystore:PrimaryRegion	
ListGroups	Grants permission to search for groups within the specified IdentityStore	List	AllGroups*		kms:Decrypt
			Identitystore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				identitystore:PrimaryRegion identitystore:GroupExternalIdIssuers	
ListUsers	Grants permission to search for users in the specified IdentityStore	List	AllUsers*		kms:Decrypt
			Identitystore*		
				identitystore:PrimaryRegion identitystore:UserExternalIdIssuers	
ReserveUser	Grants permission to reserve a user by getting a userId	Write	Identitystore*		kms:Decrypt
				identitystore:PrimaryRegion	
UpdateGroup	Grants permission to update information about a group in the specified IdentityStore	Write	Group*		kms:Decrypt

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Identitystore*		
				identitystore:PrimaryRegion identitystore:GroupExternalIdIssuers	
UpdateIdentityStore	Grants permission to update the configuration of an IdentityStore	Write			kms:Decrypt kms:DescribeKey kms:Encrypt kms:GenerateDataKeyWithoutPlaintext
UpdateUser	Grants permission to update user information in the specified IdentityStore	Write	Identitystore*		kms:Decrypt
			User*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				identitystore:PrimaryRegion identitystore:UserExternalIdIssuers	

Resource types defined by AWS Identity Store

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
Identitystore	`arn:${Partition}:identitystore::${Account}:identitystore/${IdentityStoreId}`	
User	`arn:${Partition}:identitystore:::user/${UserId}`	
Group	`arn:${Partition}:identitystore:::group/${GroupId}`	
GroupMembership	`arn:${Partition}:identitystore:::membership/${MembershipId}`	

Resource types	ARN	Condition keys
AllUsers	arn:${Partition}:identitystore:::user/*	
AllGroups	arn:${Partition}:identitystore:::group/*	
AllGroupMemberships	arn:${Partition}:identitystore:::membership/*	

Condition keys for AWS Identity Store

AWS Identity Store defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
identitystore:GroupExternalIdIssuers	Filters access by Issuer present in ExternalIds for Group resources	ArrayOfARN
identitystore:IdentityStoreArn	Filters access by Identity Store ARN	ARN
identitystore:PrimaryRegion	Filters access by Primary Region of Identity Store	String

Condition keys	Description	Type
identitystore:ReservedUserId	Filters access by a previously reserved User ID for CreateUser operation	String
identitystore:UserExternalIdIssuers	Filters access by Issuer present in ExternalIds for User resources	ArrayOfARN
identitystore:UserId	Filters access by Identity Store User ID	String

Actions, resources, and condition keys for AWS Key Management Service

AWS Key Management Service (service prefix: `kms`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Key Management Service
- Resource types defined by AWS Key Management Service
- Condition keys for AWS Key Management Service

Actions defined by AWS Key Management Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelKeyDeletion	Controls permission to cancel the scheduled deletion of an AWS KMS key	Write	key*		
				kms:CallerAccount kms:ViaService	
ConnectCustomKeyStore	Controls permission to connect or reconnect a custom key store to its associated AWS CloudHSM cluster or external key manager outside of AWS	Write		kms:CallerAccount	
CreateAlias	Controls permission to create an alias for an AWS KMS key. Aliases are optional friendly names that you can associate with KMS keys	Write	alias*		
			key*		
				kms:CallerAccount kms:ViaService	
CreateCustomKeyStore	Controls permission to create a custom key store that is backed by an AWS CloudHSM cluster or an external key manager outside of AWS	Write		kms:CallerAccount	cloudhsm:DescribeClusters ec2:DescribeVpcEndpointServices

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGrant	Controls permission to add a grant to an AWS KMS key. You can use grants to add permissions without changing the key policy or IAM policy	Permissions management	key*	kms:CallerAccount kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:GrantConstraintType kms:GranteePrincipal kms:GrantIsForAWSResource kms:GrantOperations kms:RetiringPrincipal	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateKey	Controls permission to create an AWS KMS key that can be used to protect data keys and other sensitive information	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys kms:BypassPolicyLockoutSafetyCheck kms:CallerAccount kms:KeySpec kms:KeyUsage kms:KeyOrigin kms:MultiRegion	iam:CreateServiceLinkedRole kms:PutKeyPolicy kms:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:MultiRegionKeyType kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Decrypt	Controls permission to decrypt ciphertext that was encrypted under an AWS KMS key	Write	key*	kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RecipientAttestation:ImageSha384 kms:RecipientAttestation:NitroTPMPCR0 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR1 kms:RecipientAttestation:NitroTPMPCR2 kms:RecipientAttestation:NitroTPMPCR3 kms:RecipientAttestation:NitroTPMPCR4 kms:RecipientAttestation:NitroTPMPCR5 kms:RecipientAttestation:NitroTPMPCR6	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR7 kms:RecipientAttestation:NitroTPMPCR8 kms:RecipientAttestation:NitroTPMPCR9 kms:RecipientAttestation:NitroTPMPCR10 kms:RecipientAttestation:NitroTPMPCR11 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR12 kms:RecipientAttestation:NitroTPMPCR13 kms:RecipientAttestation:NitroTPMPCR14 kms:RecipientAttestation:NitroTPMPCR15 kms:RecipientAttestation:NitroTPMPCR16 kms:RecipientAttestation:NitroTPMPCR17	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR18 kms:RecipientAttestation:NitroTPMPCR19 kms:RecipientAttestation:NitroTPMPCR20 kms:RecipientAttestation:NitroTPMPCR21 kms:RecipientAttestation:NitroTPMPCR22 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR23 kms:RecipientAttestation:PCR0 kms:RecipientAttestation:PCR1 kms:RecipientAttestation:PCR2 kms:RecipientAttestation:PCR3 kms:RecipientAttestation:PCR4 kms:RecipientAttestation:PCR5	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR6 kms:RecipientAttestation:PCR7 kms:RecipientAttestation:PCR8 kms:RecipientAttestation:PCR9 kms:RecipientAttestation:PCR10 kms:RecipientAttestation:PCR11 kms:RecipientAttestation:PCR12	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR13 kms:RecipientAttestation:PCR14 kms:RecipientAttestation:PCR15 kms:RecipientAttestation:PCR16 kms:RecipientAttestation:PCR17 kms:RecipientAttestation:PCR18 kms:RecipientAttestation:PCR19	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR20 kms:RecipientAttestation:PCR21 kms:RecipientAttestation:PCR22 kms:RecipientAttestation:PCR23 kms:RecipientAttestation:PCR24 kms:RecipientAttestation:PCR25 kms:RecipientAttestation:PCR26	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR27 kms:RecipientAttestation:PCR28 kms:RecipientAttestation:PCR29 kms:RecipientAttestation:PCR30 kms:RecipientAttestation:PCR31 kms:RequestAlias kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAlias	Controls permission to delete an alias. Aliases are optional friendly names that you can associate with AWS KMS keys	Write	alias*		
			key*		
				kms:CallerAccount kms:ViaService	
DeleteCustomKeyStore	Controls permission to delete a custom key store	Write		kms:CallerAccount	
DeleteImportedKeyMaterial	Controls permission to delete cryptographic material that you imported into an AWS KMS key. This action makes the key unusable	Write	key*		
				kms:CallerAccount kms:ViaService	
DeriveSharedSecret	Controls permission to use the specified AWS KMS key to derive shared secrets	Write	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:CallerAccount kms:KeyAgreementAlgorithm kms:RecipientAttestation:ImageSha384 kms:RecipientAttestation:NitroTPMPCR0 kms:RecipientAttestation:NitroTPMPCR1 kms:RecipientAttestation:NitroTPMPCR2 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR3 kms:RecipientAttestation:NitroTPMPCR4 kms:RecipientAttestation:NitroTPMPCR5 kms:RecipientAttestation:NitroTPMPCR6 kms:RecipientAttestation:NitroTPMPCR7 kms:RecipientAttestation:NitroTPMPCR8	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR9 kms:RecipientAttestation:NitroTPMPCR10 kms:RecipientAttestation:NitroTPMPCR11 kms:RecipientAttestation:NitroTPMPCR12 kms:RecipientAttestation:NitroTPMPCR13 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR14 kms:RecipientAttestation:NitroTPMPCR15 kms:RecipientAttestation:NitroTPMPCR16 kms:RecipientAttestation:NitroTPMPCR17 kms:RecipientAttestation:NitroTPMPCR18 kms:RecipientAttestation:NitroTPMPCR19	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR20 kms:RecipientAttestation:NitroTPMPCR21 kms:RecipientAttestation:NitroTPMPCR22 kms:RecipientAttestation:NitroTPMPCR23 kms:RecipientAttestation:PCR0 kms:RecipientAttestation:PCR1	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR2 kms:RecipientAttestation:PCR3 kms:RecipientAttestation:PCR4 kms:RecipientAttestation:PCR5 kms:RecipientAttestation:PCR6 kms:RecipientAttestation:PCR7 kms:RecipientAttestation:PCR8	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR9 kms:RecipientAttestation:PCR10 kms:RecipientAttestation:PCR11 kms:RecipientAttestation:PCR12 kms:RecipientAttestation:PCR13 kms:RecipientAttestation:PCR14 kms:RecipientAttestation:PCR15	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR16 kms:RecipientAttestation:PCR17 kms:RecipientAttestation:PCR18 kms:RecipientAttestation:PCR19 kms:RecipientAttestation:PCR20 kms:RecipientAttestation:PCR21 kms:RecipientAttestation:PCR22	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR23 kms:RecipientAttestation:PCR24 kms:RecipientAttestation:PCR25 kms:RecipientAttestation:PCR26 kms:RecipientAttestation:PCR27 kms:RecipientAttestation:PCR28 kms:RecipientAttestation:PCR29	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR30 kms:RecipientAttestation:PCR31 kms:RequestAlias kms:ViaService	
DescribeCustomKeyStores	Controls permission to view detailed information about custom key stores in the account and region	Read		kms:CallerAccount	
DescribeKey	Controls permission to view detailed information about an AWS KMS key	Read	key*	kms:CallerAccount kms:RequestAlias kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableKey	Controls permission to disable an AWS KMS key, which prevents it from being used in cryptographic operations	Write	key*		
				kms:CallerAccount kms:ViaService	
DisableKeyRotation	Controls permission to disable automatic rotation of a customer managed AWS KMS key	Write	key*		
				kms:CallerAccount kms:ViaService	
DisconnectCustomKeyStore	Controls permission to disconnect the custom key store from its associated AWS CloudHSM cluster or external key manager outside of AWS	Write		kms:CallerAccount	
EnableKey	Controls permission to change the state of an AWS KMS key to enabled. This allows the KMS key to be used in cryptographic operations	Write	key*		
				kms:CallerAccount kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableKeyRotation	Controls permission to enable automatic rotation of the cryptographic material in an AWS KMS key	Write	key*		
				kms:CallerAccount kms:RotationPeriodInDays kms:ViaService	
Encrypt	Controls permission to use the specified AWS KMS key to encrypt data and data keys	Write	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RequestAlias kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateDataKey	Controls permission to use the AWS KMS key to generate data keys. You can use the data keys to encrypt data outside of AWS KMS	Write	key*		
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RecipientAttestation:ImageSha384 kms:RecipientAttestation:NitroTPMPCR0 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR1 kms:RecipientAttestation:NitroTPMPCR2 kms:RecipientAttestation:NitroTPMPCR3 kms:RecipientAttestation:NitroTPMPCR4 kms:RecipientAttestation:NitroTPMPCR5 kms:RecipientAttestation:NitroTPMPCR6	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR7 kms:RecipientAttestation:NitroTPMPCR8 kms:RecipientAttestation:NitroTPMPCR9 kms:RecipientAttestation:NitroTPMPCR10 kms:RecipientAttestation:NitroTPMPCR11 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR12 kms:RecipientAttestation:NitroTPMPCR13 kms:RecipientAttestation:NitroTPMPCR14 kms:RecipientAttestation:NitroTPMPCR15 kms:RecipientAttestation:NitroTPMPCR16 kms:RecipientAttestation:NitroTPMPCR17	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR18 kms:RecipientAttestation:NitroTPMPCR19 kms:RecipientAttestation:NitroTPMPCR20 kms:RecipientAttestation:NitroTPMPCR21 kms:RecipientAttestation:NitroTPMPCR22 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR23 kms:RecipientAttestation:PCR0 kms:RecipientAttestation:PCR1 kms:RecipientAttestation:PCR2 kms:RecipientAttestation:PCR3 kms:RecipientAttestation:PCR4 kms:RecipientAttestation:PCR5	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR6 kms:RecipientAttestation:PCR7 kms:RecipientAttestation:PCR8 kms:RecipientAttestation:PCR9 kms:RecipientAttestation:PCR10 kms:RecipientAttestation:PCR11 kms:RecipientAttestation:PCR12	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR13 kms:RecipientAttestation:PCR14 kms:RecipientAttestation:PCR15 kms:RecipientAttestation:PCR16 kms:RecipientAttestation:PCR17 kms:RecipientAttestation:PCR18 kms:RecipientAttestation:PCR19	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR20 kms:RecipientAttestation:PCR21 kms:RecipientAttestation:PCR22 kms:RecipientAttestation:PCR23 kms:RecipientAttestation:PCR24 kms:RecipientAttestation:PCR25 kms:RecipientAttestation:PCR26	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR27 kms:RecipientAttestation:PCR28 kms:RecipientAttestation:PCR29 kms:RecipientAttestation:PCR30 kms:RecipientAttestation:PCR31 kms:RequestAlias kms:ViaService	
GenerateDataKeyPair	Controls permission to use the AWS KMS key to generate data key pairs	Write	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:CallerAccount kms:DataKeyPairSpec kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RecipientAttestation:ImageSha384 kms:RecipientAttestation:NitroTPMPCR0 kms:RecipientAttes	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tation:NitroTPMPCR1 kms:RecipientAttestation:NitroTPMPCR2 kms:RecipientAttestation:NitroTPMPCR3 kms:RecipientAttestation:NitroTPMPCR4 kms:RecipientAttestation:NitroTPMPCR5 kms:RecipientAttestation:NitroTPMPCR6	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR7 kms:RecipientAttestation:NitroTPMPCR8 kms:RecipientAttestation:NitroTPMPCR9 kms:RecipientAttestation:NitroTPMPCR10 kms:RecipientAttestation:NitroTPMPCR11 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR12 kms:RecipientAttestation:NitroTPMPCR13 kms:RecipientAttestation:NitroTPMPCR14 kms:RecipientAttestation:NitroTPMPCR15 kms:RecipientAttestation:NitroTPMPCR16 kms:RecipientAttestation:NitroTPMPCR17	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR18 kms:RecipientAttestation:NitroTPMPCR19 kms:RecipientAttestation:NitroTPMPCR20 kms:RecipientAttestation:NitroTPMPCR21 kms:RecipientAttestation:NitroTPMPCR22 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR23 kms:RecipientAttestation:PCR0 kms:RecipientAttestation:PCR1 kms:RecipientAttestation:PCR2 kms:RecipientAttestation:PCR3 kms:RecipientAttestation:PCR4 kms:RecipientAttestation:PCR5	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR6 kms:RecipientAttestation:PCR7 kms:RecipientAttestation:PCR8 kms:RecipientAttestation:PCR9 kms:RecipientAttestation:PCR10 kms:RecipientAttestation:PCR11 kms:RecipientAttestation:PCR12	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR13 kms:RecipientAttestation:PCR14 kms:RecipientAttestation:PCR15 kms:RecipientAttestation:PCR16 kms:RecipientAttestation:PCR17 kms:RecipientAttestation:PCR18 kms:RecipientAttestation:PCR19	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR20 kms:RecipientAttestation:PCR21 kms:RecipientAttestation:PCR22 kms:RecipientAttestation:PCR23 kms:RecipientAttestation:PCR24 kms:RecipientAttestation:PCR25 kms:RecipientAttestation:PCR26	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR27 kms:RecipientAttestation:PCR28 kms:RecipientAttestation:PCR29 kms:RecipientAttestation:PCR30 kms:RecipientAttestation:PCR31 kms:RequestAlias kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateDataKeyPairWithoutPlaintext	Controls permission to use the AWS KMS key to generate data key pairs. Unlike the GenerateDataKeyPair operation, this operation returns an encrypted private key without a plaintext copy	Write	key*	kms:CallerAccount kms:DataKeyPairSpec kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RequestAlias kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateDataKeyWithoutPlaintext	Controls permission to use the AWS KMS key to generate a data key. Unlike the GenerateDataKey operation, this operation returns an encrypted data key without a plaintext version of the data key	Write	key*		
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RequestAlias kms:ViaService	
GenerateMac	Controls permission to use the AWS KMS key to generate message authentication codes	Write	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:CallerAccount kms:MacAlgorithm kms:RequestAlias kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateRandom	Controls permission to get a cryptographically secure random byte string from AWS KMS	Write		kms:RecipientAttestation:ImageSha384 kms:RecipientAttestation:NitroTPMPCR0 kms:RecipientAttestation:NitroTPMPCR1 kms:RecipientAttestation:NitroTPMPCR2 kms:RecipientAttestation:NitroTPMPCR3 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR4 kms:RecipientAttestation:NitroTPMPCR5 kms:RecipientAttestation:NitroTPMPCR6 kms:RecipientAttestation:NitroTPMPCR7 kms:RecipientAttestation:NitroTPMPCR8 kms:RecipientAttestation:NitroTPMPCR9	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR10 kms:RecipientAttestation:NitroTPMPCR11 kms:RecipientAttestation:NitroTPMPCR12 kms:RecipientAttestation:NitroTPMPCR13 kms:RecipientAttestation:NitroTPMPCR14 kms:RecipientAttestation:Ni	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				troTPMPCR15 kms:RecipientAttestation:NitroTPMPCR16 kms:RecipientAttestation:NitroTPMPCR17 kms:RecipientAttestation:NitroTPMPCR18 kms:RecipientAttestation:NitroTPMPCR19 kms:RecipientAttestation:NitroTPMPCR20	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:NitroTPMPCR21 kms:RecipientAttestation:NitroTPMPCR22 kms:RecipientAttestation:NitroTPMPCR23 kms:RecipientAttestation:PCR0 kms:RecipientAttestation:PCR1 kms:RecipientAttestation:PCR2	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR3 kms:RecipientAttestation:PCR4 kms:RecipientAttestation:PCR5 kms:RecipientAttestation:PCR6 kms:RecipientAttestation:PCR7 kms:RecipientAttestation:PCR8 kms:RecipientAttestation:PCR9	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR10 kms:RecipientAttestation:PCR11 kms:RecipientAttestation:PCR12 kms:RecipientAttestation:PCR13 kms:RecipientAttestation:PCR14 kms:RecipientAttestation:PCR15 kms:RecipientAttestation:PCR16	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR17 kms:RecipientAttestation:PCR18 kms:RecipientAttestation:PCR19 kms:RecipientAttestation:PCR20 kms:RecipientAttestation:PCR21 kms:RecipientAttestation:PCR22 kms:RecipientAttestation:PCR23	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR24 kms:RecipientAttestation:PCR25 kms:RecipientAttestation:PCR26 kms:RecipientAttestation:PCR27 kms:RecipientAttestation:PCR28 kms:RecipientAttestation:PCR29 kms:RecipientAttestation:PCR30	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR31	
GetKeyPolicy	Controls permission to view the key policy for the specified AWS KMS key	Read	key*		
				kms:CallerAccount kms:ViaService	
GetKeyRotationStatus	Controls permission to view the key rotation status for an AWS KMS key	Read	key*		
				kms:CallerAccount kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetParametersForImport	Controls permission to get data that is required to import cryptographic material into a customer managed key, including a public key and import token	Read	key*		
				kms:CallerAccount kms:ViaService kms:WrappingAlgorithm kms:WrappingKeySpec	
GetPublicKey	Controls permission to download the public key of an asymmetric AWS KMS key	Read	key*		
				kms:CallerAccount kms:RequestAlias kms:ViaService	
ImportKeyMaterial	Controls permission to import cryptographic material into an AWS KMS key	Write	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:CallerAccount kms:ExpirationModel kms:ValidTo kms:ViaService	
ListAliases	Controls permission to view the aliases that are defined in the account. Aliases are optional friendly names that you can associate with AWS KMS keys	List			
ListGrants	Controls permission to view all grants for an AWS KMS key	List	key*		
				kms:CallerAccount kms:GrantIsForAWSResource kms:ViaService	
ListKeyPolicies		List	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Controls permission to view the names of key policies for an AWS KMS key			kms:CallerAccount kms:ViaService	
ListKeyRotations	Controls permission to view the list of key materials for an AWS KMS key	List	key*		
				kms:CallerAccount kms:ViaService	
ListKeys	Controls permission to view the key ID and Amazon Resource Name (ARN) of all AWS KMS keys in the account	List			
ListResourceTags	Controls permission to view all tags that are attached to an AWS KMS key	List	key*		
				kms:CallerAccount kms:ViaService	
ListRetirableGrants	Controls permission to view grants in which the specified principal is the retiring principal. Other principals might be able to retire the grant and this principal might be able to retire other grants	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutKeyPolicy	Controls permission to replace the key policy for the specified AWS KMS key	Permissions management	key*		
				kms:BypassPolicyLockoutSafetyCheck kms:CallerAccount kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReEncryptFrom	Controls permission to decrypt data as part of the process that decrypts and reencrypts the data within AWS KMS	Write	key*		
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:ReEncryptOnSameKey kms:RequestAlias kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReEncryptTo	Controls permission to encrypt data as part of the process that decrypts and reencrypts the data within AWS KMS	Write	key*		
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:ReEncryptOnSameKey kms:RequestAlias kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReplicateKey	Controls permission to replicate a multi-Region primary key	Write	key*		iam:CreateServiceLinkedRole kms:CreateKey kms:PutKeyPolicy kms:TagResource
				kms:CallerAccount kms:ReplicaRegion kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RetireGrant	Controls permission to retire a grant. The RetireGrant operation is typically called by the grant user after they complete the tasks that the grant allowed them to perform	Permissions management	key*		
				kms:CallerAccount kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:GrantConstraintType kms:ViaService	
RevokeGrant	Controls permission to revoke a grant, which denies permission for all operations that depend on the grant	Permissions management	key*		
				kms:CallerAccount kms:GrantIsForAWSResource kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RotateKeyOnDemand	Controls permission to invoke on-demand rotation of the cryptographic material in an AWS KMS key	Write	key*		
				kms:CallerAccount kms:ViaService	
ScheduleKeyDeletion	Controls permission to schedule deletion of an AWS KMS key	Write	key*		
				kms:CallerAccount kms:ScheduleKeyDeletionPendingWindowInDays kms:ViaService	
Sign	Controls permission to produce a digital signature for a message	Write	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:CallerAccount kms:MessageType kms:RequestAlias kms:SigningAlgorithm kms:ViaService	
SynchronizeMultiRegionKey [permission only]	Controls access to internal APIs that synchronize multi-Region keys	Write	key*		
TagResource	Controls permission to create or update tags that are attached to an AWS KMS key	Tagging	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys kms:CallerAccount kms:ViaService	
UntagResource	Controls permission to delete tags that are attached to an AWS KMS key	Tagging	key*		
				aws:TagKeys kms:CallerAccount kms:ViaService	
UpdateAlias	Controls permission to associate an alias with a different AWS KMS key. An alias is an optional friendly name that you can associate with a KMS key	Write	alias*		
			key*		
				kms:CallerAccount kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCustomKeyStore	Controls permission to change the properties of a custom key store	Write		kms:CallerAccount	ec2:DescribeVpcEndpointServices
UpdateKeyDescription	Controls permission to delete or change the description of an AWS KMS key	Write	key*		
				kms:CallerAccount kms:ViaService	
UpdatePrimaryRegion	Controls permission to update the primary Region of a multi-Region primary key	Write	key*		
				kms:CallerAccount kms:PrimaryRegion kms:ViaService	
Verify	Controls permission to use the specified AWS KMS key to verify digital signatures	Write	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:CallerAccount kms:MessageType kms:RequestAlias kms:SigningAlgorithm kms:ViaService	
VerifyMac	Controls permission to use the AWS KMS key to verify message authentication codes	Write	key*		
				kms:CallerAccount kms:MacAlgorithm kms:RequestAlias kms:ViaService	

Resource types defined by AWS Key Management Service

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types

that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
alias	`arn:${Partition}:kms:${Region}:${Account}:alias/${Alias}`	
key	`arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}`	aws:ResourceTag/${TagKey} kms:KeyOrigin kms:KeySpec kms:KeyUsage kms:MultiRegion kms:MultiRegionKeyType kms:ResourceAliases

Condition keys for AWS Key Management Service

AWS Key Management Service defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access to the specified AWS KMS operations based on both the key and value of the tag in the request	String
aws:ResourceTag/${TagKey}	Filters access to the specified AWS KMS operations based on tags assigned to the AWS KMS key	String
aws:TagKeys	Filters access to the specified AWS KMS operations based on tag keys in the request	ArrayOfString
kms:BypassPolicyLockoutSafetyCheck	Filters access to the CreateKey and PutKeyPolicy operations based on the value of the BypassPolicyLockoutSafetyCheck parameter in the request	Bool
kms:CallerAccount	Filters access to specified AWS KMS operations based on the AWS account ID of the caller. You can use this condition key to allow or deny access to all IAM users and roles in an AWS account in a single policy statement	String
kms:CustomerMasterKeySpec	The kms:CustomerMasterKeySpec condition key is deprecated. Instead, use the kms:KeySpec condition key	String
kms:CustomerMasterKeyUsage	The kms:CustomerMasterKeyUsage condition key is deprecated. Instead, use the kms:KeyUsage condition key	String
kms:DataKeyPairSpec	Filters access to GenerateDataKeyPair and GenerateDataKeyPairWithoutPlaintext operations based on the value of the KeyPairSpec parameter in the request	String
kms:EncryptionAlgorithm	Filters access to encryption operations based on the value of the encryption algorithm in the request	String

Condition keys	Description	Type
kms:EncryptionContext:${EncryptionContextKey}	Filters access to a symmetric AWS KMS key based on the encryption context in a cryptographic operation. This condition evaluates the key and value in each key-value encryption context pair	String
kms:EncryptionContextKeys	Filters access to a symmetric AWS KMS key based on the encryption context in a cryptographic operation. This condition key evaluates only the key in each key-value encryption context pair	ArrayOfString
kms:ExpirationModel	Filters access to the ImportKeyMaterial operation based on the value of the ExpirationModel parameter in the request	String
kms:GrantConstraintType	Filters access to the CreateGrant operation based on the grant constraint in the request	String
kms:GrantIsForAWSResource	Filters access to the CreateGrant operation when the request comes from a specified AWS service	Bool
kms:GrantOperations	Filters access to the CreateGrant operation based on the operations in the grant	ArrayOfString
kms:GranteePrincipal	Filters access to the CreateGrant operation based on the grantee principal in the grant	String
kms:KeyAgreementAlgorithm	Filters access to the DeriveSharedSecret operation based on the value of the KeyAgreementAlgorithm parameter in the request	String
kms:KeyOrigin	Filters access to an API operation based on the Origin property of the AWS KMS key created by or used in the operation. Use it to qualify authorization of the CreateKey operation or any operation that is authorized for a KMS key	String

Condition keys	Description	Type
kms:KeySpec	Filters access to an API operation based on the KeySpec property of the AWS KMS key that is created by or used in the operation. Use it to qualify authorization of the CreateKey operation or any operation that is authorized for a KMS key resource	String
kms:KeyUsage	Filters access to an API operation based on the KeyUsage property of the AWS KMS key created by or used in the operation. Use it to qualify authorization of the CreateKey operation or any operation that is authorized for a KMS key resource	String
kms:MacAlgorithm	Filters access to the GenerateMac and VerifyMac operations based on the MacAlgorithm parameter in the request	String
kms:MessageType	Filters access to the Sign and Verify operations based on the value of the MessageType parameter in the request	String
kms:MultiRegion	Filters access to an API operation based on the MultiRegion property of the AWS KMS key created by or used in the operation. Use it to qualify authorization of the CreateKey operation or any operation that is authorized for a KMS key resource	Bool
kms:MultiRegionKeyType	Filters access to an API operation based on the MultiRegionKeyType property of the AWS KMS key created by or used in the operation. Use it to qualify authorization of the CreateKey operation or any operation that is authorized for a KMS key resource	String
kms:PrimaryRegion	Filters access to the UpdatePrimaryRegion operation based on the value of the PrimaryRegion parameter in the request	String

Condition keys	Description	Type
kms:ReEncryptOnSameKey	Filters access to the ReEncrypt operation when it uses the same AWS KMS key that was used for the Encrypt operation	Bool
kms:RecipientAttestation:ImageSha384	Filters access to the API operations based on the image hash in the attestation document in the request	String
kms:RecipientAttestation:NitroTPMPCR0	Filters access by the platform configuration register (PCR) 0 in the attestation document in the request. PCR0 is a contiguous measure of core system firmware executable code	String
kms:RecipientAttestation:NitroTPMPCR1	Filters access by the platform configuration register (PCR) 1 in the attestation document in the request. PCR1 is a contiguous measure of core system firmware data/ host platform configuration, typically including serial and model numbers	String
kms:RecipientAttestation:NitroTPMPCR10	Filters access by the platform configuration register (PCR) 10 in the attestation document in the request. PCR10 is a contiguous measure of protection of the IMA measurement log	String
kms:RecipientAttestation:NitroTPMPCR11	Filters access by the platform configuration register (PCR) 11 in the attestation document in the request. PCR11 is a contiguous measure of all components of unified kernel images (UKIs)	String
kms:RecipientAttestation:NitroTPMPCR12	Filters access by the platform configuration register (PCR) 12 in the attestation document in the request. PCR12 is a contiguous measure of kernel command line, system credentials and system configuration images	String

Condition keys	Description	Type
kms:RecipientAttestation:NitroTPMPCR13	Filters access by the platform configuration register (PCR) 13 in the attestation document in the request. PCR13 is a contiguous measure of all system extension images for the initrd	String
kms:RecipientAttestation:NitroTPMPCR14	Filters access by the platform configuration register (PCR) 14 in the attestation document in the request. PCR14 is a contiguous measure of "MOK" certificates and hashes	String
kms:RecipientAttestation:NitroTPMPCR15	Filters access by the platform configuration register (PCR) 15 in the attestation document in the request. PCR15 is a contiguous measure of root file system volume encryption key	String
kms:RecipientAttestation:NitroTPMPCR16	Filters access by the platform configuration register (PCR) 16 in the attestation document in the request. PCR16 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:NitroTPMPCR17	Filters access by the platform configuration register (PCR) 17 in the attestation document in the request. PCR17 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:NitroTPMPCR18	Filters access by the platform configuration register (PCR) 18 in the attestation document in the request. PCR18 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:NitroTPMPCR19	Filters access by the platform configuration register (PCR) 19 in the attestation document in the request. PCR19 is a custom PCR that can be defined by the user for specific use cases	String

Condition keys	Description	Type
kms:RecipientAttestation:NitroTPMPCR2	Filters access by the platform configuration register (PCR) 2 in the attestation document in the request. PCR2 is a contiguous measure of extended or pluggable executable code, including option ROMs on pluggable hardware	String
kms:RecipientAttestation:NitroTPMPCR20	Filters access by the platform configuration register (PCR) 20 in the attestation document in the request. PCR20 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:NitroTPMPCR21	Filters access by the platform configuration register (PCR) 21 in the attestation document in the request. PCR21 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:NitroTPMPCR22	Filters access by the platform configuration register (PCR) 22 in the attestation document in the request. PCR22 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:NitroTPMPCR23	Filters access by the platform configuration register (PCR) 23 in the attestation document in the request. PCR23 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:NitroTPMPCR3	Filters access by the platform configuration register (PCR) 3 in the attestation document in the request. PCR3 is a contiguous measure of extended or pluggable firmware data, including information about pluggable hardware	String

Condition keys	Description	Type
kms:RecipientAttestation:NitroTPMPCR4	Filters access by the platform configuration register (PCR) 4 in the attestation document in the request. PCR4 is a contiguous measure of boot loader and additional drivers, including binaries and extensions loaded by the boot loader	String
kms:RecipientAttestation:NitroTPMPCR5	Filters access by the platform configuration register (PCR) 5 in the attestation document in the request. PCR5 is a contiguous measure of GPT/Partition table	String
kms:RecipientAttestation:NitroTPMPCR6	Filters access by the platform configuration register (PCR) 6 in the attestation document in the request. PCR6 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:NitroTPMPCR7	Filters access by the platform configuration register (PCR) 7 in the attestation document in the request. PCR7 is a contiguous measure of SecureBoot state	String
kms:RecipientAttestation:NitroTPMPCR8	Filters access by the platform configuration register (PCR) 8 in the attestation document in the request. PCR8 is a contiguous measure of commands and kernel command line	String
kms:RecipientAttestation:NitroTPMPCR9	Filters access by the platform configuration register (PCR) 9 in the attestation document in the request. PCR9 is a contiguous measure of all files read (including kernel image)	String
kms:RecipientAttestation:PCR0	Filters access by the platform configuration register (PCR) 0 in the attestation document in the request. PCR0 is a contiguous measure of the contents of the enclave image file, without the section data	String

Condition keys	Description	Type
kms:RecipientAttestation:PCR1	Filters access by the platform configuration register (PCR) 1 in the attestation document in the request. PCR1 is a contiguous measurement of the Linux kernel and bootstrap data	String
kms:RecipientAttestation:PCR10	Filters access by the platform configuration register (PCR) 10 in the attestation document in the request. PCR10 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR11	Filters access by the platform configuration register (PCR) 11 in the attestation document in the request. PCR11 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR12	Filters access by the platform configuration register (PCR) 12 in the attestation document in the request. PCR12 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR13	Filters access by the platform configuration register (PCR) 13 in the attestation document in the request. PCR13 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR14	Filters access by the platform configuration register (PCR) 14 in the attestation document in the request. PCR14 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR15	Filters access by the platform configuration register (PCR) 15 in the attestation document in the request. PCR15 is a custom PCR that can be defined by the user for specific use cases	String

Condition keys	Description	Type
kms:RecipientAttestation:PCR16	Filters access by the platform configuration register (PCR) 16 in the attestation document in the request. PCR16 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR17	Filters access by the platform configuration register (PCR) 17 in the attestation document in the request. PCR17 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR18	Filters access by the platform configuration register (PCR) 18 in the attestation document in the request. PCR18 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR19	Filters access by the platform configuration register (PCR) 19 in the attestation document in the request. PCR19 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR2	Filters access by the platform configuration register (PCR) 2 in the attestation document in the request. PCR2 is a contiguous, in-order measurement of the user applications, without the boot ramfs	String
kms:RecipientAttestation:PCR20	Filters access by the platform configuration register (PCR) 20 in the attestation document in the request. PCR20 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR21	Filters access by the platform configuration register (PCR) 21 in the attestation document in the request. PCR21 is a custom PCR that can be defined by the user for specific use cases	String

Condition keys	Description	Type
kms:RecipientAttestation:PCR22	Filters access by the platform configuration register (PCR) 22 in the attestation document in the request. PCR22 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR23	Filters access by the platform configuration register (PCR) 23 in the attestation document in the request. PCR23 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR24	Filters access by the platform configuration register (PCR) 24 in the attestation document in the request. PCR24 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR25	Filters access by the platform configuration register (PCR) 25 in the attestation document in the request. PCR25 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR26	Filters access by the platform configuration register (PCR) 26 in the attestation document in the request. PCR26 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR27	Filters access by the platform configuration register (PCR) 27 in the attestation document in the request. PCR27 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR28	Filters access by the platform configuration register (PCR) 28 in the attestation document in the request. PCR28 is a custom PCR that can be defined by the user for specific use cases	String

Condition keys	Description	Type
kms:RecipientAttestation:PCR29	Filters access by the platform configuration register (PCR) 29 in the attestation document in the request. PCR29 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR3	Filters access by the platform configuration register (PCR) 3 in the attestation document in the request. PCR3 is a contiguous measurement of the IAM role assigned to the parent instance	String
kms:RecipientAttestation:PCR30	Filters access by the platform configuration register (PCR) 30 in the attestation document in the request. PCR30 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR31	Filters access by the platform configuration register (PCR) 31 in the attestation document in the request. PCR31 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR4	Filters access by the platform configuration register (PCR) 4 in the attestation document in the request. PCR4 is a contiguous measurement of the ID of the parent instance	String
kms:RecipientAttestation:PCR5	Filters access by the platform configuration register (PCR) 5 in the attestation document in the request. PCR5 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR6	Filters access by the platform configuration register (PCR) 6 in the attestation document in the request. PCR6 is a custom PCR that can be defined by the user for specific use cases	String

Condition keys	Description	Type
kms:RecipientAttestation:PCR7	Filters access by the platform configuration register (PCR) 7 in the attestation document in the request. PCR7 is a custom PCR that can be defined by the user for specific use cases	String
kms:RecipientAttestation:PCR8	Filters access by the platform configuration register (PCR) 8 in the attestation document in the request. PCR8 is a measure of the signing certificate specified for the enclave image file	String
kms:RecipientAttestation:PCR9	Filters access by the platform configuration register (PCR) 9 in the attestation document in the request. PCR9 is a custom PCR that can be defined by the user for specific use cases	String
kms:ReplicaRegion	Filters access to the ReplicateKey operation based on the value of the ReplicaRegion parameter in the request	String
kms:RequestAlias	Filters access to cryptographic operations, DescribeKey, and GetPublicKey based on the alias in the request	String
kms:ResourceAliases	Filters access to specified AWS KMS operations based on aliases associated with the AWS KMS key	ArrayOfString
kms:RetiringPrincipal	Filters access to the CreateGrant operation based on the retiring principal in the grant	String
kms:RotationPeriodInDays	Filters access to the EnableKeyRotation operation based on the value of the RotationPeriodInDays parameter in the request	Numeric
kms:ScheduleKeyDeletionPendingWindowInDays	Filters access to the ScheduleKeyDeletion operation based on the value of the PendingWindowInDays parameter in the request	Numeric

Condition keys	Description	Type
kms:SigningAlgorithm	Filters access to the Sign and Verify operations based on the signing algorithm in the request	String
kms:ValidTo	Filters access to the ImportKeyMaterial operation based on the value of the ValidTo parameter in the request. You can use this condition key to allow users to import key material only when it expires by the specified date	Date
kms:ViaService	Filters access when a request made on the principal's behalf comes from a specified AWS service	String
kms:WrappingAlgorithm	Filters access to the GetParametersForImport operation based on the value of the WrappingAlgorithm parameter in the request	String
kms:WrappingKeySpec	Filters access to the GetParametersForImport operation based on the value of the WrappingKeySpec parameter in the request	String

Actions, resources, and condition keys for Amazon Kinesis Data Streams

Amazon Kinesis Data Streams (service prefix: `kinesis`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Kinesis Data Streams
- Resource types defined by Amazon Kinesis Data Streams
- Condition keys for Amazon Kinesis Data Streams

Actions defined by Amazon Kinesis Data Streams

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddTagsToStream	Grants permission to add or update tags for the specified Amazon Kinesis stream. Each stream can have up to 50 tags	Tagging	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateStream	Grants permission to create a Amazon Kinesis stream	Write	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DecreaseStreamRetentionPeriod	Grants permission to decrease the stream's retention period, which is the length of time data records are accessible after they are added to the stream	Write	stream*	aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Grants permission to delete a resource policy associated with a specified stream or consumer	Write	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	
DeleteStream	Grants permission to delete a stream and all its shards and data	Write	stream*	aws:ResourceTag/${TagKey}	
DeregisterStreamConsumer	Grants permission to deregister a stream consumer with a Kinesis data stream	Write	consumer*	aws:ResourceTag/${TagKey}	
DescribeAccountSettings	Grants permission to describe the account-level settings for Amazon Kinesis Data Streams	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLimits	Grants permission to describe the shard limits and usage for the account	Read			
DescribeStream	Grants permission to describe the specified stream	Read	stream*	aws:ResourceTag/${TagKey}	
DescribeStreamConsumer	Grants permission to get the description of a registered stream consumer	Read	consumer*	aws:ResourceTag/${TagKey}	
DescribeStreamSummary	Grants permission to provide a summarized description of the specified Kinesis data stream without the shard list	Read	stream*	aws:ResourceTag/${TagKey}	
DisableEnhancedMonitoring	Grants permission to disables enhanced monitoring	Write			
EnableEnhancedMonitoring	Grants permission to enable enhanced Kinesis data stream monitoring for shard-level metrics	Write			
GetRecords	Grants permission to get data records from a shard	Read	stream*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResourcePolicy	Grants permission to get a resource policy associated with a specified stream or consumer	Read	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	
GetShardIterator	Grants permission to get a shard iterator. A shard iterator expires five minutes after it is returned to the requester	Read	stream*	aws:ResourceTag/${TagKey}	
IncreaseStreamRetentionPeriod	Grants permission to increase the stream's retention period, which is the length of time data records are accessible after they are added to the stream	Write	stream*	aws:ResourceTag/${TagKey}	
InjectApiError [permission only]	Grants permission to temporarily inject errors for target API requests	Write		kinesis:FisActionId kinesis:FisTargetArns kinesis:FisInjectPercentage	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListShards	Grants permission to list the shards in a stream and provides information about each shard	List	stream*	aws:ResourceTag/${TagKey}	
ListStreamConsumers	Grants permission to list the stream consumers registered to receive data from a Kinesis stream using enhanced fan-out, and provides information about each consumer	List	stream*	aws:ResourceTag/${TagKey}	
ListStreams	Grants permission to list your streams	List			
ListTagsForResource	Grants permission to list the tags for the specified Amazon Kinesis resource	Read	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	
ListTagsForStream	Grants permission to list the tags for the specified Amazon Kinesis stream	Read	stream*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
MergeShards	Grants permission to merge two adjacent shards in a stream and combines them into a single shard to reduce the stream's capacity to ingest and transport data	Write	stream*	aws:ResourceTag/${TagKey}	
PutRecord	Grants permission to write a single data record from a producer into an Amazon Kinesis stream	Write	stream*	aws:ResourceTag/${TagKey}	
PutRecords	Grants permission to write multiple data records from a producer into an Amazon Kinesis stream in a single call (also referred to as a PutRecords request)	Write	stream*	aws:ResourceTag/${TagKey}	
PutResourcePolicy	Grants permission to attach a resource policy to a specified stream or consumer	Write	consumer*	aws:ResourceTag/${TagKey}	
			stream*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterStreamConsumer	Grants permission to register a stream consumer with a Kinesis data stream	Write	stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
RemoveTagsFromStream	Grants permission to remove tags from the specified Kinesis data stream. Removed tags are deleted and cannot be recovered after this operation successfully completes	Tagging	stream*	aws:TagKeys aws:ResourceTag/${TagKey}	
SplitShard	Grants permission to split a shard into two new shards in the Kinesis data stream, to increase the stream's capacity to ingest and transport data	Write	stream*	aws:ResourceTag/${TagKey}	
StartStreamEncryption	Grants permission to enable or update server-side encryption using an AWS KMS key for a specified stream	Write	kmsKey*		
			stream*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopStreamEncryption	Grants permission to disable server-side encryption for a specified stream	Write	kmsKey*		
			stream*	aws:ResourceTag/${TagKey}	
SubscribeToShard	Grants permission to listen to a specific shard with enhanced fan-out	Read	consumer*	aws:ResourceTag/${TagKey}	
TagResource	Grants permission to add or update tags for the specified Amazon Kinesis resource. Each resource can have up to 50 tags	Tagging	consumer*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			stream*	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to remove tags from the specified Kinesis data resource. Removed tags are deleted and cannot be recovered after this operation successfully completes	Tagging	consumer*	aws:TagKeys aws:ResourceTag/${TagKey}	
			stream*	aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAccountSettings	Grants permission to update the account-level settings for Amazon Kinesis Data Streams	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateMaxRecordSize	Grants permission to update the maximum record size for a Kinesis data stream	Write	stream*	aws:ResourceTag/${TagKey}	
UpdateShardCount	Grants permission to update the shard count of the specified stream to the specified number of shards	Write			
UpdateStreamMode	Grants permission to update the capacity mode of the data stream	Write			
UpdateStreamWarmThroughput	Grants permission to update the warm throughput for a Kinesis on-demand data stream	Write	stream*	aws:ResourceTag/${TagKey}	

Resource types defined by Amazon Kinesis Data Streams

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
stream	`arn:${Partition}:kinesis:${Region}:${Account}:stream/${StreamName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
consumer	arn:${Partition}:kinesis:${Region}:${Account}:${StreamType}/${StreamName}/consumer/${ConsumerName}:${ConsumerCreationTimpstamp}	aws:ResourceTag/${TagKey}
kmsKey	arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}	

Condition keys for Amazon Kinesis Data Streams

Amazon Kinesis Data Streams defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
kinesis:FisActionId	Filters access by the ID of an AWS FIS action	String
kinesis:FisInjectPercentage	Filters access by the percentage of calls being affected by an AWS FIS action	Numeric

Condition keys	Description	Type
kinesis:FisTargetArns	Filters access by the ARN of an AWS FIS target	ArrayOfARN

Actions, resources, and condition keys for Amazon Kinesis Firehose

Amazon Kinesis Firehose (service prefix: `firehose`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Kinesis Firehose
- Resource types defined by Amazon Kinesis Firehose
- Condition keys for Amazon Kinesis Firehose

Actions defined by Amazon Kinesis Firehose

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDeliveryStream	Grants permission to create a delivery stream	Write	deliverystream*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDeliveryStream	Grants permission to delete a delivery stream and its data	Write	deliverystream*		
DescribeDeliveryStream	Grants permission to describe the specified delivery stream and gets the status	Read	deliverystream*		
ListDeliveryStreams	Grants permission to list your delivery streams	List			
ListTagsForDeliveryStream	Grants permission to list the tags for the specified delivery stream	List	deliverystream*		
PutRecord	Grants permission to write a single data record into an Amazon Kinesis Firehose delivery stream	Write	deliverystream*		
PutRecordBatch	Grants permission to write multiple data records into a delivery stream in a single call, which can achieve higher throughput per producer than when writing single records	Write	deliverystream*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartDeliveryStreamEncryption	Grants permission to enable server-side encryption (SSE) for the delivery stream	Write	deliverystream*		
StopDeliveryStreamEncryption	Grants permission to disable the specified destination of the specified delivery stream	Write	deliverystream*		
TagDeliveryStream	Grants permission to add or update tags for the specified delivery stream	Tagging	deliverystream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagDeliveryStream	Grants permission to remove tags from the specified delivery stream	Tagging	deliverystream*		
				aws:TagKeys	
UpdateDestination	Grants permission to update the specified destination of the specified delivery stream	Write	deliverystream*		

Resource types defined by Amazon Kinesis Firehose

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types

that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
deliverystream	`arn:${Partition}:firehose:${Region}:${Account}:deliverystream/${DeliveryStreamName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Kinesis Firehose

Amazon Kinesis Firehose defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Lambda

AWS Lambda (service prefix: `lambda`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Lambda
- Resource types defined by AWS Lambda
- Condition keys for AWS Lambda

Actions defined by AWS Lambda

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddLayerVersionPermission	Grants permission to add permissions to the resource-based policy of a version of an AWS Lambda layer	Permissions management	layerVersion*		
AddPermission	Grants permission to give an AWS service or another account permission to use an AWS Lambda function	Permissions management	function*		
				lambda:Principal lambda:FunctionUrlAuthType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CheckpointDurableExecution	Grants permission to save the progress of an AWS Lambda durable execution	Write	durableexecution*		
CreateAlias	Grants permission to create an alias for a Lambda function version	Write	function*		
CreateCapacityProvider	Grants permission to create an AWS Lambda capacity provider	Write	capacityProvider*		iam:CreateServiceLinkedRole iam:PassRole kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys lambda:SecurityGroupIds lambda:SubnetIds	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCodeSigningConfig	Grants permission to create an AWS Lambda code signing config	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventSourceMapping	Grants permission to create a mapping between an event source and an AWS Lambda function	Write		lambda:FunctionArn aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunction	Grants permission to create an AWS Lambda function	Write	function*		iam:PassRole lambda:PassCapacityProvider

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				lambda:Layer lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds lambda:CodeSigningConfigArn aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunctionUrlConfig	Grants permission to create a function url configuration for a Lambda function	Write	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAlias	Grants permission to delete an AWS Lambda function alias	Write	function*		
DeleteCapacityProvider	Grants permission to delete an AWS Lambda capacity provider	Write	capacityProvider*		
DeleteCodeSigningConfig	Grants permission to delete an AWS Lambda code signing config	Write	codesigningconfig*		
DeleteEventSourceMapping	Grants permission to delete an AWS Lambda event source mapping	Write	eventSourceMapping*		
				lambda:FunctionArn	
DeleteFunction	Grants permission to delete an AWS Lambda function	Write	function*		
DeleteFunctionCodeSigningConfig	Grants permission to detach a code signing config from an AWS Lambda function	Write	function*		
DeleteFunctionConcurrency	Grants permission to remove a concurrent execution limit from an AWS Lambda function	Write	function*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFunctionEventInvokeConfig	Grants permission to delete the configuration for asynchronous invocation for an AWS Lambda function, version, or alias	Write	function*		
DeleteFunctionUrlConfig	Grants permission to delete function url configuration for a Lambda function	Write	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	
DeleteLayerVersion	Grants permission to delete a version of an AWS Lambda layer	Write	layerVersion*		
DeleteProvisionedConcurrencyConfig	Grants permission to delete the provisioned concurrency configuration for an AWS Lambda function	Write	function alias		
			function version		
DisableReplication [permission only]	Grants permission to disable replication for a Lambda@Edge function	Permissions management	function*		
EnableReplication [permission only]	Grants permission to enable replication for a Lambda@Edge function	Permissions management	function*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccountSettings	Grants permission to view details about an account's limits and usage in an AWS Region	Read			
GetAlias	Grants permission to view details about an AWS Lambda function alias	Read	function*		
GetCapacityProvider	Grants permission to view details about an AWS Lambda capacity provider	Read	capacityProvider*		
GetCodeSigningConfig	Grants permission to view details about an AWS Lambda code signing config	Read	code signing config*		
GetDurableExecution	Grants permission to view details of an AWS Lambda durable execution	Read	durable execution*		
GetDurableExecutionHistory	Grants permission to view execution history of an AWS Lambda durable execution	Read	durable execution*		
GetDurableExecutionState	Grants permission to view current state of an AWS Lambda durable execution	Read	durable execution*		
GetEventSourceMapping	Grants permission to view details about an AWS Lambda event source mapping	Read	eventSourceMapping*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				lambda:FunctionArn	
GetFunction	Grants permission to view details about an AWS Lambda function	Read	function*		
GetFunctionCodeSigningConfig	Grants permission to view the code signing config arn attached to an AWS Lambda function	Read	function*		
GetFunctionConcurrency	Grants permission to view details about the reserved concurrency configuration for a function	Read	function*		
GetFunctionConfiguration	Grants permission to view details about the version-specific settings of an AWS Lambda function or version	Read	function*		
GetFunctionEventInvokeConfig	Grants permission to view the configuration for asynchronous invocation for a function, version, or alias	Read	function*		
GetFunctionRecursionConfig	Grants permission to view the recursion configuration of an AWS Lambda function	Read	function*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFunctionScalingConfig	Grants permission to view the scaling configuration of an AWS Lambda function running on a capacity provider	Read	function*		
GetFunctionUrlConfig	Grants permission to read function url configuration for a Lambda function	Read	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	
GetLayerVersion	Grants permission to view details about a version of an AWS Lambda layer. Note this action also supports GetLayerVersionByArn API	Read	layerVersion*		
GetLayerVersionPolicy	Grants permission to view the resource-based policy for a version of an AWS Lambda layer	Read	layerVersion*		
GetPolicy	Grants permission to view the resource-based policy for an AWS Lambda function, version, or alias	Read	function*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetProvisionedConcurrencyConfig	Grants permission to view the provisioned concurrency configuration for an AWS Lambda function's alias or version	Read	function alias		
			function version		
GetRuntimeManagementConfig	Grants permission to view the runtime management configuration of an AWS Lambda function	Read	function*		
InvokeAsync	Grants permission to invoke a function asynchronously (Deprecated)	Write	function*		
InvokeFunction	Grants permission to invoke an AWS Lambda function	Write	function*		
				lambda:EventSourceToken lambda:InvokedViaFunctionUrl	
InvokeFunctionUrl [permission only]	Grants permission to invoke an AWS Lambda function through url	Write	function*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				lambda:FunctionUrlAuthType lambda:FunctionArn lambda:EventSourceToken	
ListAliases	Grants permission to retrieve a list of aliases for an AWS Lambda function	List	function*		
ListCapacityProviders	Grants permission to retrieve a list of AWS Lambda capacity providers	List			
ListCodeSigningConfigs	Grants permission to retrieve a list of AWS Lambda code signing configs	List			
ListDurableExecutionsByFunction	Grants permission to retrieve a list of AWS Lambda durable executions of an AWS Lambda function	List	function*		
ListEventSourceMappings	Grants permission to retrieve a list of AWS Lambda event source mappings	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListFunctionEventInvokeConfigs	Grants permission to retrieve a list of configurations for asynchronous invocation for a function	List	function*		
ListFunctionUrlConfigs	Grants permission to read function url configurations for a function	List	function*		
				lambda:FunctionUrlAuthType	
ListFunctionVersionsByCapacityProvider	Grants permission to retrieve a list of AWS Lambda function versions by the capacity provider assigned	List	capacityProvider*		
ListFunctions	Grants permission to retrieve a list of AWS Lambda functions, with the version-specific configuration of each function	List			
ListFunctionsByCodeSigningConfig	Grants permission to retrieve a list of AWS Lambda functions by the code signing config assigned	List	code signing config*		
ListLayerVersions	Grants permission to retrieve a list of versions of an AWS Lambda layer	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListLayers	Grants permission to retrieve a list of AWS Lambda layers, with details about the latest version of each layer	List			
ListProvisionedConcurrencyConfigs	Grants permission to retrieve a list of provisioned concurrency configurations for an AWS Lambda function	List	function*		
ListTags	Grants permission to retrieve a list of tags for an AWS Lambda function, event source mapping, capacity provider, or code signing configuration resource	Read	capacityProvider		
			codesigningconfig		
			eventSourceMapping		
			function		
ListVersionsByFunction	Grants permission to retrieve a list of versions for an AWS Lambda function	List	function*		
PassCapacityProvider [permission only]	Grants permission to pass an AWS Lambda capacity provider to a service	Write	capacityProvider*		
PublishLayerVersion	Grants permission to create an AWS Lambda layer	Write	layer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PublishVersion	Grants permission to create an AWS Lambda function version	Write	function*		
PutFunctionCodeSigningConfig	Grants permission to attach a code signing config to an AWS Lambda function	Write	code signing config*		
			function*		
				lambda:CodeSigningConfigArn	
PutFunctionConcurrency	Grants permission to configure reserved concurrency for an AWS Lambda function	Write	function*		
PutFunctionEventInvokeConfig	Grants permission to configures options for asynchronous invocation on an AWS Lambda function, version, or alias	Write	function*		
PutFunctionRecursionConfig	Grants permission to update the recursion configuration of an AWS Lambda function	Write	function*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutFunctionScalingConfig	Grants permission to update the scaling configuration of an AWS Lambda function running on a capacity provider	Write	function*		
PutProvisionedConcurrencyConfig	Grants permission to configure provisioned concurrency for an AWS Lambda function's alias or version	Write	function alias		
			function version		
PutRuntimeManagementConfig	Grants permission to update the runtime management configuration of an AWS Lambda function	Write	function*		
RemoveLayerVersionPermission	Grants permission to remove a statement from the permissions policy for a version of an AWS Lambda layer	Permissions management	layerVersion*		
RemovePermission	Grants permission to revoke function-use permission from an AWS service or another account	Permissions management	function*		
				lambda:Principal lambda:FunctionUrlAuthType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendDurableExecutionCallbackFailure	Grants permission to send a failure response for a callback operation in an AWS Lambda durable execution	Write	durable execution*		
SendDurableExecutionCallbackHeartbeat	Grants permission to send a heartbeat for a callback operation in an AWS Lambda durable execution	Write	durable execution*		
SendDurableExecutionCallbackSuccess	Grants permission to send a successful response for a callback operation in an AWS Lambda durable execution	Write	durable execution*		
StopDurableExecution	Grants permission to stop an AWS Lambda durable execution	Write	durable execution*		
TagResource	Grants permission to add tags to an AWS Lambda function, event source mapping, capacity provider, or code signing configuration resource	Tagging	capacityProvider		
			code signing config		
			eventSourceMapping		
			function		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from an AWS Lambda function, event source mapping, capacity provider, or code signing configuration resource	Tagging	capacityProvider		
			codesigningconfig		
			eventSourceMapping		
			function		
				aws:TagKeys	
UpdateAlias	Grants permission to update the configuration of an AWS Lambda function's alias	Write	function*		
UpdateCapacityProvider	Grants permission to update an AWS Lambda capacity provider	Write	capacityProvider*		
UpdateCodeSigningConfig	Grants permission to update an AWS Lambda code signing config	Write	codesigningconfig*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEventSourceMapping	Grants permission to update the configuration of an AWS Lambda event source mapping	Write	eventSourceMapping*		
				lambda:FunctionArn	
UpdateFunctionCode	Grants permission to update the code of an AWS Lambda function	Write	function*		
UpdateFunctionCodeSigningConfig	Grants permission to update the code signing config of an AWS Lambda function	Write	codesigningconfig*		
			function*		
UpdateFunctionConfiguration	Grants permission to modify the version-specific settings of an AWS Lambda function	Write	function*		
				lambda:Layer lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFunctionEventInvokeConfig	Grants permission to modify the configuration for asynchronous invocation for an AWS Lambda function, version, or alias	Write	function*		
UpdateFunctionUrlConfig	Grants permission to update a function url configuration for a Lambda function	Write	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	

Resource types defined by AWS Lambda

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
capacityProvider	`arn:${Partition}:lambda:${Region}:${Account}:capacity-provider:${CapacityProviderName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
code signing config	arn:${Partition}:lambda:${Region}:${Account}:code-signing-config:${CodeSigningConfigId}	aws:ResourceTag/${TagKey}
durable execution	arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Version}/durable-execution/${ExecutionName}/${ExecutionId}	
eventSourceMapping	arn:${Partition}:lambda:${Region}:${Account}:event-source-mapping:${UUID}	aws:ResourceTag/${TagKey}
function	arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}	aws:ResourceTag/${TagKey}
function alias	arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Alias}	aws:ResourceTag/${TagKey}
function version	arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}:${Version}	aws:ResourceTag/${TagKey}
layer	arn:${Partition}:lambda:${Region}:${Account}:layer:${LayerName}	
layerVersion	arn:${Partition}:lambda:${Region}:${Account}:layer:${LayerName}:${LayerVersion}	

Condition keys for AWS Lambda

AWS Lambda defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
lambda:CodeSigningConfigArn	Filters access by the ARN of an AWS Lambda code signing config	ARN
lambda:EventSourceToken	Filters access by the ID from a non-AWS event source configured for the AWS Lambda function	String
lambda:FunctionArn	Filters access by the ARN of an AWS Lambda function	ARN
lambda:FunctionUrlAuthType	Filters access by authorization type specified in request. Available during CreateFunctionUrlConfig, UpdateFunctionUrlConfig, DeleteFunctionUrlConfig, GetFunctionUrlConfig, ListFunctionUrlConfig, AddPermission and RemovePermission operations	String

Condition keys	Description	Type
lambda:InvokedViaFunctionUrl	Limits the scope of lambda:InvokeFunction action to Function URLs only. Available during AddPermission operation	Bool
lambda:Layer	Filters access by the ARN of a version of an AWS Lambda layer	ArrayOfString
lambda:Principal	Filters access by restricting the AWS service or account that can invoke a function	String
lambda:SecurityGroupIds	Filters access by the ID of security groups configured for the AWS Lambda function	ArrayOfString
lambda:SourceFunctionArn	Filters access by the ARN of the AWS Lambda function from which the request originated	ARN
lambda:SubnetIds	Filters access by the ID of subnets configured for the AWS Lambda function	ArrayOfString
lambda:VpcIds	Filters access by the ID of the VPC configured for the AWS Lambda function	String

Actions, resources, and condition keys for Amazon Managed Streaming for Apache Kafka

Amazon Managed Streaming for Apache Kafka (service prefix: `kafka`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Managed Streaming for Apache Kafka
- Resource types defined by Amazon Managed Streaming for Apache Kafka
- Condition keys for Amazon Managed Streaming for Apache Kafka

Actions defined by Amazon Managed Streaming for Apache Kafka

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchAssociateScramSecret	Grants permission to associate one or more Scram Secrets with an Amazon MSK cluster	Write	cluster*		kms:CreateGrant kms:RetireGrant
BatchDisassociateScramSecret	Grants permission to disassociate one or more Scram Secrets from an Amazon MSK cluster	Write	cluster*		kms:RetireGrant
CreateCluster	Grants permission to create an MSK cluster	Write	cluster*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateClusterV2	Grants permission to create an MSK cluster	Write	cluster*		ec2:CreateTags ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs iam:AttachRolePolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:CreateServiceLinkedRole iam:PutRolePolicy kms:CreateGrant kms:DescribeKey
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfiguration	Grants permission to create an MSK configuration	Write	configuration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateReplicator	Grants permission to create a MSK replicator	Write	replicator*		ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole iam:PassRole iam:PutRolePolicy kafka:DescribeClusterV2 kafka:GetBootstrapBrokers

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVpcConnection	Grants permission to create a MSK VPC connection	Write	cluster*		ec2:CreateTags ec2:CreateVpcEndpoint ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints ec2:DescribeVpcs iam:AttachRolePolicy iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:PutRolePolicy
			vpc-connection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCluster	Grants permission to delete an MSK cluster	Write	cluster*		ec2:DeleteVpcEndpoints ec2:DescribeVpcAttribute ec2:DescribeVpcEndpoints
DeleteClusterPolicy	Grants permission to delete a cluster resource-based policy	Write	cluster*		
DeleteConfiguration	Grants permission to delete the specified MSK configuration	Write	configuration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteReplicator	Grants permission to delete a MSK replicator	Write	replicator*		
DeleteVpcConnection	Grants permission to delete a MSK VPC connection	Write	vpc-connection*		ec2:DeleteVpcEndpoints ec2:DescribeVpcEndpoints
DescribeCluster	Grants permission to describe an MSK cluster	Read	cluster*		
DescribeClusterOperation	Grants permission to describe the cluster operation that is specified by the given ARN	Read			
DescribeClusterOperationV2	Grants permission to describe the cluster operation that is specified by the given ARN	Read			
DescribeClusterV2	Grants permission to describe an MSK cluster	Read	cluster*		
DescribeConfiguration	Grants permission to describe an MSK configuration	Read	configuration*		
DescribeConfigurationRevision	Grants permission to describe an MSK configuration revision	Read	configuration*		
DescribeReplicator	Grants permission to describe a MSK replicator	Read	replicator*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTopic	Grants permission to return metadata details about a specific Kafka topic	Read	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic kafka-cluster:DescribeTopicDynamicConfiguration
DescribeTopicPartitions	Grants permission to list all partitions of a specific topic	Read	topic*		kafka-cluster:Connect kafka-cluster:DescribeTopic kafka-cluster:DescribeTopicDynamicConfiguration
DescribeVpcConnection	Grants permission to describe a MSK VPC connection	Read	vpc-connection*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBootstrapBrokers	Grants permission to get connection details for the brokers in an MSK cluster	Read			
GetClusterPolicy	Grants permission to describe a cluster resource-based policy	Read	cluster*		
GetCompatibleKafkaVersions	Grants permission to get a list of the Apache Kafka versions to which you can update an MSK cluster	List			
ListClientVpcConnections	Grants permission to list all MSK VPC connections created for a cluster	List	cluster*		
ListClusterOperations	Grants permission to return a list of all the operations that have been performed on the specified MSK cluster	List	cluster*		
ListClusterOperationsV2	Grants permission to return a list of all the operations that have been performed on the specified MSK cluster	List	cluster*		
ListClusters	Grants permission to list all MSK clusters in this account	List			
ListClustersV2	Grants permission to list all MSK clusters in this account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListConfigurationRevisions	Grants permission to list all revisions for an MSK configuration in this account	List	configuration*		
ListConfigurations	Grants permission to list all MSK configurations in this account	List			
ListKafkaVersions	Grants permission to list all Apache Kafka versions supported by Amazon MSK	List			
ListNodes	Grants permission to list brokers in an MSK cluster	List	cluster*		
ListReplicators	Grants permission to list all MSK replicators in this account	List			
ListScramSecrets	Grants permission to list the Scram Secrets associated with an Amazon MSK cluster	List	cluster*		
ListTagsForResource	Grants permission to list tags of an MSK resource	Read	cluster*		
ListTopics	Grants permission to list all Kafka topics for a specified MSK cluster	List	cluster*		kafka-cluster:Connect kafka-cluster:DescribeTopic

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListVpcConnections	Grants permission to list all MSK VPC connections that this account uses	List			
PutClusterPolicy	Grants permission to create or update the resource-based policy for a cluster	Write	cluster*		
RebootBroker	Grants permission to reboot broker	Write	cluster*		
RejectClientVpcConnection	Grants permission to reject a MSK VPC connection	Write	cluster*		
			vpc-connection*		
TagResource	Grants permission to tag an MSK resource	Tagging	cluster		
			vpc-connection		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from an MSK resource	Tagging	cluster		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			vpc-connection		
				aws:TagKeys	
UpdateBrokerCount	Grants permission to update the number of brokers of the MSK cluster	Write	cluster*		
UpdateBrokerStorage	Grants permission to update the storage size of the brokers of the MSK cluster	Write	cluster*		
UpdateBrokerType	Grants permission to update the broker type of an Amazon MSK cluster	Write	cluster*		
UpdateClusterConfiguration	Grants permission to update the configuration of the MSK cluster	Write	cluster*		
			configuration*		
UpdateClusterKafkaVersion	Grants permission to update the MSK cluster to the specified Apache Kafka version	Write	cluster*		
UpdateConfiguration	Grants permission to create a new revision of the MSK configuration	Write	configuration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateConnectivity	Grants permission to update the connectivity settings for the MSK cluster	Write	cluster*		ec2:DescribeRouteTables ec2:DescribeSubnets
				kafka:publicAccessEnabled	
UpdateMonitoring	Grants permission to update the monitoring settings for the MSK cluster	Write	cluster*		
UpdateRebalancing	Grants permission to update the intelligent rebalancing status of the MSK cluster	Write	cluster*		
UpdateReplicationInfo	Grants permission to update the replication info of the MSK replicator	Write	replicator*		
UpdateSecurity	Grants permission to update the security settings for the MSK cluster	Write	cluster*		kms:RetireGrant

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateStorage	Grants permission to update the EBS storage (size or provisioned throughput) associated with MSK brokers or set cluster storage mode to TIERED	Write	cluster*		

Resource types defined by Amazon Managed Streaming for Apache Kafka

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
cluster	`arn:${Partition}:kafka:${Region}:${Account}:cluster/${ClusterName}/${Uuid}`	aws:ResourceTag/${TagKey}
configuration	`arn:${Partition}:kafka:${Region}:${Account}:configuration/${ConfigurationName}/${Uuid}`	
vpc-connection	`arn:${Partition}:kafka:${Region}:${VpcOwnerAccount}:vpc-connection/${ClusterOwnerAccount}/${ClusterName}/${Uuid}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
replicator	arn:${Partition}:kafka:${Region}:${Account}:replicator/${ReplicatorName}/${Uuid}	aws:ResourceTag/${TagKey}
topic	arn:${Partition}:kafka:${Region}:${Account}:topic/${ClusterName}/${ClusterUuid}/${TopicName}	
group	arn:${Partition}:kafka:${Region}:${Account}:group/${ClusterName}/${ClusterUuid}/${GroupName}	
transactional-id	arn:${Partition}:kafka:${Region}:${Account}:transactional-id/${ClusterName}/${ClusterUuid}/${TransactionalId}	

Condition keys for Amazon Managed Streaming for Apache Kafka

Amazon Managed Streaming for Apache Kafka defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
kafka:publicAccessEnabled	Filters access by the presence of public access enabled in the request	Bool

Actions, resources, and condition keys for AWS Marketplace Discovery

AWS Marketplace Discovery (service prefix: `aws-marketplace`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Marketplace Discovery
- Resource types defined by AWS Marketplace Discovery
- Condition keys for AWS Marketplace Discovery

Actions defined by AWS Marketplace Discovery

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPrivateListings	Grants permission to users to list their private offers	List			

Resource types defined by AWS Marketplace Discovery

AWS Marketplace Discovery does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Marketplace Discovery, specify `"Resource": "*"` in your policy.

Condition keys for AWS Marketplace Discovery

Marketplace Discovery has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Marketplace Entitlement Service

AWS Marketplace Entitlement Service (service prefix: `aws-marketplace`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Marketplace Entitlement Service
- Resource types defined by AWS Marketplace Entitlement Service
- Condition keys for AWS Marketplace Entitlement Service

Actions defined by AWS Marketplace Entitlement Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEntitlements	Grants permission to retrieve entitlement values for a given product. The results can be filtered based on customer identifier or product dimensions	Read			

Resource types defined by AWS Marketplace Entitlement Service

AWS Marketplace Entitlement Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Marketplace Entitlement Service, specify `"Resource": "*"` in your policy.

Condition keys for AWS Marketplace Entitlement Service

Marketplace Entitlement has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Marketplace Metering Service

AWS Marketplace Metering Service (service prefix: `aws-marketplace`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Marketplace Metering Service
- Resource types defined by AWS Marketplace Metering Service
- Condition keys for AWS Marketplace Metering Service

Actions defined by AWS Marketplace Metering Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchMeterUsage	Grants permission to post metering records for a set of customers for SaaS applications	Write			
MeterUsage	Grants permission to emit metering records	Write			
RegisterUsage	Grants permission to to verify that the customer running your paid software is subscribed to your product on AWS Marketplace, enabling you to guard against unauthorized use. Meters software use per ECS task, per	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	hour, with usage prorated to the second				
ResolveCustomer	Grants permission to resolve a registration token to obtain a CustomerIdentifier and product code	Write			

Resource types defined by AWS Marketplace Metering Service

AWS Marketplace Metering Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Marketplace Metering Service, specify `"Resource": "*"` in your policy.

Condition keys for AWS Marketplace Metering Service

Marketplace Metering has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for Amazon OpenSearch Service

Amazon OpenSearch Service (service prefix: `es`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon OpenSearch Service
- Resource types defined by Amazon OpenSearch Service
- Condition keys for Amazon OpenSearch Service

Actions defined by Amazon OpenSearch Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptInboundConnection	Grants permission to the destination domain owner to accept an inbound cross-cluster search connection request	Write			
AcceptInboundCrossClusterSearchConnection	Grants permission to the destination domain owner to accept an inbound cross-cluster search connection request. This permission is deprecated. Use AcceptInboundConnection instead	Write			
AddDataSource	Grants permission to add the data source for the OpenSearch Service domain	Write	domain*		
AddDirectQueryDataSource	Grants permission to add the data source for the provided OpenSearch arns	Write	datasource*		
				aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
AddTags	Grants permission to attach resource tags to an OpenSearch Service domain, data source, or application	Tagging	application*		
			datasource*		
			domain*		
				aws:RequestTag/${TagKey} aws:TagKeys	
Associate Package	Grants permission to associate a package with an OpenSearch Service domain	Write	domain*		
Associate Packages	Grants permission to associate multiple packages with an OpenSearch Service domain	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AuthorizeVpcEndpointAccess	Grants permission to provide access to an Amazon OpenSearch Service domain through the use of an interface VPC endpoint	Write			
CancelDomainConfigChange	Grants permission to cancel a change on an OpenSearch Service domain	Write	domain*		
CancelElasticsearchServiceSoftwareUpdate	Grants permission to cancel a service software update of a domain. This permission is deprecated. Use CancelServiceSoftwareUpdate instead	Write	domain*		
CancelServiceSoftwareUpdate	Grants permission to cancel a service software update of a domain	Write	domain*		
CreateApplication	Grants permission to create an OpenSearch Application	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDomain	Grants permission to create an Amazon OpenSearch Service domain	Write	domain		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateElasticsearchDomain	Grants permission to create an OpenSearch Service domain. This permission is deprecated. Use CreateDomain instead	Write	domain		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateElasticsearchServiceRole	Grants permission to create the service-linked role required for OpenSearch Service domains that use VPC access. This permission is deprecated. OpenSearch Service creates the service-linked role for you	Write			
CreateIndex	Grants permission to create index for the OpenSearch Service domain	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateOutboundConnection	Grants permission to create a new cross-cluster search connection from a source domain to a destination domain	Write	domain*		
CreateOutboundCrossClusterSearchConnection	Grants permission to create a new cross-cluster search connection from a source domain to a destination domain. This permission is deprecated. Use CreateOutboundConnection instead	Write	domain*		
CreatePackage	Grants permission to add a package for use with OpenSearch Service domains	Write			
CreateServiceRole	Grants permission to create the service-linked role required for Amazon OpenSearch Service domains that use VPC access	Write			
CreateVpcEndpoint	Grants permission to create an Amazon OpenSearch Service-managed VPC endpoint	Write			
DeleteApplication	Grants permission to delete an OpenSearch Application	Write	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDataSource	Grants permission to delete the data source for the OpenSearch Service domain	Write	domain*		
DeleteDirectQueryDataSource	Grants permission to delete the data source for the provided OpenSearch arns	Write	datasource*		
DeleteDomain	Grants permission to delete an Amazon OpenSearch Service domain and all of its data	Write	domain*		
DeleteElasticsearchDomain	Grants permission to delete an OpenSearch Service domain and all of its data. This permission is deprecated. Use DeleteDomain instead	Write	domain*		
DeleteElasticsearchServiceRole	Grants permission to delete the service-linked role required for OpenSearch Service domains that use VPC access. This permission is deprecated. Use the IAM API to delete service-linked roles	Write			
DeleteInboundConnection	Grants permission to the destination domain owner to delete an existing inbound cross-cluster search connection	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteInboundCrossClusterSearchConnection	Grants permission to the destination domain owner to delete an existing inbound cross-cluster search connection. This permission is deprecated. Use DeleteInboundConnection instead	Write			
DeleteIndex	Grants permission to delete Index for the OpenSearch Service domain	Write	domain*		
DeleteOutboundConnection	Grants permission to the source domain owner to delete an existing outbound cross-cluster search connection	Write			
DeleteOutboundCrossClusterSearchConnection	Grants permission to the source domain owner to delete an existing outbound cross-cluster search connection. This permission is deprecated. Use DeleteOutboundConnection instead	Write			
DeletePackage	Grants permission to delete a package from OpenSearch Service. The package cannot be associated with any domains	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVpcEndpoint	Grants permission to delete an Amazon OpenSearch Service-managed interface VPC endpoint	Write			
DescribeDomain	Grants permission to view a description of the domain configuration for the specified OpenSearch Service domain, including the domain ID, service endpoint, and ARN	Read	domain*		
DescribeDomainAutoTunes	Grants permission to view the Auto-Tune configuration of the domain for the specified OpenSearch Service domain, including the Auto-Tune state and maintenance schedules	Read	domain*		
DescribeDomainChangeProgress	Grants permission to view detail stage progress of an OpenSearch Service domain	Read	domain*		
DescribeDomainConfig	Grants permission to view a description of the configuration options and status of an OpenSearch Service domain	Read	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDomainHealth	Grants permission to view information about domain and node health, the standby Availability Zone, number of nodes per Availability Zone, and shard count per node	Read	domain*		
DescribeDomainNodes	Grants permission to view information about nodes configured for the domain and their configurations- the node id, type of node, status of node, Availability Zone, instance type and storage	Read	domain*		
DescribeDomains	Grants permission to view a description of the domain configuration for up to five specified OpenSearch Service domains	List	domain*		
DescribeDryRunProgress	Grants permission to describe the status of a pre-update validation check on an OpenSearch Service domain	Read	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeElasticsearchDomain	Grants permission to view a description of the domain configuration for the specified OpenSearch Service domain, including the domain ID, service endpoint, and ARN. This permission is deprecated. Use DescribeDomain instead	Read	domain*		
DescribeElasticsearchDomainConfig	Grants permission to view a description of the configuration and status of an OpenSearch Service domain. This permission is deprecated. Use DescribeDomainConfig instead	Read	domain*		
DescribeElasticsearchDomains	Grants permission to view a description of the domain configuration for up to five specified Amazon OpenSearch domains. This permission is deprecated. Use DescribeDomains instead	List	domain*		
DescribeElasticsearchInstanceTypeLimits	Grants permission to view the instance count, storage, and master node limits for a given OpenSearch version and instance type. This permission is deprecated. Use DescribeInstanceTypeLimits instead	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInboundConnections	Grants permission to list all the inbound cross-cluster search connections for a destination domain	List			
DescribeInboundCrossClusterSearchConnections	Grants permission to list all the inbound cross-cluster search connections for a destination domain. This permission is deprecated. Use DescribeInboundConnections instead	List			
DescribeInstanceTypeLimits	Grants permission to view the instance count, storage, and master node limits for a given engine version and instance type	List			
DescribeOutboundConnections	Grants permission to list all the outbound cross-cluster search connections for a source domain	List			
DescribeOutboundCrossClusterSearchConnections	Grants permission to list all the outbound cross-cluster search connections for a source domain. This permission is deprecated. Use DescribeOutboundConnections instead	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribePackages	Grants permission to describe all packages available to OpenSearch Service domains	Read			
DescribeReservedElasticsearchInstanceOfferings	Grants permission to fetch Reserved Instance offerings for Amazon OpenSearch Service. This permission is deprecated. Use DescribeReservedInstanceOfferings instead	List			
DescribeReservedElasticsearchInstances	Grants permission to fetch OpenSearch Service Reserved Instances that have already been purchased. This permission is deprecated. Use DescribeReservedInstances instead	List			
DescribeReservedInstanceOfferings	Grants permission to fetch Reserved Instance offerings for OpenSearch Service	List			
DescribeReservedInstances	Grants permission to fetch OpenSearch Service Reserved Instances that have already been purchased	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVpcEndpoints	Grants permission to describe one or more Amazon OpenSearch Service-managed VPC endpoints	List			
DissociatePackage	Grants permission to disassociate a package from the specified OpenSearch Service domain	Write	domain*		
DissociatePackages	Grants permission to disassociate multiple packages from the specified OpenSearch Service domain	Write	domain*		
ESCrossClusterGet	Grants permission to send cross-cluster requests to a destination domain	Read	domain		
ESHttpDelete	Grants permission to send HTTP DELETE requests to the OpenSearch APIs	Write	domain		
ESHttpGet	Grants permission to send HTTP GET requests to the OpenSearch APIs	Read	domain		
ESHttpHead	Grants permission to send HTTP HEAD requests to the OpenSearch APIs	Read	domain		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ESHttpPatch	Grants permission to send HTTP PATCH requests to the OpenSearch APIs	Write	domain		
ESHttpPost	Grants permission to send HTTP POST requests to the OpenSearch APIs	Write	domain		
ESHttpPut	Grants permission to send HTTP PUT requests to the OpenSearch APIs	Write	domain		
GetApplication	Grants permission to get information about an OpenSearch Application	Read	application*		
GetCompatibleElasticsearchVersions	Grants permission to fetch a list of compatible OpenSearch and Elasticsearch versions to which an OpenSearch Service domain can be upgraded. This permission is deprecated. Use GetCompatibleVersions instead	List	domain*		
GetCompatibleVersions	Grants permission to fetch list of compatible engine versions to which an OpenSearch Service domain can be upgraded	List	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDataSource	Grants permission to get the data source for the OpenSearch Service domain	Read	domain*		
GetDirectQueryDataSource	Grants permission to get the data source for the provided OpenSearch arns	Read	datasource*		
GetDomainMaintenanceStatus	Grants permission to retrieve the status of maintenance action for the node	Read	domain*		
GetIndex	Grants permission to get index for the OpenSearch Service domain	Read	domain*		
GetPackageVersionHistory	Grants permission to fetch the version history for a package	Read			
GetUpgradeHistory	Grants permission to fetch the upgrade history of a given OpenSearch Service domain	Read	domain*		
GetUpgradeStatus	Grants permission to fetch the upgrade status of a given OpenSearch Service domain	Read	domain*		
ListApplications	Grants permission to list OpenSearch Applications	List	application*		
ListDataSources	Grants permission to retrieve a list of data source for the OpenSearch Service domain	List	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDirectQueryDataSources	Grants permission to retrieve a list of data source for the provided OpenSearch arns	List	datasource*		
ListDomainMaintenances	Grants permission to retrieve a list of maintenance actions for the OpenSearch Service domain	List	domain*		
ListDomainNames	Grants permission to display the names of all OpenSearch Service domains that the current user owns	List			
ListDomainsForPackage	Grants permission to list all OpenSearch Service domains that a package is associated with	List			
ListElasticsearchInstanceTypeDetails	Grants permission to list all instance types and available features for a given OpenSearch version. This permission is deprecated. Use ListInstanceTypeDetails instead	List			
ListElasticsearchInstanceTypes	Grants permission to list all EC2 instance types that are supported for a given OpenSearch version	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListElasticsearchVersions	Grants permission to list all supported OpenSearch versions on Amazon OpenSearch Service. This permission is deprecated. Use ListVersions instead	List			
ListInstanceTypeDetails	Grants permission to list all instance types and available features for a given OpenSearch or Elasticsearch version	List			
ListPackagesForDomain	Grants permission to list all packages associated with the OpenSearch Service domain	List	domain*		
ListScheduledActions	Grants permission to retrieve a list of configuration changes that are scheduled for a OpenSearch Service domain	List	domain*		
ListTags	Grants permission to display all resource tags for an OpenSearch Service domain, data source, or application	Read	application*		
			datasource*		
			domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListVersions	Grants permission to list all supported OpenSearch and Elasticsearch versions in Amazon OpenSearch Service	List			
ListVpcEndpointAccess	Grants permission to retrieve information about each AWS principal that is allowed to access a given Amazon OpenSearch Service domain through the use of an interface VPC endpoint	List			
ListVpcEndpoints	Grants permission to retrieve all Amazon OpenSearch Service-managed VPC endpoints in the current AWS account and Region	List			
ListVpcEndpointsForDomain	Grants permission to retrieve all Amazon OpenSearch Service-managed VPC endpoints associated with a particular domain	List			
PurchaseReservedElasticsearchInstanceOffering	Grants permission to purchase OpenSearch Service Reserved Instances. This permission is deprecated. Use PurchaseReservedInstanceOffering instead	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PurchaseReservedInstanceOffering	Grants permission to purchase OpenSearch reserved instances	Write			
RejectInboundConnection	Grants permission to the destination domain owner to reject an inbound cross-cluster search connection request	Write			
RejectInboundCrossClusterSearchConnection	Grants permission to the destination domain owner to reject an inbound cross-cluster search connection request. This permission is deprecated. Use RejectInboundConnection instead	Write			
RemoveTags	Grants permission to remove resource tags from an OpenSearch Service domain, data source, or application	Tagging	application*		
			datasource*		
			domain*		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RevokeVpcEndpointAccess	Grants permission to revoke access to an Amazon OpenSearch Service domain that was provided through an interface VPC endpoint	Write			
StartDomainMaintenance	Grants permission to initiate the maintenance on the node	Write	domain*		
StartElasticsearchServiceSoftwareUpdate	Grants permission to start a service software update of a domain. This permission is deprecated. Use StartServiceSoftwareUpdate instead	Write	domain*		
StartServiceSoftwareUpdate	Grants permission to start a service software update of a domain	Write	domain*		
UpdateApplication	Grants permission to update an OpenSearch Application	Write	application*		
UpdateDataSource	Grants permission to update the data source for the OpenSearch Service domain	Write	domain*		
UpdateDirectQueryDataSource	Grants permission to update the data source for the provided OpenSearch arns	Write	datasource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDomainConfig	Grants permission to modify the configuration of an OpenSearch Service domain, such as the instance type or number of instances	Write	domain*		
UpdateElasticsearchDomainConfig	Grants permission to modify the configuration of an OpenSearch Service domain, such as the instance type or number of instances. This permission is deprecated. Use UpdateDomainConfig instead	Write	domain*		
UpdateIndex	Grants permission to update index for the OpenSearch Service domain	Write	domain*		
UpdatePackage	Grants permission to update a package for use with OpenSearch Service domains	Write			
UpdatePackageScope	Grants permission to update scope a package	Write			
UpdateScheduledAction	Grants permission to reschedule a planned OpenSearch Service domain configuration change for a later time	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateVpcEndpoint	Grants permission to modify an Amazon OpenSearch Service-managed interface VPC endpoint	Write			
UpgradeDomain	Grants permission to initiate upgrade of an OpenSearch Service domain to a given version	Write	domain*		
UpgradeElasticsearchDomain	Grants permission to initiate upgrade of an OpenSearch Service domain to a specified version. This permission is deprecated. Use UpgradeDomain instead	Write	domain*		

Resource types defined by Amazon OpenSearch Service

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
domain	`arn:${Partition}:es:${Region}:${Account}:domain/${DomainName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
application	arn:${Partition}:opensearch:${Region}:${Account}:application/${AppId}	aws:ResourceTag/${TagKey}
es_role	arn:${Partition}:iam::${Account}:role/aws-service-role/es.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService	aws:ResourceTag/${TagKey}
opensearchservice_role	arn:${Partition}:iam::${Account}:role/aws-service-role/opensearchservice.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService	aws:ResourceTag/${TagKey}
datasource	arn:${Partition}:opensearch:${Region}:${Account}:datasource/${DataSourceName}	aws:ResourceTag/${TagKey}

Condition keys for Amazon OpenSearch Service

Amazon OpenSearch Service defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access based on the tags that are passed in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access based on the tags associated with the resource	String
aws:TagKeys	Filters access based on the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Organizations

AWS Organizations (service prefix: `organizations`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Organizations
- Resource types defined by AWS Organizations
- Condition keys for AWS Organizations

Actions defined by AWS Organizations

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of

access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptHandshake	Grants permission to send a response to the originator of a handshake agreeing to the action proposed by the handshake request	Write	handshake*		iam:CreateServiceLinkedRole
AttachPolicy	Grants permission to attach a policy to a root, an organizational unit, or an individual account	Write	policy*		
			account		
			organizationalunit		
			root		
				organizations:PolicyType	
CancelHandshake	Grants permission to cancel a handshake	Write	handshake*		
CloseAccount	Grants permission to close an AWS account that is now a part of an Organizations, either created within the organization, or invited to join the organization	Write	account*		
CreateAccount	Grants permission to create an AWS account that is automatically a member of the organization with the	Write		aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	credentials that made the request			aws:TagKeys aws:ResourceTag/${TagKey}	
CreateGovCloudAccount	Grants permission to create an AWS GovCloud (US) account	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateOrganization	Grants permission to create an organization. The account with the credentials that calls the CreateOrganization operation automatically becomes the management account of the new organization	Write			iam:CreateServiceLinkedRole
CreateOrganizationalUnit	Grants permission to create an organizational unit (OU) within a root or parent OU	Write	organizationalunit root		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePolicy	Grants permission to create a policy that you can attach to a root, an organizational unit (OU), or an individual AWS account	Write		organizations:PolicyType aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeclineHandshake	Grants permission to decline a handshake request. This sets the handshake state to DECLINED and effectively deactivates the request	Write	handshake*		
DeleteOrganization	Grants permission to delete the organization	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteOrganizationalUnit	Grants permission to delete an organizational unit from a root or another OU	Write	organizationalunit*		
DeletePolicy	Grants permission to delete a policy from your organization	Write	policy*		
				organizations:PolicyType	
DeleteResourcePolicy	Grants permission to delete a resource policy from your organization	Write			
DeregisterDelegatedAdministrator	Grants permission to deregister the specified member AWS account as a delegated administrator for the AWS service that is specified by ServicePrincipal	Write	account*		
				organizations:ServicePrincipal	
DescribeAccount	Grants permission to retrieve Organizations-related details about the specified account	Read	account*		
DescribeCreateAccountStatus	Grants permission to retrieve the current status of an asynchronous request to create an account	Read			
DescribeEffectivePolicy	Grants permission to retrieve the effective policy for an account	Read	account*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				organizations:PolicyType	
DescribeHandshake	Grants permission to retrieve details about a previously requested handshake	Read	handshake*		
DescribeOrganization	Grants permission to retrieve details about the organization that the calling credentials belong to	Read			
DescribeOrganizationalUnit	Grants permission to retrieve details about an organizational unit (OU)	Read	organizationalunit*		
DescribePolicy	Grants permission to retrieve details about a policy	Read	policy*		
				organizations:PolicyType	
DescribeResourcePolicy	Grants permission to retrieve information about a resource policy	Read			
DescribeResponsibilityTransfer	Grants permission to retrieve details about a previously responsibility transfer	Read	responsibilitytransfer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				organizations:TransferType organizations:TransferDirection	
DetachPolicy	Grants permission to detach a policy from a target root, organizational unit, or account	Write	policy*		
			account		
			organizationalunit		
			root		
				organizations:PolicyType	
DisableAWSServiceAccess	Grants permission to disable integration of an AWS service (the service that is specified by ServicePrincipal) with AWS Organizations	Write		organizations:ServicePrincipal	
DisablePolicyType	Grants permission to disable an organization policy type in a root	Write	root*		
				organizations:PolicyType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableAWSServiceAccess	Grants permission to enable integration of an AWS service (the service that is specified by ServicePrincipal) with AWS Organizations	Write		organizations:ServicePrincipal	
EnableAllFeatures	Grants permission to start the process to enable all features in an organization, upgrading it from supporting only Consolidated Billing features	Write			
EnablePolicyType	Grants permission to enable a policy type in a root	Write	root*		
				organizations:PolicyType	
InviteAccountToOrganization	Grants permission to send an invitation to another AWS account, asking it to join your organization as a member account	Write	account		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
InviteOrganizationToTransferResponsibility	Grants permission to send an invitation to another AWS account, asking it to transfer a particular responsibility to your organization	Write	account		
				organizations:TransferType	
LeaveOrganization	Grants permission to remove a member account from its parent organization	Write			
ListAWSServiceAccessForOrganization	Grants permission to retrieve the list of the AWS services for which you enabled integration with your organization	List			
ListAccounts	Grants permission to list all of the accounts in the organization	List			
ListAccountsForParent	Grants permission to list the accounts in an organization that are contained by a root or organizational unit (OU)	List	organizationalunit		
			root		
ListAccountsWithInvalidEffectivePolicy	Grants permission to list accounts that have invalid effective policies for a specified policy type	List		organizations:PolicyType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListChildren	Grants permission to list all of the OUs or accounts that are contained in a parent OU or root	List	organizationalunit		
			root		
ListCreateAccountStatus	Grants permission to list the asynchronous account creation requests that are currently being tracked for the organization	List			
ListDelegatedAdministrators	Grants permission to list the AWS accounts that are designated as delegated administrators in this organization	List		organizations:ServicePrincipal	
ListDelegatedServicesForAccount	Grants permission to list the AWS services for which the specified account is a delegated administrator in this organization	List	account*		
ListEffectivePolicyValidationErrors	Grants permission to list validation errors found in the effective policy for a specific account and policy type	List	account*		
				organizations:PolicyType	
ListHandshakesForAccount	Grants permission to list all of the handshakes that are associated with an account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListHandshakesForOrganization	Grants permission to list the handshakes that are associated with the organization	List			
ListInboundResponsibilityTransfers	Grants permission to list all responsibilities of a particular type transfered to your organization	List		organizations:TransferType organizations:TransferDirection	
ListOrganizationalUnitsForParent	Grants permission to list all of the organizational units (OUs) in a parent organizational unit or root	List	organizationalunit root		
ListOutboundResponsibilityTransfers	Grants permission to list all responsibilities of a particular type transfered to another organization	List		organizations:TransferType organizations:TransferDirection	
ListParents	Grants permission to list the root or organizational units (OUs) that serve as the immediate parent of a child OU or account	List	account organizationalunit		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPolicies	Grants permission to list all of the policies in an organization	List		organizations:PolicyType	
ListPoliciesForTarget	Grants permission to list all of the policies that are directly attached to a root, organizational unit (OU), or account	List	account		
			organizationalunit		
			root		
				organizations:PolicyType	
ListRoots	Grants permission to list all of the roots that are defined in the organization	List			
ListTagsForResource	Grants permission to list all tags for the specified resource	List	account		
			organizationalunit		
			policy		
			resourcepolicy		
			responsibilitytransfer		
			root		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				organizations:PolicyType	
ListTargetsForPolicy	Grants permission to list all the roots, OUs, and accounts to which a policy is attached	List	policy*		
				organizations:PolicyType	
MoveAccount	Grants permission to move an account from its current root or OU to another parent root or OU	Write	account*		
			organizationalunit*		
			root*		
PutResourcePolicy	Grants permission to create or update a resource policy	Write	resourcepolicy*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterDelegatedAdministrator	Grants permission to register the specified member account to administer the Organizations features of the AWS service that is specified by ServicePrincipal	Write	account*		
				organizations:ServicePrincipal	
RemoveAccountFromOrganization	Grants permission to remove the specified account from the organization	Write	account*		
TagResource	Grants permission to add one or more tags to the specified resource	Tagging	account		
			organizationalunit		
			policy	organizations:PolicyType	
			resourcepolicy		
			responsibilitytransfer	organizations:TransferType organizations:TransferDirection	
			root		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} organizations:PolicyType	
TerminateResponsibilityTransfer	Grants permission to end the transfer for a responsibility to or from your organization	Write	responsibilitytransfer*		
				organizations:TransferType organizations:TransferDirection	
UntagResource	Grants permission to remove one or more tags from the specified resource	Tagging	account		
			organizationalunit		
			policy		
			resourcepolicy		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			responsibilitytransfer	organizations:TransferType organizations:TransferDirection	
			root		
				aws:TagKeys organizations:PolicyType	
UpdateOrganizationalUnit	Grants permission to rename an organizational unit (OU)	Write	organizationalunit*		
UpdatePolicy	Grants permission to update an existing policy with a new name, description, or content	Write	policy*		
				organizations:PolicyType	
UpdateResponsibilityTransfer	Grants permission to rename a responsibility transfer to or from your organization	Write	responsibilitytransfer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				organizations:TransferType organizations:TransferDirection	

Resource types defined by AWS Organizations

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
account	`arn:${Partition}:organizations::${Account}:account/o-${OrganizationId}/${AccountId}`	aws:ResourceTag/${TagKey}
handshake	`arn:${Partition}:organizations::${Account}:handshake/o-${OrganizationId}/${HandshakeType}/h-${HandshakeId}`	
organization	`arn:${Partition}:organizations::${Account}:organization/o-${OrganizationId}`	

Resource types	ARN	Condition keys
organizationalunit	arn:${Partition}:organizations::${Account}:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}	aws:ResourceTag/${TagKey}
policy	arn:${Partition}:organizations::${Account}:policy/o-${OrganizationId}/${PolicyType}/p-${PolicyId}	aws:ResourceTag/${TagKey}
resourcepolicy	arn:${Partition}:organizations::${Account}:resourcepolicy/o-${OrganizationId}/rp-${ResourcePolicyId}	aws:ResourceTag/${TagKey}
awspolicy	arn:${Partition}:organizations::aws:policy/${PolicyType}/p-${PolicyId}	
root	arn:${Partition}:organizations::${Account}:root/o-${OrganizationId}/r-${RootId}	aws:ResourceTag/${TagKey}
responsibilitytransfer	arn:${Partition}:organizations::${Account}:transfer/o-${OrganizationId}/${TransferType}/${TransferDirection}/rt-${ResponsibilityTransferId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Organizations

AWS Organizations defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
organizations:PolicyType	Filters access by the specified policy type names	String
organizations:ServicePrincipal	Filters access by the specified service principal names	String
organizations:TransferDirection	Filters access by the specified responsibility transfer by the direction	String
organizations:TransferType	Filters access by the specified responsibility transfer type names	String

Actions, resources, and condition keys for AWS Performance Insights

AWS Performance Insights (service prefix: `pi`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Performance Insights
- Resource types defined by AWS Performance Insights
- Condition keys for AWS Performance Insights

Actions defined by AWS Performance Insights

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePerformanceAnalysisReport	Grants permission to call CreatePerformanceAnalysisReport API to create a Performance Analysis Report for a specified DB instance	Write	perf-reports-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePerformanceAnalysisReport	Grants permission to call DeletePerformanceAnalysisReport API to delete a Performance Analysis Report for a specified DB instance	Write	perf-reports-resource*		
DescribeDimensionKeys	Grants permission to call DescribeDimensionKeys API to retrieve the top N dimension keys for a metric for a specific time period	Read	metric-resource*		
				pi:Dimensions	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDimensionKeyDetails	Grants permission to call GetDimensionKeyDetails API to retrieve the attributes of the specified dimension group	Read	metric-resource*		
				pi:Dimensions	
GetPerformanceAnalysisReport	Grants permission to call GetPerformanceAnalysisReport API to retrieve a Performance Analysis Report for a specified DB instance	Read	perf-reports-resource*		
GetResourceMetadata	Grants permission to call GetResourceMetadata API to retrieve the metadata for different features	Read	metric-resource*		
GetResourceMetrics	Grants permission to call GetResourceMetrics API to retrieve PI metrics for a set of data sources, over a time period	Read	metric-resource*		
				pi:Dimensions	
ListAvailableResourceDimensions	Grants permission to call ListAvailableResourceDimensions API to retrieve the dimensions that can be queried for each specified metric type on a specified DB instance	Read	metric-resource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAvailableResourceMetrics	Grants permission to call ListAvailableResourceMetrics API to retrieve metrics of the specified types that can be queried for a specified DB instance	Read	metric-resource*		
ListPerformanceAnalysisReports	Grants permission to call ListPerformanceAnalysisReports API to list Performance Analysis Reports for a specified DB instance	List	perf-reports-resource*		
ListTagsForResource	Grants permission to call ListTagsForResource API to list tags for a resource	List	metric-resource*		
			perf-reports-resource*		
TagResource	Grants permission to call TagResource API to tag a resource	Tagging	perf-reports-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to call UntagResource API to untag a resource	Tagging	perf-reports-resource*		
				aws:TagKeys	

Resource types defined by AWS Performance Insights

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
metric-resource	`arn:${Partition}:pi:${Region}:${Account}:metrics/${ServiceType}/${Identifier}`	aws:ResourceTag/${TagKey}
perf-reports-resource	`arn:${Partition}:pi:${Region}:${Account}:perf-reports/${ServiceType}/${Identifier}/${ReportId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Performance Insights

AWS Performance Insights defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the

policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
pi:Dimensions	Filters access by the requested dimensions	ArrayOfString

Actions, resources, and condition keys for AWS Price List

AWS Price List (service prefix: `pricing`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Price List
- Resource types defined by AWS Price List
- Condition keys for AWS Price List

Actions defined by AWS Price List

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeServices	Grants permission to retrieve service details for all (paginated) services (if serviceCode is not set) or service detail for a particular service (if given serviceCode)	Read			
GetAttributeValues	Grants permission to retrieve all (paginated) possible values for a given attribute	Read			
GetPriceListFileUrl	Grants permission to retrieve the price list file URL for the given parameters	Read			
GetProducts	Grants permission to retrieve all matching products with given search criteria	Read			
ListPriceLists	Grants permission to list all (paginated) eligible price lists for the given parameters	Read			

Resource types defined by AWS Price List

AWS Price List does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Price List, specify `"Resource": "*"` in your policy.

Condition keys for AWS Price List

Price List has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Private Certificate Authority

AWS Private Certificate Authority (service prefix: `acm-pca`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Private Certificate Authority
- Resource types defined by AWS Private Certificate Authority
- Condition keys for AWS Private Certificate Authority

Actions defined by AWS Private Certificate Authority

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCertificateAuthority	Grants permission to create an AWS Private CA and its associated private key and configuration	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateCertificateAuthorityAuditReport	Grants permission to create an audit report for an AWS Private CA	Write	certificate-authority*		
CreatePermission	Grants permission to create a permission for an AWS Private CA	Permissions management	certificate-authority*		
DeleteCertificateAuthority	Grants permission to delete an AWS Private CA and its associated private key and configuration	Write	certificate-authority*		
DeletePermission	Grants permission to delete a permission for an AWS Private CA	Permissions management	certificate-authority*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePolicy	Grants permission to delete the policy for an AWS Private CA	Permissions management	certificate-authority*		
DescribeCertificateAuthority	Grants permission to return a list of the configuration and status fields contained in the specified AWS Private CA	Read	certificate-authority*		
DescribeCertificateAuthorityAuditReport	Grants permission to return the status and information about an AWS Private CA audit report	Read	certificate-authority*		
GetCertificate	Grants permission to retrieve an AWS Private CA certificate and certificate chain for the certificate authority specified by an ARN	Read	certificate-authority*		
GetCertificateAuthorityCertificate	Grants permission to retrieve an AWS Private CA certificate and certificate chain for the certificate authority specified by an ARN	Read	certificate-authority*		
GetCertificateAuthorityCsr	Grants permission to retrieve an AWS Private CA certificate signing request (CSR) for the certificate-authority specified by an ARN	Read	certificate-authority*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPolicy	Grants permission to retrieve the policy on an AWS Private CA	Read	certificate-authority*		
ImportCertificateAuthorityCertificate	Grants permission to import an SSL/TLS certificate into AWS Private CA for use as the CA certificate of an AWS Private CA	Write	certificate-authority*		
IssueCertificate	Grants permission to issue an AWS Private CA certificate	Write	certificate-authority*		
				acm-pca:TemplateArn	
ListCertificateAuthorities	Grants permission to retrieve a list of the AWS Private CA certificate authority ARNs, and a summary of the status of each CA in the calling account	List			
ListPermissions	Grants permission to list the permissions that have been applied to the AWS Private CA certificate authority	Read	certificate-authority*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTags	Grants permission to list the tags that have been applied to the AWS Private CA certificate authority	Read	certificate-authority*		
PutPolicy	Grants permission to put a policy on an AWS Private CA	Permissions management	certificate-authority*		
RestoreCertificateAuthority	Grants permission to restore an AWS Private CA from the deleted state to the state it was in when deleted	Write	certificate-authority*		
RevokeCertificate	Grants permission to revoke a certificate issued by an AWS Private CA	Write	certificate-authority*		
TagCertificateAuthority	Grants permission to add one or more tags to an AWS Private CA	Tagging	certificate-authority*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagCertificateAuthority	Grants permission to remove one or more tags from an AWS Private CA	Tagging	certificate-authority*	aws:RequestTag/${TagKey}	
				aws:TagKeys	
UpdateCertificateAuthority	Grants permission to update the configuration of an AWS Private CA	Write	certificate-authority*		

Resource types defined by AWS Private Certificate Authority

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
certificate-authority	`arn:${Partition}:acm-pca:${Region}:${Account}:certificate-authority/${CertificateAuthorityId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Private Certificate Authority

AWS Private Certificate Authority defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions

under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
acm-pca:TemplateArn	Filters access by the arn of the certificate template used in Issue Certificate request	ARN
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon RDS

Amazon RDS (service prefix: `rds`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon RDS
- Resource types defined by Amazon RDS
- Condition keys for Amazon RDS

Actions defined by Amazon RDS

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddRoleToDBCluster	Grants permission to associate an Identity and Access Management (IAM) role from an Aurora DB cluster	Write	cluster*		iam:PassRole
AddRoleToDBInstance	Grants permission to associate an AWS Identity and Access Management (IAM) role with a DB instance	Write	db*		iam:PassRole
AddSourceIdentifierToSubscription	Grants permission to add a source identifier to an existing RDS event notification subscription	Write	es*		
AddTagsToResource	Grants permission to add metadata tags to an Amazon RDS resource	Tagging	auto-backup		
			cev		
			cluster		
			cluster-auto-backup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			cluster-endpoint		
			cluster-pg		
			cluster-snapshot		
			db		
			deployment		
			es		
			global-cluster		
			integration		
			og		
			pg		
			proxy		
			proxy-endpoint		
			ri		
			secgrp		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			shardgrp		
			snapshot		
			snapshot-tenant-database		
			subgrp		
			target-group		
			tenant-database		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
ApplyPendingMaintenanceAction	Grants permission to apply a pending maintenance action to a resource	Write	cluster		
			db		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AuthorizeDBSecurityGroupIngress	Grants permission to enable ingress to a DBSecurityGroup using one of two forms of authorization	Permissions management	secgrp*		
BacktrackDBCluster	Grants permission to backtrack a DB cluster to a specific time, without creating a new DB cluster	Write	cluster*		
CancelExportTask	Grants permission to cancel an export task in progress	Write			
CopyCustomDBEngineVersion [permission only]	Grants permission to copy a custom engine version	Write	cev*		
CopyDBClusterParameterGroup	Grants permission to copy the specified DB cluster parameter group	Write	cluster-pg*		rds:AddTagsToResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CopyDBClusterSnapshot	Grants permission to create a snapshot of a DB cluster	Write	cluster-snapshot*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CopyDBParameterGroup	Grants permission to copy the specified DB parameter group	Write	pg*		rds:AddTagsToResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CopyDBSnapshot	Grants permission to copy the specified DB snapshot	Write	snapshot*		rds:AddTagsToResource rds:CopyCustomDBEngineVersion

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:CopyOptionGroup	
CopyOptionGroup	Grants permission to copy the specified option group	Write	og*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBlueGreenDeployment	Grants permission to create a blue-green deployment for a given source cluster or instance	Write	deployment*		rds:AddTagsToResource rds:CreateDBCluster rds:CreateDBClusterEndpoint rds:CreateDBInstance rds:CreateDBInstanceReadReplica
			cluster		
			cluster-pg		
			db		
			pg		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys rds:cluster-tag/${TagKey} rds:cluster-pg-tag/${TagKey} rds:db-tag/${TagKey} rds:pg-tag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				rds:req-tag/${TagKey} rds:DatabaseEngine rds:DatabaseName rds:StorageEncrypted rds:DatabaseClass rds:StorageSize rds:MultiAz rds:Piops rds:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCustomDBEngineVersion	Grants permission to create a custom engine version	Write	cev*		iam:CreateServiceLinkedRole mediaimport:CreateDatabaseBinarySnapshot rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDBCluster	Grants permission to create a new DB cluster	Write	cluster*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:AddTagsToResource rds:CreateDBInstance secretsmanager:CreateSecret secretsmanager:TagResource
			cluster-pg*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			og*		
			subgrp*		
			db		
			global-cluster		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:DatabaseEngine rds:DatabaseName rds:StorageEncrypted rds:DatabaseClass rds:StorageSize rds:Piops rds:ManageMasterUs	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				erPassword	
CreateDBClusterEndpoint	Grants permission to create a new custom endpoint and associates it with an Amazon Aurora DB cluster or Amazon DocumentDB cluster	Write	cluster*		rds:AddTagsToResource
			cluster-endpoint*		
				rds:EndpointType aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateDBClusterParameterGroup	Grants permission to create a new DB cluster parameter group	Write	cluster-pg*		rds:AddTagsToResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateDBClusterSnapshot	Grants permission to create a snapshot of a DB cluster	Write	cluster*		rds:AddTagsToResource
			cluster-snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDBInstance	Grants permission to create a new DB instance	Write	db*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:AddTagsToResource rds:CreateTenantDatabase secretsmanager:CreateSecret secretsmanager:TagResource
			cluster		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			og		
			pg		
			secgrp		
			subgrp		
				rds:BackupTarget aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:ManageMasterUserPassword rds:PubliclyAccessible	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDBInstanceReadReplica	Grants permission to create a DB instance that acts as a Read Replica of a source DB instance	Write	cluster*		iam:PassRole rds:AddTagsToResource
			db*		
			og*		
			pg*		
			subgrp*		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:PubliclyAccessible	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDBParameterGroup	Grants permission to create a new DB parameter group	Write	pg*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateDBProxy	Grants permission to create a database proxy	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole rds:AddTagsToResource
CreateDBProxyEndpoint	Grants permission to create a database proxy endpoint	Write	proxy*		rds:AddTagsToResource
			proxy-endpoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDBSecurityGroup	Grants permission to create a new DB security group. DB security groups control access to a DB instance	Write	secgrp*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateDBShardGroup	Grants permission to create a new Aurora Limitless Database DB shard group	Write	cluster*		rds:AddTagsToResource
			shardgrp*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:PubliclyAccessible	
CreateDBSnapshot	Grants permission to create a DBSnapshot	Write	db*		rds:AddTagsToResource
			snapshot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				rds:BackupTarget aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateDBSubnetGroup	Grants permission to create a new DB subnet group	Write	subgrp*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEventSubscription	Grants permission to create an RDS event notification subscription	Write	es*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateGlobalCluster	Grants permission to create an Aurora global database or DocumentDB global database spread across multiple regions	Write	cluster*		rds:AddTagsToResource
			global-cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateIntegration	Grants permission to create an Aurora zero-ETL integration with Redshift	Write	cluster*		kms:CreateGrant kms:DescribeKey rds:AddTagsToResource
			integration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateOptionGroup	Grants permission to create a new option group	Write	og*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
CreateTenantDatabase	Grants permission to create a new tenant database	Write	db*		rds:AddTagsToResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			tenant-database*		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:TenantDatabaseName rds:ManageMasterUserPassword	
CrossRegionCommunication [permission only]	Grants permission to access a resource in the remote Region when executing cross-Region operations, such as cross-Region snapshot copy or cross-Region read replica creation	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBlueGreenDeployment	Grants permission to delete blue green deployments	Write	deployment*		rds:DeleteDBCluster rds:DeleteDBClusterEndpoint rds:DeleteDBInstance rds:PromoteReadReplica rds:PromoteReadReplicaDBCluster
				aws:ResourceTag/${TagKey}	
DeleteCustomDBEngineVersion	Grants permission to delete an existing custom engine version	Write	cev*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDBCluster	Grants permission to delete a previously provisioned DB cluster	Write	cluster*		rds:AddTagsToResource rds:CreateDBClusterSnapshot rds:DeleteDBInstance
			cluster-snapshot*		
DeleteDBClusterAutomatedBackup	Grants permission to delete cluster automated backups based on the source cluster's DbClusterResourceId value or the restorable cluster's resource ID	Write	cluster-auto-backup*		
DeleteDBClusterEndpoint	Grants permission to delete a custom endpoint and removes it from an Amazon Aurora DB cluster or Amazon DocumentDB cluster	Write	cluster-endpoint*		
DeleteDBClusterParameterGroup	Grants permission to delete a specified DB cluster parameter group	Write	cluster-pg*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDBClusterSnapshot	Grants permission to delete a DB cluster snapshot	Write	cluster-snapshot*		
DeleteDBInstance	Grants permission to delete a previously provisioned DB instance	Write	db*		rds:AddTagsToResource rds:CreateDBSnapshot rds:DeleteTenantDatabase
DeleteDBInstanceAutomatedBackup	Grants permission to delete automated backups based on the source instance's DbiResourceId value or the restorable instance's resource ID	Write	auto-backup*		
DeleteDBParameterGroup	Grants permission to delete a specified DBParameterGroup	Write	pg*		
DeleteDBProxy	Grants permission to delete a database proxy	Write	proxy*		
DeleteDBProxyEndpoint	Grants permission to delete a database proxy endpoint	Write	proxy-endpoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDBSecurityGroup	Grants permission to delete a DB security group	Write	secgrp*		
DeleteDBShardGroup	Grants permission to delete an Aurora Limitless Database DB shard group	Write	shardgrp*		
DeleteDBSnapshot	Grants permission to delete a DBSnapshot	Write	snapshot*		
DeleteDBSubnetGroup	Grants permission to delete a DB subnet group	Write	subgrp*		
DeleteEventSubscription	Grants permission to delete an RDS event notification subscription	Write	es*		
DeleteGlobalCluster	Grants permission to delete a global database cluster	Write	global-cluster*		
DeleteIntegration	Grants permission to delete an Aurora zero-ETL integration with Redshift	Write	integration*		
DeleteOptionGroup	Grants permission to delete an existing option group	Write	og*		
DeleteTenantDatabase	Grants permission to delete a tenant database	Write	db*		rds:AddTagsToResource rds:CreateDBSnapshot

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			tenant-database*		
DeregisterDBProxyTargets	Grants permission to remove targets from a database proxy target group	Write	cluster*		
			db*		
			proxy*		
			target-group*		
DescribeAccountAttributes	Grants permission to list all of the attributes for a customer account	List			
DescribeBlueGreenDeployments	Grants permission to describe blue green deployments	List	deployment		
DescribeCertificates	Grants permission to list the set of CA certificates provided by Amazon RDS for this AWS account	List			
DescribeDBClusterAutomatedBackups	Grants permission to return a list of cluster automated backups for both current and deleted clusters	List	cluster		
			cluster-auto-backup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDBClusterBacktracks	Grants permission to return information about backtracks for a DB cluster	List	cluster*		
DescribeDBClusterEndpoints	Grants permission to return information about endpoints for an Amazon Aurora DB cluster	List	cluster		
			cluster-endpoint		
DescribeDBClusterParameterGroups	Grants permission to return a list of DBClusterParameter Group descriptions	List	cluster-pg		
DescribeDBClusterParameters	Grants permission to return the detailed parameter list for a particular DB cluster parameter group	List	cluster-pg*		
DescribeDBClusterSnapshotAttributes	Grants permission to return a list of DB cluster snapshot attribute names and values for a manual DB cluster snapshot	List	cluster-snapshot*		
DescribeDBClusterSnapshots	Grants permission to return information about DB cluster snapshots	List	cluster		
			cluster-snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDBClusters	Grants permission to return information about provisioned Aurora DB clusters or DocumentDB clusters	List	cluster		
DescribeDBEngineVersions	Grants permission to return a list of the available DB engines	List			
DescribeDBInstanceAutomatedBackups	Grants permission to return a list of automated backups for both current and deleted instances	List	auto-backup		
			db		
DescribeDBInstances	Grants permission to return information about provisioned RDS instances	List	db		
DescribeDBLogFiles	Grants permission to return a list of DB log files for the DB instance	List	db*		
DescribeDBMajorEngineVersions	Grants permission to return information specific for each DB major engine versions	List			
DescribeDBParameterGroups	Grants permission to return a list of DBParameterGroup descriptions	List	pg		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDBParameters	Grants permission to return the detailed parameter list for a particular DB parameter group	List	pg*		
DescribeDBProxies	Grants permission to view proxies	List	proxy		
DescribeDBProxyEndpoints	Grants permission to view proxy endpoints	List	proxy		
			proxy-endpoint		
DescribeDBProxyTargetGroups	Grants permission to view database proxy target group details	List	proxy*		
DescribeDBProxyTargets	Grants permission to view database proxy target details	List	proxy*		
			target-group*		
DescribeDBRecommendations	Grants permission to list recommendation details	List			
DescribeDBSecurityGroups	Grants permission to return a list of DBSecurityGroup descriptions	List	secgrp		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDBShardGroups	Grants permission to return information about all Aurora Limitless Database DB shard groups for this account. You can filter by shard group(s)	List	shardgrp		
DescribeDBSnapshotAttributes	Grants permission to return a list of DB snapshot attribute names and values for a manual DB snapshot	List	snapshot*		
DescribeDBSnapshotTenantDatabases	Grants permission to return information about tenant databases in DB snapshots. You can filter by Region or snapshot	List	db		
			snapshot		
			snapshot-tenant-database		
DescribeDBSnapshots	Grants permission to return information about DB snapshots	List	db		
			snapshot		
DescribeDBSubnetGroups	Grants permission to return a list of DBSubnetGroup descriptions	List	subgrp		
DescribeEngineDefaultClusterParameters	Grants permission to return the default engine and system parameter information for the cluster database engine	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeEngineDefaultParameters	Grants permission to return the default engine and system parameter information for the specified database engine	List			
DescribeEventCategories	Grants permission to display a list of categories for all event source types, or, if specified, for a specified source type	List			
DescribeEventSubscriptions	Grants permission to list all the subscription descriptions for a customer account	List	es		
DescribeEvents	Grants permission to return events related to DB instances, DB security groups, DB snapshots, and DB parameter groups for the past 14 days	List			
DescribeExportTasks	Grants permission to return information about the export tasks	List	cluster		
			cluster-snapshot		
			snapshot		
DescribeGlobalClusters	Grants permission to return information about Aurora global database clusters or DocumentDB global database clusters	List	global-cluster		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeIntegrations	Grants permission to describe an Aurora zero-ETL integration with Redshift	List	integration		
				aws:ResourceTag/${TagKey}	
DescribeOptionGroupOptions	Grants permission to describe all available options	List			
DescribeOptionGroups	Grants permission to describe the available option groups	List	og		
DescribeOrderableDBInstanceOptions	Grants permission to return a list of orderable DB instance options for the specified engine	List			
DescribePendingMaintenanceActions	Grants permission to return a list of resources (for example, DB instances) that have at least one pending maintenance action	List	cluster		
			db		
DescribeRecommendationGroups [permission only]	Grants permission to return information about recommendation groups	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeRecommendations [permission only]	Grants permission to return information about recommendations	Read			
DescribeReservedDBInstances	Grants permission to return information about reserved DB instances for this account, or about a specified reserved DB instance	List	ri		
DescribeReservedDBInstancesOfferings	Grants permission to list available reserved DB instance offerings	List			
DescribeSourceRegions	Grants permission to return a list of the source AWS Regions where the current AWS Region can create a Read Replica or copy a DB snapshot from	List			
DescribeTenantDatabases	Grants permission to return information about provisioned tenant databases. You can filter by Region or snapshot	List	db tenant-database		
DescribeValidDBInstanceModifications	Grants permission to list available modifications you can make to your DB instance	List	db*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableHttpEndpoint	Grants permission to disable http endpoint for a DB cluster	Write	cluster*		
DownloadCompleteDBLogFile	Grants permission to download specified log file	Read	db*		
DownloadDBLogFilePortion	Grants permission to download all or a portion of the specified log file, up to 1 MB in size	Read	db*		
EnableHttpEndpoint	Grants permission to enable http endpoint for a DB cluster	Write	cluster*		
FailoverDBCluster	Grants permission to force a failover for a DB cluster	Write	cluster*		
FailoverGlobalCluster	Grants permission to failover a global cluster	Write	cluster*		
			global-cluster*		
ListTagsForResource	Grants permission to list all tags on an Amazon RDS resource	Read	auto-backup		
			cev		
			cluster		
			cluster-auto-backup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			cluster-endpoint		
			cluster-pg		
			cluster-snapshot		
			db		
			es		
			global-cluster		
			integration		
			og		
			pg		
			proxy		
			proxy-endpoint		
			ri		
			secgrp		
			shardgrp		
			snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot-tenant-database		
			subgrp		
			target-group		
			tenant-database		
ModifyActivityStream	Grants permission to modify a database activity stream	Write	db*		
ModifyCertificates	Grants permission to modify the system-default Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificate for Amazon RDS for new DB instances	Write			
ModifyCurrentDBClusterCapacity	Grants permission to modify current cluster capacity for an Amazon Aurora Serverless DB cluster	Write	cluster*		
ModifyCustomDBEngineVersion	Grants permission to modify an existing custom engine version	Write	cev*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyDBCluster	Grants permission to modify a setting for an Amazon Aurora DB cluster or Amazon DocumentDB cluster	Write	cluster*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:ModifyDBInstance secretsmanager:CreateSecret secretsmanager:RotateSecret secretsmanager:TagResource
			cluster-pg		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			og		
			pg		
				rds:DatabaseClass rds:StorageSize rds:Piops rds:ManageMasterUserPassword	
ModifyDBClusterEndpoint	Grants permission to modify the properties of an endpoint in an Amazon Aurora DB cluster or Amazon DocumentDB cluster	Write	cluster-endpoint*		
ModifyDBClusterParameterGroup	Grants permission to modify the parameters of a DB cluster parameter group	Write	cluster-pg*		
ModifyDBClusterSnapshotAttribute	Grants permission to add an attribute and values to, or removes an attribute and values from, a manual DB cluster snapshot	Write	cluster-snapshot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyDBInstance	Grants permission to modify settings for a DB instance	Write	db*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:AddTagsToResource rds:CreateTenantDatabase secretsmanager:CreateSecret secretsmanager:RotateSecret

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:TagResource
			og		
			pg		
			secgrp		
			subgrp		
				rds:ManageMasterUserPassword	
ModifyDBParameterGroup	Grants permission to modify the parameters of a DB parameter group	Write	pg*		
ModifyDBProxy	Grants permission to modify database proxy	Write	proxy*		iam:PassRole
ModifyDBProxyEndpoint	Grants permission to modify database proxy endpoint	Write	proxy-endpoint*		
ModifyDBProxyTargetGroup	Grants permission to modify target group for a database proxy	Write	target-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyDBRecommendation	Grants permission to modify recommendation	Write			
ModifyDBShardGroup	Grants permission to modify properties of an Aurora Limitless Database DB shard group	Write	shardgrp*		
ModifyDBSnapshot	Grants permission to update a manual DB snapshot, which can be encrypted or not encrypted, with a new engine version	Write	snapshot* og		
ModifyDBSnapshotAttribute	Grants permission to add an attribute and values to, or removes an attribute and values from, a manual DB snapshot	Write	snapshot*		
ModifyDBSubnetGroup	Grants permission to modify an existing DB subnet group	Write	subgrp*		
ModifyEventSubscription	Grants permission to modify an existing RDS event notification subscription	Write	es*		
ModifyGlobalCluster	Grants permission to modify a setting for an Amazon Aurora global cluster or Amazon DocumentDB global cluster	Write	global-cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyIntegration	Grants permission to modify an Aurora zero-ETL integration with Redshift	Write	integration*		
ModifyOptionGroup	Grants permission to modify an existing option group	Write	og*		iam:PassRole
ModifyRecommendation [permission only]	Grants permission to modify recommendation	Write			
ModifyTenantDatabase	Grants permission to modify a tenant database	Write	db*		
			tenant-database*		
				rds:TenantDatabaseName rds:ManageMasterUserPassword	
PromoteReadReplica	Grants permission to promote a Read Replica DB instance to a standalone DB instance	Write	db*		rds:AddTagsToResource
PromoteReadReplicaDBCluster	Grants permission to promote a Read Replica DB cluster to a standalone DB cluster	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PurchaseReservedDBInstancesOffering	Grants permission to purchase a reserved DB instance offering	Write	ri*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
RebootDBCluster	Grants permission to reboot a previously provisioned DB cluster	Write	cluster*		rds:RebootDBInstance
RebootDBInstance	Grants permission to restart the database engine service	Write	db*		
RebootDBShardGroup	Grants permission to reboot an Aurora Limitless Database DB shard group	Write	shardgrp*		
RegisterDBProxyTargets	Grants permission to add targets to a database proxy target group	Write	target-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveFromGlobalCluster	Grants permission to detach an Aurora secondary cluster from an Aurora global database cluster or DocumentDB global cluster	Write	cluster*		
			global-cluster*		
RemoveRoleFromDBCluster	Grants permission to disassociate an AWS Identity and Access Management (IAM) role from an Amazon Aurora DB cluster	Write	cluster*		iam:PassRole
RemoveRoleFromDBInstance	Grants permission to disassociate an AWS Identity and Access Management (IAM) role from a DB instance	Write	db*		iam:PassRole
RemoveSourceIdentifierFromSubscription	Grants permission to remove a source identifier from an existing RDS event notification subscription	Write	es*		
RemoveTagsFromResource	Grants permission to remove metadata tags from an Amazon RDS resource	Tagging	auto-backup		
			cev		
			cluster		
			cluster-auto-backup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			cluster-endpoint		
			cluster-pg		
			cluster-snapshot		
			db		
			deployment		
			es		
			global-cluster		
			integration		
			og		
			pg		
			proxy		
			proxy-endpoint		
			ri		
			secgrp		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			shardgrp		
			snapshot		
			snapshot-tenant-database		
			subgrp		
			target-group		
			tenant-database		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
ResetDBClusterParameterGroup	Grants permission to modify the parameters of a DB cluster parameter group to the default value	Write	cluster-pg*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResetDBParameterGroup	Grants permission to modify the parameters of a DB parameter group to the engine/system default value	Write	pg*		
RestoreDBClusterFromS3	Grants permission to create an Amazon Aurora DB cluster from data stored in an Amazon S3 bucket	Write	cluster*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:AddTagsToResource secretsmanager:CreateSecret secretsmanager:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			cluster-pg*		
			og*		
			subgrp*		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:DatabaseEngine rds:DatabaseName rds:StorageEncrypted rds:ManageMasterUserPassword	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreDBClusterFromSnapshot	Grants permission to create a new DB cluster from a DB cluster snapshot	Write	cluster*		iam:PassRole rds:AddTagsToResource rds:CreateDBInstance
			cluster-pg*		
			og*		
			subgrp*		
			cluster-snapshot		
			snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:DatabaseClass rds:StorageSize rds:Piops	
RestoreDBClusterToPointInTime	Grants permission to restore a DB cluster to an arbitrary point in time	Write	cluster*		iam:PassRole rds:AddTagsToResource rds:CreateDBInstance
			cluster-pg*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			og*		
			subgrp*		
			cluster-auto-backup		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:DatabaseClass rds:StorageSize rds:Piops	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreDBInstanceFromDBSnapshot	Grants permission to create a new DB instance from a DB snapshot	Write	db*		iam:PassRole rds:AddTagsToResource rds:CreateTenantDatabase
			og*		
			pg*		
			subgrp*		
			cluster-snapshot		
			snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				rds:BackupTarget aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:ManageMasterUserPassword rds:PubliclyAccessible	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreDBInstanceFromS3	Grants permission to create a new DB instance from an Amazon S3 bucket	Write	db*		iam:PassRole kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey rds:AddTagsToResource secretsmanager:CreateSecret secretsmanager:TagResource
			og*		
			pg*		
			subgrp*		
			secgrp		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:ManageMasterUserPassword rds:PubliclyAccessible	
RestoreDBInstanceToPointInTime	Grants permission to restore a DB instance to an arbitrary point in time	Write	db*		iam:PassRole rds:AddTagsToResource rds:CreateTenantDatabase
			og*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			pg*		
			subgrp*		
			auto-backup		
				rds:BackupTarget aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey} rds:ManageMasterUserPassword rds:PubliclyAccessible	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RevokeDBSecurityGroupIngress	Grants permission to revoke ingress from a DBSecurityGroup for previously authorized IP ranges or EC2 or VPC Security Groups	Write	secgrp*		
StartActivityStream	Grants permission to start Activity Stream	Write	cluster		
			db		
StartDBCluster	Grants permission to start the DB cluster	Write	cluster*		
StartDBInstance	Grants permission to start the DB instance	Write	db*		
StartDBInstanceAutomatedBackupsReplication	Grants permission to start replication of automated backups to a different AWS Region	Write	auto-backup*		rds:AddTagsToResource
			db*		
				aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartExportTask	Grants permission to start a new Export task for a DB snapshot	Write	cluster		iam:PassRole
			cluster-snapshot		
			snapshot		
StopActivityStream	Grants permission to stop Activity Stream	Write	cluster		
			db		
StopDBCluster	Grants permission to stop the DB cluster	Write	cluster*		
StopDBInstance	Grants permission to stop the DB instance	Write	db*		rds:AddTagsToResource rds:CreateDBSnapshot
			snapshot		
StopDBInstanceAutomatedBackupsReplication	Grants permission to stop automated backup replication for a DB instance	Write	db*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SwitchoverBlueGreenDeployment	Grants permission to switch a blue-green deployment from source instance or cluster to target	Write	deployment*		rds:ModifyDBCluster rds:ModifyDBInstance rds:PromoteReadReplica rds:PromoteReadReplicaDBCluster
				aws:ResourceTag/${TagKey}	
SwitchoverGlobalCluster	Grants permission to switchover a global cluster	Write	cluster*		
			global-cluster*		
SwitchoverReadReplica	Grants permission to switch over a read replica, making it the new primary database	Write	db*		

Resource types defined by Amazon RDS

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
cluster	`arn:${Partition}:rds:${Region}:${Account}:cluster:${DbClusterInstanceName}`	aws:ResourceTag/${TagKey} rds:cluster-tag/${TagKey}
shardgrp	`arn:${Partition}:rds:${Region}:${Account}:shard-group:${DbShardGroupResourceId}`	aws:ResourceTag/${TagKey}
cluster-auto-backup	`arn:${Partition}:rds:${Region}:${Account}:cluster-auto-backup:${DbClusterAutomatedBackupId}`	aws:ResourceTag/${TagKey}
auto-backup	`arn:${Partition}:rds:${Region}:${Account}:auto-backup:${DbInstanceAutomatedBackupId}`	aws:ResourceTag/${TagKey}
cluster-endpoint	`arn:${Partition}:rds:${Region}:${Account}:cluster-endpoint:${DbClusterEndpoint}`	aws:ResourceTag/${TagKey}
cluster-pg	`arn:${Partition}:rds:${Region}:${Account}:cluster-pg:${ClusterParameterGroupName}`	aws:ResourceTag/${TagKey} rds:cluster-pg-tag/${TagKey}

Resource types	ARN	Condition keys
cluster-snapshot	arn:${Partition}:rds:${Region}:${Account}:cluster-snapshot:${ClusterSnapshotName}	aws:ResourceTag/${TagKey} rds:cluster-snapshot-tag/${TagKey}
db	arn:${Partition}:rds:${Region}:${Account}:db:${DbInstanceName}	aws:ResourceTag/${TagKey} rds:DatabaseClass rds:DatabaseEngine rds:DatabaseName rds:MultiAz rds:Piops rds:StorageEncrypted rds:StorageSize rds:Vpc rds:db-tag/${TagKey}
es	arn:${Partition}:rds:${Region}:${Account}:es:${SubscriptionName}	aws:ResourceTag/${TagKey} rds:es-tag/${TagKey}
global-cluster	arn:${Partition}:rds::${Account}:global-cluster:${GlobalCluster}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
og	arn:${Partition}:rds:${Region}:${Account}:og:${OptionGroupName}	aws:ResourceTag/${TagKey} rds:og-tag/${TagKey}
pg	arn:${Partition}:rds:${Region}:${Account}:pg:${ParameterGroupName}	aws:ResourceTag/${TagKey} rds:pg-tag/${TagKey}
proxy	arn:${Partition}:rds:${Region}:${Account}:db-proxy:${DbProxyId}	aws:ResourceTag/${TagKey}
proxy-endpoint	arn:${Partition}:rds:${Region}:${Account}:db-proxy-endpoint:${DbProxyEndpointId}	aws:ResourceTag/${TagKey}
ri	arn:${Partition}:rds:${Region}:${Account}:ri:${ReservedDbInstanceName}	aws:ResourceTag/${TagKey} rds:ri-tag/${TagKey}
secgrp	arn:${Partition}:rds:${Region}:${Account}:secgrp:${SecurityGroupName}	aws:ResourceTag/${TagKey} rds:secgrp-tag/${TagKey}
snapshot	arn:${Partition}:rds:${Region}:${Account}:snapshot:${SnapshotName}	aws:ResourceTag/${TagKey} rds:snapshot-tag/${TagKey}

Resource types	ARN	Condition keys
subgrp	arn:${Partition}:rds:${Region}:${Account}:subgrp:${SubnetGroupName}	aws:ResourceTag/${TagKey} rds:subgrp-tag/${TagKey}
target-group	arn:${Partition}:rds:${Region}:${Account}:target-group:${TargetGroupId}	aws:ResourceTag/${TagKey}
cev	arn:${Partition}:rds:${Region}:${Account}:cev:${Engine}/${EngineVersion}/${CustomDbEngineVersionId}	aws:ResourceTag/${TagKey}
deployment	arn:${Partition}:rds:${Region}:${Account}:deployment:${BlueGreenDeploymentIdentifier}	aws:ResourceTag/${TagKey}
integration	arn:${Partition}:rds:${Region}:${Account}:integration:${IntegrationIdentifier}	aws:ResourceTag/${TagKey}
snapshot-tenant-database	arn:${Partition}:rds:${Region}:${Account}:snapshot-tenant-database:${SnapshotName}:${TenantResourceId}	aws:ResourceTag/${TagKey}
tenant-database	arn:${Partition}:rds:${Region}:${Account}:tenant-database:${TenantResourceId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon RDS

Amazon RDS defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the set of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by the set of tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the set of tag keys in the request	ArrayOfString
rds:BackupTarget	Filters access by the type of backup target. One of: region, outposts	String
rds:CopyOptionGroup	Filters access by the value that specifies whether the CopyDBSnapshot action requires copying the DB option group	Bool
rds:DatabaseClass	Filters access by the type of DB instance class	String
rds:DatabaseEngine	Filters access by the database engine. For possible values refer to the engine parameter in CreateDBInstance API	String
rds:DatabaseName	Filters access by the user-defined name of the database on the DB instance	String
rds:EndpointType	Filters access by the type of the endpoint. One of: READER, WRITER, CUSTOM	String
rds:ManageMasterUserPassword	Filters access by the value that specifies whether RDS manages master user password in AWS Secrets Manager for the DB instance or cluster	Bool

Condition keys	Description	Type
rds:MultiAz	Filters access by the value that specifies whether the DB instance runs in multiple Availability Zones. To indicate that the DB instance is using Multi-AZ, specify true	Bool
rds:Piops	Filters access by the value that contains the number of Provisioned IOPS (PIOPS) that the instance supports. To indicate a DB instance that does not have PIOPS enabled, specify 0	Numeric
rds:PubliclyAccessible	Filters access by the value that specifies whether the DB Instance or DB ShardGroup is publicly accessible	Bool
rds:StorageEncrypted	Filters access by the value that specifies whether the DB instance storage should be encrypted. To enforce storage encryption, specify true	Bool
rds:StorageSize	Filters access by the storage volume size (in GB)	Numeric
rds:TenantDatabaseName	Filters access by the tenant database name in CreateTenantDatabase and by the new tenant database name in ModifyTenantDatabase	String
rds:Vpc	Filters access by the value that specifies whether the DB instance runs in an Amazon Virtual Private Cloud (Amazon VPC). To indicate that the DB instance runs in an Amazon VPC, specify true	Bool
rds:cluster-pg-tag/${TagKey}	Filters access by the tag attached to a DB cluster parameter group	String
rds:cluster-snapshot-tag/${TagKey}	Filters access by the tag attached to a DB cluster snapshot	String
rds:cluster-tag/${TagKey}	Filters access by the tag attached to a DB cluster	String

Condition keys	Description	Type
rds:db-tag/${TagKey}	Filters access by the tag attached to a DB instance	String
rds:es-tag/${TagKey}	Filters access by the tag attached to an event subscription	String
rds:og-tag/${TagKey}	Filters access by the tag attached to a DB option group	String
rds:pg-tag/${TagKey}	Filters access by the tag attached to a DB parameter group	String
rds:req-tag/${TagKey}	Filters access by the set of tag keys and values that can be used to tag a resource	String
rds:ri-tag/${TagKey}	Filters access by the tag attached to a reserved DB instance	String
rds:secgrp-tag/${TagKey}	Filters access by the tag attached to a DB security group	String
rds:snapshot-tag/${TagKey}	Filters access by the tag attached to a DB snapshot	String
rds:subgrp-tag/${TagKey}	Filters access by the tag attached to a DB subnet group	String

Actions, resources, and condition keys for AWS Resource Access Manager (RAM)

AWS Resource Access Manager (RAM) (service prefix: `ram`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.

- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Resource Access Manager (RAM)
- Resource types defined by AWS Resource Access Manager (RAM)
- Condition keys for AWS Resource Access Manager (RAM)

Actions defined by AWS Resource Access Manager (RAM)

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptResourceShareInvitation	Grants permission to accept the specified resource share invitation	Write	resource-share-invitation*		
				ram:ShareOwnerAccountId ram:ResourceShareName	
AssociateResourceShare	Grants permission to associate resource(s) and/or principal(s) to a resource share	Write	resource-share*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:Principal ram:RequestedResourceType ram:ResourceArn	
AssociateResourceSharePermission	Grants permission to associate a Permission with a Resource Share	Write	customer-managed-permission*		
			permission*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			resource-share*		
CreatePermission	Grants permission to create a Permission that can be associated to a Resource Share	Write		ram:PermissionArn ram:PermissionResourceType aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	ram:TagResource
CreatePermissionVersion	Grants permission to create a new version of a Permission that can be associated to a Resource Share	Write	customer-managed-permission*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ram:PermissionArn ram:PermissionResourceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateResourceShare	Grants permission to create a resource share with provided resource(s) and/or principal(s)	Write		aws:RequestTag/${TagKey} aws:TagKeys ram:RequestedResourceType ram:ResourceArn ram:RequestedAllowsExternalPrincipals ram:Principal ram:AllowsExternalPrincipals	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePermission	Grants permission to delete a specified Permission	Write	customer-managed-permission*		
				aws:ResourceTag/${TagKey} ram:PermissionArn ram:PermissionResourceType	
DeletePermissionVersion	Grants permission to delete a specified version of a permission	Write	customer-managed-permission*		
				ram:PermissionArn ram:PermissionResourceType	
DeleteResourceShare	Grants permission to delete resource share	Write	resource-share*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals	
DisassociateResourceShare	Grants permission to disassociate resource(s) and/or principal(s) from a resource share	Write	resource-share*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:Principal ram:RequestedResourceType ram:ResourceArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateResourceSharePermission	Grants permission to disassociate a Permission from a Resource Share	Write	customer-managed-permission*		
			permission*		
			resource-share*		
EnableSharingWithAwsOrganization	Grants permission to access customer's organization and create a SLR in the customer's account	Permissions management			iam:CreateServiceLinkedRole organizations:DescribeOrganization organizations:EnableAWSServiceAccess
GetPermission	Grants permission to get the contents of an AWS RAM permission	Read	customer-managed-permission*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			permission*		
				ram:PermissionArn	
GetResourcePolicies	Grants permission to get the policies for the specified resources that you own and have shared	Read			
GetResourceShareAssociations	Grants permission to get a set of resource share associations from a provided list or with a specified status of the specified type	Read			
GetResourceShareInvitations	Grants permission to get resource share invitations by the specified invitation arn or those for the resource share	Read			
GetResourceShares	Grants permission to get a set of resource shares from a provided list or with a specified status	Read		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPendingInvitationResources	Grants permission to list the resources in a resource share that is shared with you but that the invitation is still pending for	Read	resource-share-invitation*		
				ram:ResourceShareName	
ListPermissionAssociations	Grants permission to list information about the permission and any associations	List	customer-managed-permission*		
			permission*		
				ram:PermissionArn ram:PermissionResourceType	
ListPermissionVersions	Grants permission to list the versions of an AWS RAM permission	List			
ListPermissions	Grants permission to list the AWS RAM permissions	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPrincipals	Grants permission to list the principals that you have shared resources with or that have shared resources with you	List			
ListReplacePermissionAssociationsWork	Grants permission to retrieve the status of the asynchronous permission replacement	List			
ListResourceSharePermissions	Grants permission to list the Permissions associated with a Resource Share	List	resource-share*		
				aws:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals	
ListResourceTypes	Grants permission to list the shareable resource types supported by AWS RAM	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResources	Grants permission to list the resources that you added to resource shares or the resources that are shared with you	List			
PromotePermissionCreatedFromPolicy	Grants permission to create a separate, fully manageable customer managed permission	Write	customer-managed-permission*		
				ram:PermissionArn ram:PermissionResourceType	
PromoteResourceShareCreatedFromPolicy	Grants permission to promote the specified resource share	Write	resource-share*		
RejectResourceShareInvitation	Grants permission to reject the specified resource share invitation	Write	resource-share-invitation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ram:ShareOwnerAccountId ram:ResourceShareName	
ReplacePermissionAssociations	Grants permission to update all resource shares to a new permission	Write	customer-managed-permission*		
			permission*		
				ram:PermissionArn ram:PermissionResourceType	
SetDefaultPermissionVersion	Grants permission to specify a version number as the default version for the respective customer managed permission	Write	customer-managed-permission*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ram:PermissionArn ram:PermissionResourceType	
TagResource	Grants permission to tag the specified resource share or permission	Tagging	customer-managed-permission		
			resource-share		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag the specified resource share or permission	Tagging	customer-managed-permission		
			resource-share		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateResourceShare	Grants permission to update attributes of the resource share	Write	resource-share*		
				aws:ResourceTag/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals ram:RequestedAllowsExternalPrincipals	

Resource types defined by AWS Resource Access Manager (RAM)

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you

can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
resource-share	arn:${Partition}:ram:${Region}:${Account}:resource-share/${ResourcePath}	aws:ResourceTag/${TagKey} ram:AllowsExternalPrincipals ram:ResourceShareName
resource-share-invitation	arn:${Partition}:ram:${Region}:${Account}:resource-share-invitation/${ResourcePath}	ram:ShareOwnerAccountId
permission	arn:${Partition}:ram::${Account}:permission/${ResourcePath}	ram:PermissionArn ram:PermissionResourceType
customer-managed-permission	arn:${Partition}:ram:${Region}:${Account}:permission/${ResourcePath}	aws:ResourceTag/${TagKey} ram:PermissionArn ram:PermissionResourceType

Condition keys for AWS Resource Access Manager (RAM)

AWS Resource Access Manager (RAM) defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request when creating or tagging a resource share. If users don't pass these specific tags, or if they don't specify tags at all, the request fails	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed when creating or tagging a resource share	ArrayOfString
ram:AllowsExternalPrincipals	Filters access by resource shares that allow or deny sharing with external principals. For example, specify true if the action can only be performed on resource shares that allow sharing with external principals. External principals are AWS accounts that are outside of its AWS organization	Bool
ram:PermissionArn	Filters access by the specified Permission ARN	ARN
ram:PermissionResourceType	Filters access by permissions of specified resource type	String
ram:Principal	Filters access by format of the specified principal	String
ram:RequestedAllowsExternalPrincipals	Filters access by the specified value for 'allowExternalPrincipals'. External principals are AWS accounts that are outside of its AWS Organization	Bool

Condition keys	Description	Type
ram:RequestedResourceType	Filters access by the specified resource type	String
ram:ResourceArn	Filters access by the specified ARN	ARN
ram:ResourceShareName	Filters access by a resource share with the specified name	String
ram:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
ram:ShareOwnerAccountId	Filters access by resource shares owned by a specific account. For example, you can use this condition key to specify which resource share invitations can be accepted or rejected based on the resource share owner's account ID	String

Actions, resources, and condition keys for Amazon Resource Group Tagging API

Amazon Resource Group Tagging API (service prefix: `tag`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Resource Group Tagging API

- Resource types defined by Amazon Resource Group Tagging API
- Condition keys for Amazon Resource Group Tagging API

Actions defined by Amazon Resource Group Tagging API

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeReportCreation	Grants permission to describe the status of the StartReportCreation operation	Read			
GetComplianceSummary	Grants permission to retrieve a summary of how many resources are noncompliant with their effective tag policies	Read			
GetResources	Grants permission to return tagged or previously tagged resources in the specified AWS Region for the calling account	Read			
GetTagKeys	Grants permission to returns tag keys currently in use in the specified AWS Region for the calling account	Read			
GetTagValues	Grants permission to return tag values for the specified	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	key that are used in the specified AWS Region for the calling account				
ListRequiredTags	Grants permission to list required tags for supported resource types in the calling account	List			
StartReportCreation	Grants permission to start generating a report listing all tagged resources in accounts across your organization, and whether each resource is compliant with the effective tag policy	Write			
TagResources	Grants permission to apply one or more tags to the specified resources	Tagging			
UntagResources	Grants permission to remove the specified tags from the specified resources	Tagging			

Resource types defined by Amazon Resource Group Tagging API

Amazon Resource Group Tagging API does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Resource Group Tagging API, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Resource Group Tagging API

Resource Group Tagging has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Resource Groups

AWS Resource Groups (service prefix: `resource-groups`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Resource Groups
- Resource types defined by AWS Resource Groups
- Condition keys for AWS Resource Groups

Actions defined by AWS Resource Groups

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which

the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate Resource [permission only]	Grants permission to associate a resource to an Application	Write	group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelTagSyncTask	Grants permission to cancel a tag-sync task for an application group	Write	group*		resource-groups:DeleteGroup
CreateGroup	Grants permission to create a resource group with a specified name, description, and resource query	Write		aws:RequestTag/${TagKey} aws:TagKeys	cloudformation:DescribeStacks
DeleteGroup	Grants permission to delete a specified resource group	Write	group*		tag:GetResources
DeleteGroupPolicy [permission only]	Grants permission to delete a resource-based policy for the specified group	Write	group*		
DisassociateResource [permission only]	Grants permission to disassociate a resource from an Application	Write	group*		
GetAccountSettings	Grants permission to get the current status of optional features in Resource Groups	Read			
GetGroup	Grants permission to get information of a specified resource group	Read	group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetGroupConfiguration	Grants permission to get the service configuration associated with the specified resource group	Read	group*		
GetGroupPolicy [permission only]	Grants permission to get a resource-based policy for the specified group	Read	group*		
GetGroupQuery	Grants permission to get the query associated with a specified resource group	Read	group*		
GetTagSyncTask	Grants permission to get information of a specified tag-sync task	Read	group*		
GetTags	Grants permission to get the tags associated with a specified resource group	Read	group*		
GroupResources	Grants permission to add the specified resources to the specified group	Write	group*		resource-groups:Tag tag:TagResources

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListGroupResources	Grants permission to list the resources that are members of a specified resource group	List	group*		cloudformation:DescribeStacks cloudformation:ListStackResources tag:GetResources
ListGroupingStatuses	Grants permission to list grouping statuses for a specified application group	List	group*		
ListGroups	Grants permission to list all resource groups in your account	List			
ListResourceTypes [permission only]	Grants permission to list supported resource types	List			
ListTagSyncTasks	Grants permission to list all tag-sync tasks in your account	List	group*		
PutGroupConfiguration	Grants permission to put the service configuration associated with the specified resource group	Write	group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutGroupPolicy [permission only]	Grants permission to add a resource-based policy for the specified group	Write	group*		
SearchResources	Grants permission to search for AWS resources matching the given query	List			cloudformation:DescribeStacks cloudformation:ListStackResources tag:GetResources
StartTagSyncTask	Grants permission to create a tag-sync task for an application group	Write	group*		iam:PassRole resource-groups:CreateGroup
Tag	Grants permission to tag a specified resource group	Tagging	group*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UngroupResources	Grants permission to remove the specified resources from the specified group	Write	group*		resource-groups:Untag tag:UntagResources
Untag	Grants permission to remove tags associated with a specified resource group	Tagging	group*		
				aws:TagKeys	
UpdateAccountSettings	Grants permission to update optional features in Resource Groups	Write			
UpdateGroup	Grants permission to update a specified resource group	Write	group*		
UpdateGroupQuery	Grants permission to update the query associated with a specified resource group	Write	group*		cloudformation:DescribeStacks

Resource types defined by AWS Resource Groups

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
group	arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}	aws:ResourceTag/${TagKey}
tagSyncTask	arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}/tag-sync-task/${TaskId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Resource Groups

AWS Resource Groups defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Route 53

Amazon Route 53 (service prefix: route53) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Route 53
- Resource types defined by Amazon Route 53
- Condition keys for Amazon Route 53

Actions defined by Amazon Route 53

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ActivateKeySigningKey	Grants permission to activate a key-signing key so that it can be used for signing by DNSSEC	Write	hostedzone*		
AssociateVPCWithHostedZone	Grants permission to associate an additional Amazon VPC with a private hosted zone	Write	hostedzone		ec2:DescribeVpcs
				route53:VPCs	
ChangeCidrCollection	Grants permission to create or delete CIDR blocks within a CIDR collection	Write	cidrcollection*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ChangeResourceRecordSets	Grants permission to create, update, or delete a record, which contains authoritative DNS information for a specified domain or subdomain name	Write	hostedzone*		
				route53:ChangeResourceRecordSetsNormalizedRecordNames route53:ChangeResourceRecordSetsRecordTypes route53:ChangeResourceRecordSetsActions	
ChangeTagsForResource	Grants permission to add, edit, or delete tags for a health check or a hosted zone	Tagging	healthcheck*		
			hostedzone*		
CreateCidrCollection	Grants permission to create a new CIDR collection	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateHealthCheck	Grants permission to create a new health check, which monitors the health and performance of your web applications, web servers, and other resources	Write			
CreateHostedZone	Grants permission to create a public hosted zone, which you use to specify how the Domain Name System (DNS) routes traffic on the Internet for a domain, such as example.com, and its subdomains	Write		route53:VPCs	ec2:DescribeVpcs
CreateKeySigningKey	Grants permission to create a new key-signing key associated with a hosted zone	Write	hostedzone*		
CreateQueryLoggingConfig	Grants permission to create a configuration for DNS query logging	Write	hostedzone*		
CreateReusableDelegationSet	Grants permission to create a delegation set (a group of four name servers) that can be reused by multiple hosted zones	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTrafficPolicy	Grants permission to create a traffic policy, which you use to create multiple DNS records for one domain name (such as example.com) or one subdomain name (such as www.example.com)	Write			
CreateTrafficPolicyInstance	Grants permission to create records in a specified hosted zone based on the settings in a specified traffic policy version	Write	hostedzone* trafficpolicy*		
CreateTrafficPolicyVersion	Grants permission to create a new version of an existing traffic policy	Write	trafficpolicy*		
CreateVPCAssociationAuthorization	Grants permission to authorize the AWS account that created a specified VPC to submit an Associate VPCWithHostedZone request, which associates the VPC with a specified hosted zone that was created by a different account	Write	hostedzone* 	 route53:VPCs	
DeactivateKeySigningKey	Grants permission to deactivate a key-signing key so that it will not be used for signing by DNSSEC	Write	hostedzone*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCidrCollection	Grants permission to delete a CIDR collection	Write	cidrcollection*		
DeleteHealthCheck	Grants permission to delete a health check	Write	healthcheck*		
DeleteHostedZone	Grants permission to delete a hosted zone	Write	hostedzone*		
DeleteKeySigningKey	Grants permission to delete a key-signing key	Write	hostedzone*		
DeleteQueryLoggingConfig	Grants permission to delete a configuration for DNS query logging	Write	queryloggingconfig*		
DeleteReusableDelegationSet	Grants permission to delete a reusable delegation set	Write	delegationset*		
DeleteTrafficPolicy	Grants permission to delete a traffic policy	Write	trafficpolicy*		
DeleteTrafficPolicyInstance	Grants permission to delete a traffic policy instance and all the records that Route 53 created when you created the instance	Write	trafficpolicyinstance*		
DeleteVPCAssociationAuthorization	Grants permission to remove authorization for associating an Amazon Virtual Private Cloud with a Route 53 private hosted zone	Write	hostedzone*		
				route53:VPCs	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableHostedZoneDNSSEC	Grants permission to disable DNSSEC signing in a specific hosted zone	Write	hostedzone*		
DisassociateVPCFromHostedZone	Grants permission to disassociate an Amazon Virtual Private Cloud from a Route 53 private hosted zone	Write	hostedzone		ec2:DescribeVpcs
				route53:VPCs	
EnableHostedZoneDNSSEC	Grants permission to enable DNSSEC signing in a specific hosted zone	Write	hostedzone*		
GetAccountLimit	Grants permission to get the specified limit for the current account, for example, the maximum number of health checks that you can create using the account	Read			
GetChange	Grants permission to get the current status of a request to create, update, or delete one or more records	List	change*		
GetCheckerIpRanges	Grants permission to get a list of the IP ranges that are used by Route 53 health checkers to check the health of your resources	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDNSSEC	Grants permission to get information about DNSSEC for a specific hosted zone, including the key-signing keys in the hosted zone	Read	hostedzone*		
GetGeoLocation	Grants permission to get information about whether a specified geographic location is supported for Route 53 geolocation records	List			
GetHealthCheck	Grants permission to get information about a specified health check	Read	healthcheck*		
GetHealthCheckCount	Grants permission to get the number of health checks that are associated with the current AWS account	List			
GetHealthCheckLastFailureReason	Grants permission to get the reason that a specified health check failed most recently	List	healthcheck*		
GetHealthCheckStatus	Grants permission to get the status of a specified health check	List	healthcheck*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetHostedZone	Grants permission to get information about a specified hosted zone including the four name servers that Route 53 assigned to the hosted zone	List	hostedzone*		
GetHostedZoneCount	Grants permission to get the number of hosted zones that are associated with the current AWS account	List			
GetHostedZoneLimit	Grants permission to get the specified limit for a specified hosted zone	Read	hostedzone*		
GetQueryLoggingConfig	Grants permission to get information about a specified configuration for DNS query logging	Read	queryloggingconfig*		
GetReusableDelegationSet	Grants permission to get information about a specified reusable delegation set, including the four name servers that are assigned to the delegation set	List	delegationset*		
GetReusableDelegationSetLimit	Grants permission to get the maximum number of hosted zones that you can associate with the specified reusable delegation set	Read	delegationset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTrafficPolicy	Grants permission to get information about a specified traffic policy version	Read	trafficpolicy*		
GetTrafficPolicyInstance	Grants permission to get information about a specified traffic policy instance	Read	trafficpolicyinstance*		
GetTrafficPolicyInstanceCount	Grants permission to get the number of traffic policy instances that are associated with the current AWS account	Read			
ListCidrBlocks	Grants permission to get a list of the CIDR blocks within a specified CIDR collection	List	cidrcollection*		
ListCidrCollections	Grants permission to get a list of the CIDR collections that are associated with the current AWS account	List			
ListCidrLocations	Grants permission to get a list of the CIDR locations that belong to a specified CIDR collection	List	cidrcollection*		
ListGeoLocations	Grants permission to get a list of geographic locations that Route 53 supports for geolocation	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListHealthChecks	Grants permission to get a list of the health checks that are associated with the current AWS account	Read			
ListHostedZones	Grants permission to get a list of the public and private hosted zones that are associated with the current AWS account	List			
ListHostedZonesByName	Grants permission to get a list of your hosted zones in lexicographic order. Hosted zones are sorted by name with the labels reversed, for example, com.example.www	List			
ListHostedZonesByVPC	Grants permission to get a list of all the private hosted zones that a specified VPC is associated with	List		route53:VPCs	ec2:DescribeVpcs
ListQueryLoggingConfigs	Grants permission to list the configurations for DNS query logging that are associated with the current AWS account or the configuration that is associated with a specified hosted zone	List	hostedzone		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResourceRecordSets	Grants permission to list the records in a specified hosted zone	List	hostedzone*		
ListReusableDelegationSets	Grants permission to list the reusable delegation sets that are associated with the current AWS account.	Read			
ListTagsForResource	Grants permission to list tags for one health check or hosted zone	Read	healthcheck		
			hostedzone		
ListTagsForResources	Grants permission to list tags for up to 10 health checks or hosted zones	Read	healthcheck		
			hostedzone		
ListTrafficPolicies	Grants permission to get information about the latest version for every traffic policy that is associated with the current AWS account. Policies are listed in the order in which they were created	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTrafficPolicyInstances	Grants permission to get information about the traffic policy instances that you created by using the current AWS account	Read			
ListTrafficPolicyInstancesByHostedZone	Grants permission to get information about the traffic policy instances that you created in a specified hosted zone	List	hostedzone*		
ListTrafficPolicyInstancesByPolicy	Grants permission to get information about the traffic policy instances that you created using a specified traffic policy version	List	trafficpolicy*		
ListTrafficPolicyVersions	Grants permission to get information about all the versions for a specified traffic policy	List	trafficpolicy*		
ListVPCAssociationAuthorizations	Grants permission to get a list of the VPCs that were created by other accounts and that can be associated with a specified hosted zone	List	hostedzone*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TestDNSAnswer	Grants permission to get the value that Route 53 returns in response to a DNS query for a specified record name and type	Read			
UpdateHealthCheck	Grants permission to update an existing health check	Write	healthcheck*		
UpdateHostedZoneComment	Grants permission to update the comment for a specified hosted zone	Write	hostedzone*		
UpdateHostedZoneFeatures	Grants permission to update features for a specified hosted zone	Write	hostedzone*		
UpdateTrafficPolicyComment	Grants permission to update the comment for a specified traffic policy version	Write	trafficpolicy*		
UpdateTrafficPolicyInstance	Grants permission to update the records in a specified hosted zone that were created based on the settings in a specified traffic policy version	Write	trafficpolicyinstance*		

Resource types defined by Amazon Route 53

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you

can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
cidrcollection	arn:${Partition}:route53:::cidrcollection/${Id}	
change	arn:${Partition}:route53:::change/${Id}	
delegationset	arn:${Partition}:route53:::delegationset/${Id}	
healthcheck	arn:${Partition}:route53:::healthcheck/${Id}	
hostedzone	arn:${Partition}:route53:::hostedzone/${Id}	
trafficpolicy	arn:${Partition}:route53:::trafficpolicy/${Id}	
trafficpolicyinstance	arn:${Partition}:route53:::trafficpolicyinstance/${Id}	
queryloggingconfig	arn:${Partition}:route53:::queryloggingconfig/${Id}	
vpc	arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}	

Condition keys for Amazon Route 53

Amazon Route 53 defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
route53:ChangeResourceRecordSetsActions	Filters access by the change actions, CREATE, UPSERT, or DELETE, in a ChangeResourceRecordSets request	ArrayOfString
route53:ChangeResourceRecordSetsNormalizedRecordNames	Filters access by the normalized DNS record names in a ChangeResourceRecordSets request	ArrayOfString
route53:ChangeResourceRecordSetsRecordTypes	Filters access by the DNS record types in a ChangeResourceRecordSets request	ArrayOfString
route53:VPCs	Filters access by VPCs in request	String

Actions, resources, and condition keys for Amazon S3

Amazon S3 (service prefix: s3) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon S3
- Resource types defined by Amazon S3
- Condition keys for Amazon S3

Actions defined by Amazon S3

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AbortMultipartUpload	Grants permission to abort a multipart upload	Write	accesspointobject		
			object		
				s3:AccessGrantsInstanceArn s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-content-sha256	
AssociateAccessGrantsIdentityCenter	Grants permission to associate Access Grants identity center	Permissions management	accessgrantsinstance*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BypassGovernanceRetention	Grants permission to allow circumvention of governance-mode object retention settings	Permissions management	accesspointobject object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:RequestObjectTag/<key> s3:RequestObjectTagKeys s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-acl s3:x-amz-content-sha256 s3:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				copy-source s3:x-amz-grant-full-control s3:x-amz-grant-read s3:x-amz-grant-read-acp s3:x-amz-grant-write s3:x-amz-grant-write-acp s3:x-amz-metadata-directive	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-server-side-encryption s3:x-amz-server-side-encryption-aws-kms-key-id s3:x-amz-server-side-encryption-customer-algorithm s3:x-amz-storage-class s3:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				website-redirect-location	
CreateAccessGrant	Grants permission to create Access Grant	Permissions management	accessgrantslocation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantScope s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateAccessGrantsInstance	Grants permission to Create Access Grants Instance	Permissions management	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAccessGrantsLocation	Grants permission to create Access Grants location	Permissions management	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsLocationScope s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey} aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
CreateAccessPoint	Grants permission to create a new access point	Write	accesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:locationconstraint s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-acl	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-content-sha256 s3:AccessPointTag/${TagKey} aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateAccessPointForObjectLambda	Grants permission to create an object lambda enabled accesspoint	Write	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBucket	Grants permission to create a new bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:locationconstraint s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-acl s3:x-amz-content-sha256 s3:x-amz-grant-full-control	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-grant-read s3:x-amz-grant-read-acp s3:x-amz-grant-write s3:x-amz-grant-write-acp s3:x-amz-object-ownership aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBucketMetadataTableConfiguration	Grants permission to create a new S3 Metadata configuration for a specified general purpose bucket	Write	bucket*		kms:DescribeKey s3tables:CreateNamespace s3tables:CreateTable s3tables:CreateTableBucket s3tables:GetTable s3tables:PutTableBucketPolicy s3tables:PutTableEncryption s3tables:PutTablePolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateJob	Grants permission to create a new Amazon S3 Batch Operations job	Write		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:RequestJobPriority s3:RequestJobOperation aws:TagKeys aws:RequestTag/	iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey}	
CreateMultiRegionAccessPoint	Grants permission to create a new Multi-Region Access Point	Write	multiregionaccesspoint*		
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateStorageLensGroup	Grants permission to create an Amazon S3 Storage Lens group	Write		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessGrant	Grants permission to delete Access Grant	Permissions management	accessgrant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantScope s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
DeleteAccessGrantsInstance	Grants permission to Delete Access Grants Instance	Permissions management	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
DeleteAccessGrantsInstanceResourcePolicy	Grants permission to read Access grants instance resource policy	Permissions management	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
DeleteAccessGrantsLocation	Grants permission to delete Access Grants location	Permissions management	accessgrantslocation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsLocationScope s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
DeleteAccessPoint	Grants permission to delete the access point named in the URI	Write	accesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessPointTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteAccessPointForObjectLambda	Grants permission to delete the object lambda enabled access point named in the URI	Write	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAccessPointPolicy	Grants permission to delete the policy on a specified access point	Permissions management	accesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessPointTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteAccessPointPolicyForObjectLambda	Grants permission to delete the policy on a specified object lambda enabled access point	Permissions management	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBucket	Grants permission to delete the bucket named in the URI	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBucketMetadataTableConfiguration	Grants permission to delete the S3 Metadata configuration for a specified general purpose bucket	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBucketPolicy	Grants permission to delete the policy on a specified bucket	Permissions management	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
DeleteBucketWebsite	Grants permission to remove the website configuration for a bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
DeleteJobTagging	Grants permission to remove tags from an existing Amazon S3 Batch Operations job	Tagging	job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:ExistingJobPriority s3:ExistingJobOperation	
DeleteMultiRegionAccessPoint	Grants permission to delete the Multi-Region Access Point named in the URI	Write	multiregionaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
DeleteObject	Grants permission to remove the null version of an object and insert a delete marker, which becomes the current version of the object	Write	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:if-match	
DeleteObjectTagging	Grants permission to use the tagging subresource to remove the entire tag set from the specified object	Tagging	accesspointobject object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
DeleteObjectVersion	Grants permission to remove a specific version of an object	Write	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-content-sha256	
DeleteObjectVersionTagging	Grants permission to remove the entire tag set for a specific version of the object	Tagging	accesspointobject object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-content-sha256	
DeleteStorageLensConfiguration	Grants permission to delete an existing Amazon S3 Storage Lens configuration	Write	storagelensconfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
DeleteStorageLensConfigurationTagging	Grants permission to remove tags from an existing Amazon S3 Storage Lens configuration	Tagging	storagelensconfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
DeleteStorageLensGroup	Grants permission to delete an existing S3 Storage Lens group	Write	storagelensgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeJob	Grants permission to retrieve the configuration parameters and status for a batch operations job	Read	job*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
DescribeMultiRegionAccessPointOperation	Grants permission to retrieve the configurations for a Multi-Region Access Point	Read	multiregionaccesspointrequestarn*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
DissociateAccessGrantsIdentityCenter	Grants permission to disassociate Access Grants identity center	Permissions management	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccelerateConfiguration	Grants permission to uses the accelerate subresource to return the Transfer Acceleration state of a bucket, which is either Enabled or Suspended	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetAccessGrant	Grants permission to read Access Grant	Read	accessgrant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantScope s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
GetAccessGrantsInstance	Grants permission to Read Access Grants Instance	Read	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
GetAccessGrantsInstanceForPrefix	Grants permission to Read Access Grants Instance by prefix	Read	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
GetAccessGrantsInstanceResourcePolicy	Grants permission to read Access grants instance resource policy	Read	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
GetAccessGrantsLocation	Grants permission to read Access Grants location	Read	accessgrantslocation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsLocationScope s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccessPoint	Grants permission to return configuration information about the specified access point	Read		s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessPointTag/${TagKey} aws:ResourceTag/${TagKey}	
GetAccessPointConfigurationForObjectLambda	Grants permission to retrieve the configuration of the object lambda enabled access point	Read	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccessPointForObjectLambda	Grants permission to create an object lambda enabled accesspoint	Read	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccessPointPolicy	Grants permission to return the access point policy associated with the specified access point	Read	accesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessPointTag/${TagKey} aws:ResourceTag/${TagKey}	
GetAccessPointPolicyForObjectLambda	Grants permission to return the access point policy associated with the specified object lambda enabled access point	Read	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccessPointPolicyStatus	Grants permission to return the policy status for a specific access point policy	Read	accesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessPointTag/${TagKey} aws:ResourceTag/${TagKey}	
GetAccessPointPolicyStatusForObjectLambda	Grants permission to return the policy status for a specific object lambda access point policy	Read	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccountPublicAccessBlock	Grants permission to retrieve the PublicAccessBlock configuration for an AWS account	Read		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAnalyticsConfiguration	Grants permission to get an analytics configuration from an Amazon S3 bucket, identified by the analytics configuration ID	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketAbac	Grants permission to retrieve ABAC configuration for a general purpose bucket	Read	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketAcl	Grants permission to use the acl subresource to return the access control list (ACL) of an Amazon S3 bucket	Read	accesspoint		
			bucket		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketCORS	Grants permission to return the CORS configuration information set for an Amazon S3 bucket	Read	accesspoint bucket		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketLocation	Grants permission to return the Region that an Amazon S3 bucket resides in	Read	accesspoint		
			bucket		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBucketLogging	Grants permission to return the logging status of an Amazon S3 bucket and the permissions users have to view or modify that status	Read	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBucketMetadataTableConfiguration	Grants permission to return the S3 Metadata configuration for a specified general purpose bucket	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketNotification	Grants permission to get the notification configuration of an Amazon S3 bucket	Read	accesspoint		
			bucket		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBucketObjectLockConfiguration	Grants permission to get the Object Lock configuration of an Amazon S3 bucket	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:signatureversion	
GetBucketOwnershipControls	Grants permission to retrieve ownership controls on a bucket	Read	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketPolicy	Grants permission to return the policy of the specified bucket	Read	accesspoint		
			bucket		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBucketPolicyStatus	Grants permission to retrieve the policy status for a specific Amazon S3 bucket, which indicates whether the bucket is public	Read	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBucketPublicAccessBlock	Grants permission to retrieve the PublicAccessBlock configuration for an Amazon S3 bucket	Read	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBucketRequestPayment	Grants permission to return the request payment configuration for an Amazon S3 bucket	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketTagging	Grants permission to return the tag set associated with an Amazon S3 bucket	Read	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketVersioning	Grants permission to return the versioning state of an Amazon S3 bucket	Read	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetBucketWebsite	Grants permission to return the website configuration for an Amazon S3 bucket	Read	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetDataAccess	Grants permission to get Access	Read	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEncryptionConfiguration	Grants permission to return the default encryption configuration an Amazon S3 bucket	Read	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIntelligentTieringConfiguration	Grants permission to get an or list all Amazon S3 Intelligent Tiering configuration in a S3 Bucket	Read	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInventoryConfiguration	Grants permission to return an inventory configuration from an Amazon S3 bucket, identified by the inventory configuration ID	Read	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetJobTagging	Grants permission to return the tag set of an existing Amazon S3 Batch Operations job	Read	job*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLifecycleConfiguration	Grants permission to return the lifecycle configuration information set on an Amazon S3 bucket	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetMetricsConfiguration	Grants permission to get a metrics configuration from an Amazon S3 bucket	Read	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetMultiRegionAccessPoint	Grants permission to return configuration information about the specified Multi-Region Access Point	Read	multiregionaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
GetMultiRegionAccessPointPolicy	Grants permission to return the access point policy associated with the specified Multi-Region Access Point	Read	multiregionaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
GetMultiRegionAccessPointPolicyStatus	Grants permission to return the policy status for a specific Multi-Region Access Point policy	Read	multiregionaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
GetMultiRegionAccessPointRoutes	Grants permission to return the route configuration for a Multi-Region Access Point	Read	multiregionaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
GetObject	Grants permission to retrieve objects from Amazon S3	Read	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectAcl	Grants permission to return the access control list (ACL) of an object	Read	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectAttributes	Grants permission to retrieve attributes related to a specific object	Read	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectLegalHold	Grants permission to get an object's current Legal Hold status	Read	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectRetention	Grants permission to retrieve the retention settings for an object	Read	accesspointobject object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectTagging	Grants permission to return the tag set of an object	Read	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectTorrent	Grants permission to return torrent files from an Amazon S3 bucket	Read	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectVersion	Grants permission to retrieve a specific version of an object	Read	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetObjectVersionAcl	Grants permission to return the access control list (ACL) of a specific object version	Read	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetObjectVersionAttributes	Grants permission to retrieve attributes related to a specific version of an object	Read	accesspointobject		
			object		
				s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetObjectVersionForReplication	Grants permission to replicate both unencrypted objects and objects encrypted with SSE-S3 or SSE-KMS	Read	object*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetObjectVersionTagging	Grants permission to return the tag set for a specific version of the object	Read	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetObjectVersionTorrent	Grants permission to get Torrent files about a different version using the versionId subresource	Read	object*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetReplicationConfiguration	Grants permission to get the replication configuration information set on an Amazon S3 bucket	Read	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetStorageLensConfiguration	Grants permission to get an Amazon S3 Storage Lens configuration	Read	storagelensconfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetStorageLensConfigurationTagging	Grants permission to get the tag set of an existing Amazon S3 Storage Lens configuration	Read	storagelensconfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetStorageLensDashboard	Grants permission to get an Amazon S3 Storage Lens dashboard	Read	storagelensconfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
GetStorageLensGroup	Grants permission to get an Amazon S3 Storage Lens group	Read	storagelensgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
InitiateReplication [permission only]	Grants permission to initiate the replication process by setting replication status of an object to pending	Write	object*		
				s3:ResourceAccount	
ListAccessGrants	Grants permission to list Access Grant	List	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAccessGrantsInstances	Grants permission to List Access Grants Instances	List		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
ListAccessGrantsLocations	Grants permission to list Access Grants locations	List	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAccessPoints	Grants permission to list access points	List		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAccessPointsForObjectLambda	Grants permission to list object lambda enabled accesspoints	List		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAllMyBuckets	Grants permission to list all buckets owned by the authenticated sender of the request	List		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
ListBucket	Grants permission to list some or all of the objects in an Amazon S3 bucket (up to 1000)	List	accesspoint bucket		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:authType s3:delimiter s3:max-keys s3:prefix s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
	Grants permission to list in-progress multipart uploads	List	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListBucketMultipartUploads					

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				content-sha256 s3:AccessPointTag/${TagKey} aws:ResourceTag/${TagKey}	
ListBucketVersions	Grants permission to list metadata about all the versions of objects in an Amazon S3 bucket	List	accesspoint		
			bucket		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:authType s3:delimiter s3:max-keys s3:prefix s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCallerAccessGrants	Grants permission to list caller's Access Grant	List	accessgrantsinstance*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListJobs	Grants permission to list current jobs and jobs that have ended recently	List		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMultiRegionAccessPoints	Grants permission to list Multi-Region Access Points	List		s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
ListMultipartUploadParts	Grants permission to list the parts that have been uploaded for a specific multipart upload	List	accesspointobject object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListStorageLensConfigurations	Grants permission to list Amazon S3 Storage Lens configurations	List		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListStorageLensGroups	Grants permission to list S3 Storage Lens groups	List		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
ListTagsForResource	Grants permission to list the tags attached to the specified resource	List	accessgrant		
			accessgrantsinstance		
			accessgrantslocation		
			accesspoint		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			bucket		
			storagelensgroup		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ObjectOwnerOverrideToBucketOwner	Grants permission to change replica ownership	Permissions management	object*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PauseReplication [permission only]	Grants permission to pause S3 Replication from target source buckets to destination buckets	Write	bucket*		s3:GetReplicationConfiguration s3:PutReplicationConfiguration

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:destinationRegion s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAccelerateConfiguration	Grants permission to use the accelerate subresource to set the Transfer Acceleration state of an existing S3 bucket	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutAccessGrantsInstanceResourcePolicy	Grants permission to put Access grants instance resource policy	Permissions management	accessgrantsinstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
PutAccessPointConfigurationForObjectLambda	Grants permission to set the configuration of the object lambda enabled access point	Write	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointArn s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAccessPointPolicy	Grants permission to associate an access policy with a specified access point	Permissions management	accesspoint*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutAccessPointPolicyForObjectLambda	Grants permission to associate an access policy with a specified object lambda enabled access point	Permissions management	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAccessPointPublicAccessBlock	Grants permission to associate public access block configurations with a specified access point, while creating a access point	Permissions management			
PutAccountPublicAccessBlock	Grants permission to create or modify the PublicAccessBlock configuration for an AWS account	Permissions management		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAnalyticsConfiguration	Grants permission to set an analytics configuration for the bucket, specified by the analytics configuration ID	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutBucketAbac	Grants permission to set ABAC configuration for a general purpose bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutBucketAcl	Grants permission to set the permissions on an existing bucket using access control lists (ACLs)	Permissions management	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-acl s3:x-amz-content-sha256 s3:x-amz-grant-full-control s3:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				grant-read s3:x-amz-grant-read-acp s3:x-amz-grant-write s3:x-amz-grant-write-acp	
PutBucketCORS	Grants permission to set the CORS configuration for an Amazon S3 bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutBucketLogging	Grants permission to set the logging parameters for an Amazon S3 bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutBucketNotification	Grants permission to receive notifications when certain events happen in an Amazon S3 bucket	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutBucketObjectLockConfiguration	Grants permission to put Object Lock configuration on a specific bucket	Write	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:TlsVersion s3:signatureversion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutBucketOwnershipControls	Grants permission to add, replace or delete ownership controls on a bucket	Permissions management	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutBucketPolicy	Grants permission to add or replace a bucket policy on a bucket	Permissions management	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutBucketPublicAccessBlock	Grants permission to create or modify the PublicAccessBlock configuration for a specific Amazon S3 bucket	Permissions management	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutBucketRequestPayment	Grants permission to set the request payment configuration of a bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutBucketTagging	Grants permission to add a set of tags to an existing Amazon S3 bucket	Tagging	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutBucketVersioning	Grants permission to set the versioning state of an existing Amazon S3 bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutBucketWebsite	Grants permission to set the configuration of the website that is specified in the website subresource	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutEncryptionConfiguration	Grants permission to set the encryption configuration for an Amazon S3 bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutIntelligentTieringConfiguration	Grants permission to create new or update or delete an existing Amazon S3 Intelligent Tiering configuration	Write	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutInventoryConfiguration	Grants permission to add an inventory configuration to the bucket, identified by the inventory ID	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:InventoryAccessibleOptionalFields	
PutJobTagging	Grants permission to replace tags on an existing Amazon S3 Batch Operations job	Tagging	job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:ExistingJobPriority s3:ExistingJobOperation aws:TagKeys aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey}	
PutLifecycleConfiguration	Grants permission to create a new lifecycle configuration for the bucket or replace an existing lifecycle configuration	Write	bucket*	s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutMetricsConfiguration	Grants permission to set or update a metrics configuration for the CloudWatch request metrics from an Amazon S3 bucket	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
PutMultiRegionAccessPointPolicy	Grants permission to associate an access policy with a specified Multi-Region Access Point	Permissions management	multiregionaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
PutObject	Grants permission to add an object to a bucket	Write	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:RequestObjectTag/<key> s3:RequestObjectTagKeys s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-acl s3:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				content-sha256 s3:x-amz-copy-source s3:x-amz-grant-full-control s3:x-amz-grant-read s3:x-amz-grant-read-acp s3:x-amz-grant-write s3:x-amz-grant-write-acp	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-metadata-directive s3:x-amz-server-side-encryption s3:x-amz-server-side-encryption-aws-kms-key-id s3:x-amz-server-side-encryption-customer-algorithm s3:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				storage-class s3:x-amz-website-redirect-location s3:object-lock-mode s3:object-lock-retain-until-date s3:object-lock-remaining-retention-days s3:object-lock-legal-hold s3:if-match s3:if-none-match	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:ObjectCreationOperation	
PutObjectAcl	Grants permission to set the access control list (ACL) permissions for new or existing objects in an S3 bucket	Permissions management	accesspointobject object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-acl s3:x-amz-content-sha256 s3:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				grant-full-control s3:x-amz-grant-read s3:x-amz-grant-read-acp s3:x-amz-grant-write s3:x-amz-grant-write-acp s3:x-amz-storage-class	
PutObjectLegalHold	Grants permission to apply a Legal Hold configuration to the specified object	Write	accesspointobject object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:object-lock-legal-hold	
PutObjectRetention	Grants permission to place an Object Retention configuration on an object	Write	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:object-lock-mode s3:object-lock-retain-until-date s3:object-lock-remaining-re	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tention-days	
PutObjectTagging	Grants permission to set the supplied tag-set to an object that already exists in a bucket	Tagging	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:ExistingObjectTag/<key> s3:RequestObjectTag/<key> s3:RequestObjectTagKeys s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutObjectVersionAcl	Grants permission to use the acl subresource to set the access control list (ACL) permissions for an object that already exists in a bucket	Permissions management	accesspointobject object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-acl s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-grant-full-control s3:x-amz-grant-read s3:x-amz-grant-read-acp s3:x-amz-grant-write s3:x-amz-grant-write-acp s3:x-amz-storage-class	
PutObjectVersionTagging	Grants permission to set the supplied tag-set for a specific version of an object	Tagging	accesspointobject object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:ExistingObjectTag/<key> s3:RequestObjectTag/<key> s3:RequestObjectTagKeys s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				content-sha256	
PutReplicationConfiguration	Grants permission to create a new replication configuration or replace an existing one	Write	bucket*		iam:PassRole
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:isReplicationPauseRequest	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutStorageLensConfiguration	Grants permission to create or update an Amazon S3 Storage Lens configuration	Write		s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:TagKeys aws:RequestTag/${TagKey}	
PutStorageLensConfigurationTagging	Grants permission to put or replace tags on an existing Amazon S3 Storage Lens configuration	Tagging	storagelensconfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:TagKeys aws:RequestTag/${TagKey}	
Replicate Delete	Grants permission to replicate delete markers to the destination bucket	Write	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
Replicate Object	Grants permission to replicate objects and object tags to the destination bucket	Write	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:x-amz-server-side-encryption s3:x-amz-server-side-encryption-aws-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms-key-id s3:x-amz-server-side-encryption-customer-algorithm	
Replicate Tags	Grants permission to replicate object tags to the destination bucket	Tagging	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
RestoreObject	Grants permission to restore an archived copy of an object back into Amazon S3	Write	accesspointobject		
			object		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
SubmitMultiRegionAccessPointRoutes	Grants permission to submit a route configuration update for a Multi-Region Access Point	Write	multiregionaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureversion s3:signatureAge s3:TlsVersion	
TagResource	Grants permission to add tags to the specified resource	Tagging	accessgrant		
			accessgrantsinstance		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			accessgrantslocation		
			accesspoint		
			bucket		
			storagelensgroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from the specified resource	Tagging	accessgrant		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			accessgrantsinstance		
			accessgrantslocation		
			accesspoint		
			bucket		
			storagelensgroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:TagKeys	
UpdateAccessGrantsLocation	Grants permission to update Access Grants location	Permissions management	accessgrantslocation*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsLocationScope s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateBucketMetadataInventoryTableConfiguration	Grants permission to update the inventory table configuration on an existing S3 Metadata configuration for a specified general purpose bucket	Write	bucket*		kms:DescribeKey s3tables:CreateNamespace s3tables:CreateTable s3tables:CreateTableBucket s3tables:GetTable s3tables:PutTableEncryption s3tables:PutTablePolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateBucketMetadataJournalTableConfiguration	Grants permission to update the journal table configuration on an existing S3 Metadata configuration for a specified general purpose bucket	Write	bucket*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
UpdateJobPriority	Grants permission to update the priority of an existing job	Write	job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:RequestJobPriority s3:ExistingJobPriority s3:ExistingJobOperation	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateJobStatus	Grants permission to update the status for the specified job	Write	job*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 s3:ExistingJobPriority s3:ExistingJobOperation s3:JobSuspendedCause	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateStorageLensGroup	Grants permission to update an existing S3 Storage Lens group	Write	storagelensgroup*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	

Resource types defined by Amazon S3

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
accesspoint	arn:${Partition}:s3:${Region}:${Account}:accesspoint/${AccessPointName}	aws:ResourceTag/${TagKey} s3:AccessPointNetworkOrigin s3:AccessPointTag/${TagKey} s3:DataAccessPointAccount s3:DataAccessPointArn
accesspointobject	arn:${Partition}:s3:${Region}:${Account}:accesspoint/${AccessPointName}/object/${ObjectName}	aws:ResourceTag/${TagKey} s3:AccessPointNetworkOrigin s3:AccessPointTag/${TagKey} s3:BucketTag/${TagKey} s3:DataAccessPointAccount s3:DataAccessPointArn
bucket	arn:${Partition}:s3:::${BucketName}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
		s3:BucketTag/${TagKey}
object	arn:${Partition}:s3:::${BucketName}/${ObjectName}	aws:ResourceTag/${TagKey} s3:BucketTag/${TagKey}
job	arn:${Partition}:s3:${Region}:${Account}:job/${JobId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
storagelensconfiguration	arn:${Partition}:s3:${Region}:${Account}:storage-lens/${ConfigId}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
storagelensgroup	arn:${Partition}:s3:${Region}:${Account}:storage-lens-group/${Name}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
objectlambdaaccesspoint	arn:${Partition}:s3-object-lambda:${Region}:${Account}:accesspoint/${AccessPointName}	

Resource types	ARN	Condition keys
multiregionaccesspoint	arn:${Partition}:s3::${Account}:accesspoint/${AccessPointAlias}	
multiregionaccesspointrequestarn	arn:${Partition}:s3:us-west-2:${Account}:async-request/mrap/${Operation}/${Token}	
accessgrantsinstance	arn:${Partition}:s3:${Region}:${Account}:access-grants/default	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
accessgrantslocation	arn:${Partition}:s3:${Region}:${Account}:access-grants/default/location/${Token}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys
accessgrant	arn:${Partition}:s3:${Region}:${Account}:access-grants/default/grant/${Token}	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Condition keys for Amazon S3

Amazon S3 defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
s3:AccessGrantScope	Filters access by the grant scope of access grants grant	String
s3:AccessGrantsInstanceArn	Filters access by access grants instance ARN	ARN
s3:AccessGrantsLocationScope	Filters access by the location scope of access grants location	String
s3:AccessPointNetworkOrigin	Filters access by the network origin (Internet or VPC)	String
s3:AccessPointTag/${TagKey}	Filters access by existing access point tag key and value	String

Condition keys	Description	Type
s3:BucketTag/${TagKey}	Filters access by the tags associated with the bucket	String
s3:DataAccessPointAccount	Filters access by the AWS Account ID that owns the access point	String
s3:DataAccessPointArn	Filters access by an access point Amazon Resource Name (ARN)	ARN
s3:ExistingJobOperation	Filters access by operation to updating the job priority	String
s3:ExistingJobPriority	Filters access by priority range to cancelling existing jobs	Numeric
s3:ExistingObjectTag/<key>	Filters access by existing object tag key and value	String
s3:InventoryAccessibleOptionalFields	Filters access by restricting which optional metadata fields a user can add when configuring S3 Inventory reports	ArrayOfString
s3:JobSuspendedCause	Filters access by a specific job suspended cause (for example, AWAITING_CONFIRMATION) to cancelling suspended jobs	String
s3:ObjectCreationOperation	Filters access by whether or not the operation creates an object	Bool
s3:RequestJobOperation	Filters access by operation to creating jobs	String

Condition keys	Description	Type
s3:RequestJobPriority	Filters access by priority range to creating new jobs	Numeric
s3:RequestObjectTag/<key>	Filters access by the tag keys and values to be added to objects	String
s3:RequestObjectTagKeys	Filters access by the tag keys to be added to objects	ArrayOfString
s3:ResourceAccount	Filters access by the resource owner AWS account ID	String
s3:TlsVersion	Filters access by the TLS version used by the client	Numeric
s3:authType	Filters access by authentication method	String
s3:delimiter	Filters access by delimiter parameter	String
s3:destinationRegion	Filters access by a specific replication destination region for targeted buckets of the AWS FIS action aws:s3:bucket-pause-replication	String
s3:if-match	Filters access by the request's 'If-Match' conditional header	String
s3:if-none-match	Filters access by the request's 'If-None-Match' conditional header	String
s3:isReplicationPauseRequest	Filters access by request made via AWS FIS action aws:s3:bucket-pause-replication	Bool
s3:locationconstraint	Filters access by a specific Region	String
s3:max-keys	Filters access by maximum number of keys returned in a ListBucket request	Numeric

Condition keys	Description	Type
s3:object-lock-legal-hold	Filters access by object legal hold status	String
s3:object-lock-mode	Filters access by object retention mode (COMPLIANCE or GOVERNANCE)	String
s3:object-lock-remaining-retention-days	Filters access by remaining object retention days	Numeric
s3:object-lock-retain-until-date	Filters access by object retain-until date	Date
s3:prefix	Filters access by key name prefix	String
s3:signatureAge	Filters access by the age in milliseconds of the request signature	Numeric
s3:signatureversion	Filters access by the version of AWS Signature used on the request	String
s3:versionid	Filters access by a specific object version	String
s3:x-amz-acl	Filters access by canned ACL in the request's x-amz-acl header	String
s3:x-amz-content-sha256	Filters access by unsigned content in your bucket	String
s3:x-amz-copy-source	Filters access by copy source bucket, prefix, or object in the copy object requests	String
s3:x-amz-grant-full-control	Filters access by x-amz-grant-full-control (full control) header	String
s3:x-amz-grant-read	Filters access by x-amz-grant-read (read access) header	String

Condition keys	Description	Type
s3:x-amz-grant-read-acp	Filters access by the x-amz-grant-read-acp (read permissions for the ACL) header	String
s3:x-amz-grant-write	Filters access by the x-amz-grant-write (write access) header	String
s3:x-amz-grant-write-acp	Filters access by the x-amz-grant-write-acp (write permissions for the ACL) header	String
s3:x-amz-metadata-directive	Filters access by object metadata behavior (COPY or REPLACE) when objects are copied	String
s3:x-amz-object-ownership	Filters access by Object Ownership	String
s3:x-amz-server-side-encryption	Filters access by server-side encryption	String
s3:x-amz-server-side-encryption-aws-kms-key-id	Filters access by AWS KMS customer managed CMK for server-side encryption	ARN
s3:x-amz-server-side-encryption-customer-algorithm	Filters access by customer specified algorithm for server-side encryption	String
s3:x-amz-storage-class	Filters access by storage class	String
s3:x-amz-website-redirect-location	Filters access by a specific website redirect location for buckets that are configured as static websites	String

Actions, resources, and condition keys for Amazon SageMaker

Amazon SageMaker (service prefix: `sagemaker`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon SageMaker
- Resource types defined by Amazon SageMaker
- Condition keys for Amazon SageMaker

Actions defined by Amazon SageMaker

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddAssociation	Grants permission to associate a lineage entity (artifact, context, action, experiment, experiment-trial-component) to each other	Write	action*		
			artifact*		
			context*		
			experiment*		
			experiment-trial-c		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			omponent*		
AddTags	Grants permission to add or overwrite one or more tags for the specified Amazon SageMaker resource	Tagging	action		
			algorithm		
			app		
			app-image-config		
			artifact		
			automl-job		
			cluster		
			cluster-scheduler-config		
			code-repository		
			compilation-job		
			compute-quota		
			context		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			data-quality-job-definition		
			device		
			device-fleet		
			domain		
			edge-deployment-plan		
			edge-packaging-job		
			endpoint		
			endpoint-config		
			experiment		
			experiment-trial		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			experiment-trial-component		
			feature-group		
			flow-definition		
			hub		
			hub-content		
			human-task-ui		
			hyper-parameter-tuning-job		
			image		
			inference-component		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			inference-recommendations-job		
			labeling-job		
			mlflow-app		
			mlflow-tracking-server		
			model		
			model-bias-job-definition		
			model-card		
			model-explainability-job-definition		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-package	sagemaker:CurrentModelLifeCycleStageStatus sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	
			model-package-group		
			model-quality-job-definition		
			monitoring-schedule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			notebook-instance		
			notebook-instance-lifecycle-config		
			optimization-job		
			partner-app		
			pipeline		
			processing-job		
			project		
			reserved-capacity		
			space		
			studio-lifecycle-config		
			training-job		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			training-plan		
			transform-job		
			user-profile		
			workteam		
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:TaggingAction	
AssociateTrialComponent	Grants permission to associate a trial component with a trial	Write	experiment-trial*		
			experiment-trial-component*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AttachClusterNodeVolume	Grants permission to attach an Amazon EBS volume to a SageMaker HyperPod cluster node	Write	cluster*		ec2:AttachVolume ec2:DescribeVolumes eks:DescribeCluster
BatchAddClusterNodes	Grants permission to add multiple nodes at a time to a SageMaker HyperPod cluster	Write	cluster*		eks:DescribeCluster
BatchDeleteClusterNodes	Grants permission to batch delete SageMaker HyperPod cluster nodes	Write	cluster*		eks:DescribeCluster

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchDescribeModelPackage	Grants permission to describe one or more ModelPackages	Read	model-package*	sagemaker:CurrentModelLifeCycleStageStatus sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	
BatchGetMetrics	Grants permission to retrieve metrics associated with SageMaker Resources such as Training Jobs or Trial Components	Read	experiment-trial-component* training-job*		
BatchGetRecord	Grants permission to get a batch of records from one or more feature groups	Read	feature-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchPutMetrics	Grants permission to publish metrics associated with a SageMaker Resource such as a Training Job or Trial Component	Write	experiment-trial-component*		
			training-job*		
CallMlflowAppApi	Grants permission to invoke MLflow APIs	Write	mlflow-app*		
CallPartnerAppApi	Grants permission for Partner App SDK to access the Partner App for reading or writing data use cases	Write	partner-app*		
CreateAction	Grants permission to create an action	Write	action*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAlgorithm	Grants permission to create an algorithm	Write	algorithm*		sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApp	Grants permission to create an App for a SageMaker UserProfile or Space	Write	app*		sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:ImageArns sagemaker:ImageVersionArns sagemaker:OwnerUserProfileArn sagemaker:SpaceSharingType sagemaker:StudioLifecycleConfigArns	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAppImageConfig	Grants permission to create an AppImageConfig	Write	app-image-config*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateArtifact	Grants permission to create an artifact	Write	artifact*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAutoMLJob	Grants permission to create an AutoML job	Write	automl-job*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InterContainerTrafficEncryption sagemaker:OutputKmsKey sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAutoMLJobV2	Grants permission to create a V2 AutoML job	Write	automl-job*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InterContainerTrafficEncryption sagemaker:OutputKmsKey sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCluster	Grants permission to create a SageMaker HyperPod cluster	Write	cluster*		ec2:DescribeImages ec2:DescribeSnapshots ec2:ModifyImageAttribute ec2:ModifySnapshotAttribute eks:AssociateAccessPolicy eks:CreateAccessEntry eks:DeleteAccessEntry eks:DescribeAccessEntry eks:DescribeCluster

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:CreateServiceLinkedRole iam:PassRole sagemaker:AddTags
			reserved-capacity		
			training-plan		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateClusterSchedulerConfig	Grants permission to create a cluster scheduler config	Write	cluster*		eks:AssociateAccessPolicy eks:DescribeCluster eks:ListAssociatedAccessPolicies sagemaker:AddTags sagemaker:DescribeCluster
			cluster-scheduler-config*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCodeRepository	Grants permission to create a CodeRepository	Write	code-repository*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCompilationJob	Grants permission to create a compilation job	Write	compilation-job*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateComputeQuota	Grants permission to create a compute quota	Write	cluster*		eks:AssociateAccessPolicy eks:DescribeCluster eks:ListAssociatedAccessPolicies sagemaker:AddTags sagemaker:DescribeCluster
			compute-quota*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateContext	Grants permission to create a context	Write	context*		sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataQualityJobDefinition	Grants permission to create a data quality job definition	Write	data-quality-job-definition*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:InterContainerTrafficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateDeviceFleet	Grants permission to create a device fleet	Write	device-fleet*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDomain	Grants permission to create a Domain for SageMaker Studio	Write	domain*		iam:CreateServiceLinkedRole iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:AppNetworkAccessType sagemaker:InstanceTypes sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets sagemaker:DomainSharingOutputKmsKey sagemaker:VolumeKmsKey	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:ImageArns sagemaker:ImageVersionArns sagemaker:StudioLifecycleConfigArns	
CreateEdgeDeploymentPlan	Grants permission to create an edge deployment plan	Write	edge-deployment-plan*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEdgeDeploymentStage	Grants permission to create an edge deployment stage	Write	edge-deployment-plan*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEdgePackagingJob	Grants permission to create an edge packaging job	Write	edge-packaging-job*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEndpoint	Grants permission to create an endpoint using the endpoint configuration specified in the request	Write	endpoint*		sagemaker:AddTags
			endpoint-config*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEndpointConfig	Grants permission to create an endpoint configuration that can be deployed using Amazon SageMaker hosting services	Write	endpoint-config*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:AcceleratorTypes sagemaker:InstanceTypes sagemaker:ModelArn sagemaker:VolumeKmsKey sagemaker:ServerlessMaxConcurrency sagemaker:ServerlessMemorySize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:NetworkIsolation sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateExperiment	Grants permission to create an experiment	Write	experiment*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFeatureGroup	Grants permission to create a feature group	Write	feature-group*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:FeatureGroupOnlineStoreKmsKey sagemaker:FeatureGroupOfflineStoreKmsKey sagemaker:FeatureGroupOfflineStoreS3Uri sagemaker:FeatureGroupEnableOnlineStore	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:FeatureGroupOfflineStoreConfig sagemaker:FeatureGroupDisableGlueTableCreation	
CreateFlowDefinition	Grants permission to create a flow definition, which defines settings for a human workflow	Write	flow-definition*		iam:PassRole sagemaker:AddTags
				sagemaker:WorkteamArn sagemaker:WorkteamType aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateHub	Grants permission to create a hub	Write	hub*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHubContentPresignedUrls	Grants permission to generate S3 presigned URLs with GetObject permission for accessing model artifacts	Read	hub*		
			hub-content*		
CreateHubContentReference	Grants permission to create hub content reference	Write	hub*		sagemaker:AddTags
			hub-content*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHumanTaskUi	Grants permission to define the settings you will use for the human review workflow user interface	Write	human-task-ui*		sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHyperParameterTuningJob	Grants permission to create a hyper parameter tuning job that can be deployed using Amazon SageMaker	Write	hyper-parameter-tuning-job*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:FileSystemAccessMode sagemaker:FileSystemDirectoryPath sagemaker:FileSystemId sagemaker:FileSystemType sagemaker:InstanceTypes sagemaker:InterContainerTra	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				fficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateImage	Grants permission to create a SageMaker Image	Write	image*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateImageVersion	Grants permission to create a SageMaker ImageVersion	Write	image*		
CreateInferenceComponent	Grants permission to create an inference component on an endpoint	Write	endpoint*		sagemaker:AddTags
			inference-component*		
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:ModelArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInferenceExperiment	Grants permission to create an inference experiment	Write	inference-experiment*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInferenceRecommendationsJob	Grants permission to create an inference recommend ations job	Write	inference-recommendations-job*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLabelingJob	Grants permission to start a labeling job. A labeling job takes unlabeled data in and produces labeled data as output, which can be used for training SageMaker models	Write	labeling-job*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:WorkteamArn sagemaker:WorkteamType sagemaker:VolumeKmsKey sagemaker:OutputKmsKey aws:RequestTag/${TagKey} aws:TagKeys	
CreateLineageGroupPolicy	Grants permission to create a lineage group policy	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMlflowApp	Grants permission to create an MLflow app	Write	mlflow-app*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMlflowTrackingServer	Grants permission to create an MLflow tracking server	Write	mlflow-tracking-server*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModel	Grants permission to create a model in Amazon SageMaker. In the request, you specify a name for the model and describe one or more containers	Write	model*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:NetworkIsolation sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets sagemaker:DirectGatedModelAccess	
CreateModelBiasJobDefinition	Grants permission to create a model bias job definition	Write	model-bias-job-definition*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:InterContainerTrafficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateModelCard	Grants permission to create a model card	Write	model-card*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelCardExportJob	Grants permission to create an export job for a model card	Write	model-card*		
CreateModelExplainabilityJobDefinition	Grants permission to create a model explainability job definition	Write	model-explainability-job-definition*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:InterContainerTrafficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateModelPackage	Grants permission to create a ModelPackage	Write	model-package	sagemaker:CurrentModelLifeCycleStageStatus sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	sagemaker:AddTags
			model-package-group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:ModelApprovalStatus sagemaker:CustomerMetadataProperties/${MetadataKey} sagemaker:ModelLifeCycle:Stage sagemaker:ModelLifeCycle:StageStatus	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateModelPackageGroup	Grants permission to create a ModelPackageGroup	Write	model-package-group*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateModelQualityJobDefinition	Grants permission to create a model quality job definition	Write	model-quality-job-definition*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:InterContainerTrafficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateMonitoringSchedule	Grants permission to create a monitoring schedule	Write	monitoring-schedule*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:InterContainerTrafficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateNotebookInstance	Grants permission to create an Amazon SageMaker notebook instance. A notebook instance is an Amazon EC2 instance running on a Jupyter Notebook	Write	notebook-instance*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:AcceleratorTypes sagemaker:DirectInternetAccess sagemaker:InstanceTypes sagemaker:MinimumInstanceMetadataServiceVersion sagemaker:RootAccess	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
CreateNotebookInstanceLifecycleConfig	Grants permission to create a notebook instance lifecycle configuration that can be deployed using Amazon SageMaker	Write	notebook-instance-lifecycle-config*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOptimizationJob	Grants permission to create an optimization job	Write	optimization-job*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePartnerApp	Grants permission to create an Amazon SageMaker Partner AI App	Write	partner-app*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePartnerAppPresignedUrl	Grants permission to return a URL that you can use from your browser to connect to the Amazon SageMaker Partner AI App	Write	partner-app*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CreatePipeline	Grants permission to create a pipeline	Write	pipeline*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePresignedDomainUrl	Grants permission to return a URL that you can use from your browser to connect to the Domain as a specified UserProfile when AuthMode is 'IAM'	Write	user-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePresignedMlflowAppUrl	Grants permission to return a URL that you can use from your browser to connect to the MLflow app	Write	mlflow-app*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CreatePresignedMlflowTrackingServerUrl	Grants permission to return a URL that you can use from your browser to connect to the MLflow tracking server	Write	mlflow-tracking-server*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
CreatePresignedNotebookInstanceUrl	Grants permission to create a URL that you can use from your browser to connect to the Notebook Instance	Write	notebook-instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateProcessingJob	Grants permission to start a processing job. After processing completes, Amazon SageMaker saves the resulting artifacts and other optional output to an Amazon S3 location that you specify	Write	processing-job*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:VpcSubnets sagemaker:InterContainerTrafficEncryption	
CreateProject	Grants permission to create a Project	Write	project*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateReservedCapacity [permission only]	Grants permission to create a reserved capacity	Write	reserved-capacity*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSharedModel [permission only]	Grants permission to create a shared model in a SageMaker Studio application	Write	shared-model*		
CreateSpace	Grants permission to create a Space for a SageMaker Domain	Write	space*		sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:ImageArns sagemaker:ImageVersionArns sagemaker:OwnerUserProfileArn sagemaker:RemoteAccess sagemaker:SpaceSharingType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:StudioLifecycleConfigArns	
CreateStudioLifecycleConfig	Grants permission to create a Studio Lifecycle Configuration that can be deployed using Amazon SageMaker	Write	studio-lifecycle-config*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrainingJob	Grants permission to start a model training job. After training completes, Amazon SageMaker saves the resulting model artifacts and other optional output to an Amazon S3 location that you specify	Write	training-job*		iam:PassRole sagemaker:AddTags
			reserved-capacity		
			training-plan		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:FileSystemAccessMode sagemaker:FileSystemDirectoryPath sagemaker:FileSystemId sagemaker:FileSystemType sagemaker:InstanceTypes sagemaker:InterContainerTra	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				fficEncryption sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets sagemaker:KeepAlivePeriod	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:EnableRemoteDebu sagemaker:DirectGatedModelAccess	
CreateTrainingPlan	Grants permission to create a training plan that allocates resources for scheduling workloads within a specified time range	Write	training-plan*		sagemaker:AddTags sagemaker:CreateReservedCapacity
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTransformJob	Grants permission to start a transform job. After the results are obtained, Amazon SageMaker saves them to an Amazon S3 location that you specify	Write	transform-job*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:ModelArn sagemaker:OutputKmsKey sagemaker:VolumeKmsKey	
CreateTrial	Grants permission to create a trial	Write	experiment*		sagemaker:AddTags
			experiment-trial*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrialComponent	Grants permission to create a trial component	Write	experiment-trial-component*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUserProfile	Grants permission to create a UserProfile for a SageMaker Domain	Write	user-profile*		iam:PassRole sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:VpcSecurityGroupIds sagemaker:InstanceTypes sagemaker:DomainSharingOutputKmsKey sagemaker:ImageArns sagemaker:ImageVersionArns sagemaker:StudioLi	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				fecycleConfigArns	
CreateWorkforce	Grants permission to create a workforce	Write	workforce*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkteam	Grants permission to create a workteam	Write	workteam*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAction	Grants permission to delete an action	Write	action*		
DeleteAlgorithm	Grants permission to delete an algorithm	Write	algorithm*		
DeleteApp	Grants permission to delete an App	Write	app*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:OwnerUserProfileArn sagemaker:SpaceSharingType	
DeleteAppImageConfig	Grants permission to delete an AppImageConfig	Write	app-image-config*		
DeleteArtifact	Grants permission to delete an artifact	Write	artifact*		
DeleteAssociation	Grants permission to delete the association from a lineage entity (artifact, context, action, experiment, experiment-trial-component) to another	Write	action*		
			artifact*		
			context*		
			experiment*		
			experiment-trial-component*		
DeleteCluster	Grants permission to delete a SageMaker HyperPod cluster	Write	cluster*		eks:DeleteAccessEntry

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteClusterSchedulerConfig	Grants permission to delete a cluster scheduler config	Write	cluster-scheduler-config*		
DeleteCodeRepository	Grants permission to delete a CodeRepository	Write	code-repository*		
DeleteCompilationJob	Grants permission to delete a compilation job	Write	compilation-job*		
DeleteComputeQuota	Grants permission to delete a compute quota	Write	compute-quota*		
DeleteContext	Grants permission to delete a context	Write	context*		
DeleteDataQualityJobDefinition	Grants permission to delete the data quality job definition created using the CreateDataQualityJobDefinition API	Write	data-quality-job-definition*		
DeleteDeviceFleet	Grants permission to delete a device fleet	Write	device-fleet*		
DeleteDomain	Grants permission to delete a Domain	Write	domain*		
DeleteEdgeDeploymentPlan	Grants permission to delete an edge deployment plan	Write	edge-deployment-plan*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEdgeDeploymentStage	Grants permission to delete an edge deployment stage	Write	edge-deployment-plan*		
DeleteEndpoint	Grants permission to delete an endpoint. Amazon SageMaker frees up all the resources that were deployed when the endpoint was created	Write	endpoint*		
DeleteEndpointConfig	Grants permission to delete the endpoint configuration created using the CreateEndpointConfig API. The DeleteEndpointConfig API deletes only the specified configuration. It does not delete any endpoints created using the configuration	Write	endpoint-config*		
DeleteExperiment	Grants permission to delete an experiment	Write	experiment*		
DeleteFeatureGroup	Grants permission to delete a feature group	Write	feature-group*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFlowDefinition	Grants permission to delete the specified flow definition	Write	flow-definition*		
DeleteHub	Grants permission to delete hubs	Write	hub*		
DeleteHubContent	Grants permission to delete hub content	Write	hub*		
			hub-content*		
DeleteHubContentReference	Grants permission to delete hub content reference	Write	hub*		
			hub-content*		
DeleteHumanLoop	Grants permission to delete a specified human loop	Write	human-loop*		
DeleteHumanTaskUi	Grants permission to delete the specified human task user interface (worker task template)	Write	human-task-ui*		
DeleteHyperParameterTuningJob	Grants permission to delete a hyper parameter tuning job	Write	hyper-parameter-tuning-job*		
DeleteImage	Grants permission to delete a SageMaker Image	Write	image*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteImageVersion	Grants permission to delete a SageMaker ImageVersion	Write	image-version*		
DeleteInferenceComponent	Grants permission to delete an inference component. Amazon SageMaker frees up the resources that were reserved when the inference component was created	Write	inference-component*		
DeleteInferenceExperiment	Grants permission to delete an inference experiment	Write	inference-experiment*		
DeleteLineageGroupPolicy	Grants permission to delete a lineage group policy	Write			
DeleteMlflowApp	Grants permission to delete an MLflow app	Write	mlflow-app*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteMlflowTrackingServer	Grants permission to delete an MLflow tracking server	Write	mlflow-tracking-server*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteModel	Grants permission to delete a model created using the CreateModel API. The DeleteModel API deletes only the model entry in Amazon SageMaker that you created by calling the CreateModel API. It does not delete model artifacts, inference code, or the IAM role that you specified when creating the model	Write	model*		
DeleteModelBiasJobDefinition	Grants permission to delete the model bias job definition created using the CreateModelBiasJobDefinition API	Write	model-bias-job-definition*		
DeleteModelCard	Grants permission to delete a model card	Write	model-card*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteModelExplainabilityJobDefinition	Grants permission to delete the model explainability job definition created using the CreateModelExplainabilityJobDefinition API	Write	model-explainability-job-definition*		
DeleteModelPackage	Grants permission to delete a ModelPackage	Write	model-package*	sagemaker:CurrentModelLifeCycleStageStatus sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	
DeleteModelPackageGroup	Grants permission to delete a ModelPackageGroup	Write	model-package-group*		
DeleteModelPackageGroupPolicy	Grants permission to delete a ModelPackageGroup policy	Write	model-package-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteModelQualityJobDefinition	Grants permission to delete the model quality job definition created using the CreateModelQualityJobDefinition API	Write	model-quality-job-definition*		
DeleteMonitoringSchedule	Grants permission to delete a monitoring schedule	Write	monitoring-schedule*		
DeleteNotebookInstance	Grants permission to delete a Amazon SageMaker notebook instance. Before you can delete a notebook instance, you must call the StopNotebookInstance API	Write	notebook-instance*		
DeleteNotebookInstanceLifecycleConfig	Grants permission to delete a notebook instance lifecycle configuration	Write	notebook-instance-lifecycle-config*		
DeleteOptimizationJob	Grants permission to delete an optimization job	Write	optimization-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePartnerApp	Grants permission to delete an Amazon SageMaker Partner AI App	Write	partner-app*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeletePipeline	Grants permission to delete a pipeline	Write	pipeline*		
DeleteProject	Grants permission to delete a project	Write	project*		
DeleteRecord	Grants permission to delete a record from a feature group	Write	feature-group*		
DeleteResourcePolicy [permission only]	Grants AWS Resource Access Manager permission to delete a resource policy on a SageMaker resource that supports cross-account sharing	Write			
DeleteSpace	Grants permission to delete a Space	Write	space*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:OwnerUserProfileArn sagemaker:SpaceSharingType	
DeleteStudioLifecycleConfig	Grants permission to delete a Studio Lifecycle Configuration	Write	studio-lifecycle-config*		
DeleteTags	Grants permission to delete the specified set of tags from an Amazon SageMaker resource	Tagging	action		
			algorithm		
			app		
			app-image-config		
			artifact		
			automl-job		
			cluster		
			cluster-scheduler-config		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			code-repository		
			compilation-job		
			compute-quota		
			context		
			data-quality-job-definition		
			device		
			device-fleet		
			domain		
			edge-deployment-plan		
			edge-packaging-job		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			endpoint		
			endpoint-config		
			experiment		
			experiment-trial		
			experiment-trial-component		
			feature-group		
			flow-definition		
			hub		
			hub-content		
			human-task-ui		
			hyper-parameter-tuning-job		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image		
			inference-component		
			inference-recommendations-job		
			labeling-job		
			mlflow-tracking-server		
			model		
			model-bias-job-definition		
			model-card		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-explainability-job-definition		
			model-package	sagemaker:CurrentModelLifeCycleStageStatus sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	
			model-package-group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-quality-job-definition		
			monitoring-schedule		
			notebook-instance		
			notebook-instance-lifecycle-config		
			optimization-job		
			partner-app		
			pipeline		
			processing-job		
			project		
			reserved-capacity		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			space		
			studio-lifecycle-config		
			training-job		
			training-plan		
			transform-job		
			user-profile		
			workteam		
				aws:TagKeys	
DeleteTrial	Grants permission to delete a trial	Write	experiment-trial*		
DeleteTrialComponent	Grants permission to delete a trial component	Write	experiment-trial-component*		
DeleteUserProfile	Grants permission to delete a UserProfile	Write	user-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteWorkforce	Grants permission to delete a workforce	Write	workforce*		
DeleteWorkteam	Grants permission to delete a workteam	Write	workteam*		
DeployHubModel	Grants permission to deploy a model in hub to an endpoint	Write	hub*		
			hub-content*		
DeregisterDevices	Grants permission to deregister a set of devices	Write	device*		
DescribeAction	Grants permission to get information about an action	Read	action*		
DescribeAlgorithm	Grants permission to describe an algorithm	Read	algorithm*		
DescribeApp	Grants permission to describe an App	Read	app*		
DescribeAppImageConfig	Grants permission to describe an AppImageConfig	Read	app-image-config*		
DescribeArtifact	Grants permission to get information about an artifact	Read	artifact*		
DescribeAutoMLJob	Grants permission to describe an AutoML job that was created via the CreateAutoMLJob API	Read	automl-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAutoMLJobV2	Grants permission to describe an AutoML job that was created via the CreateAutoMLJobV2 API	Read	automl-job*		
DescribeCluster	Grants permission to return information about a SageMaker HyperPod cluster	Read	cluster*		
DescribeClusterEvent	Grants permission to return information about an Event within a SageMaker HyperPod cluster	Read	cluster*		
DescribeClusterInference [permission only]	Grants permission to get information about the inference operator for a SageMaker HyperPod cluster	Read	cluster*		
DescribeClusterNode	Grants permission to return information about a SageMaker HyperPod cluster node	Read	cluster*		
DescribeClusterSchedulerConfig	Grants permission to get information about a cluster scheduler config	Read	cluster-scheduler-config*		
DescribeCodeRepository	Grants permission to describe a CodeRepository	Read	code-repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCompilationJob	Grants permission to return information about a compilation job	Read	compilation-job*		
DescribeComputeQuota	Grants permission to get information about a compute quota	Read	compute-quota*		
DescribeContext	Grants permission to get information about a context	Read	context*		
DescribeDataQualityJobDefinition	Grants permission to return information about a data quality job definition	Read	data-quality-job-definition*		
DescribeDevice	Grants permission to access information about a device	Read	device*		
DescribeDeviceFleet	Grants permission to access information about a device fleet	Read	device-fleet*		
DescribeDomain	Grants permission to describe a Domain	Read	domain*		
DescribeEdgeDeploymentPlan	Grants permission to access information about an edge deployment plan	Read	edge-deployment-plan*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeEdgePackagingJob	Grants permission to access information about an edge packaging job	Read	edge-packaging-job*		
DescribeEndpoint	Grants permission to return the description of an endpoint	Read	endpoint*		
DescribeEndpointConfig	Grants permission to return the description of an endpoint configuration, which was created using the CreateEndpointConfig API	Read	endpoint-config*		
DescribeExperiment	Grants permission to return information about an experiment	Read	experiment*		
DescribeFeatureGroup	Grants permission to return information about a feature group	Read	feature-group*		
DescribeFeatureMetadata	Grants permission to return information about a feature metadata	Read	feature-group*		
DescribeFlowDefinition	Grants permission to return information about the specified flow definition	Read	flow-definition*		
DescribeHub	Grants permission to describe hubs	Read	hub*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeHubContent	Grants permission to describe hub content	Read	hub*		
			hub-content*		
DescribeHumanLoop	Grants permission to return information about the specified human loop	Read	human-loop*		
DescribeHumanTaskUi	Grants permission to return detailed information about the specified human review workflow user interface	Read	human-task-ui*		
DescribeHyperParameterTuningJob	Grants permission to describe a hyper parameter tuning job that was created via the CreateHyperParameterTuningJob API	Read	hyper-parameter-tuning-job*		
DescribeImage	Grants permission to return information about a SageMaker Image	Read	image*		
DescribeImageVersion	Grants permission to return information about a SageMaker ImageVersion	Read	image-version*		
DescribeInferenceComponent	Grants permission to return the description of an inference component	Read	inference-component*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInferenceExperiment	Grants permission to get information about an inference experiment	Read	inference-experiment*		
DescribeInferenceRecommendationsJob	Grants permission to get information about an inference recommendations job	Read	inference-recommendations-job*		
DescribeLabelingJob	Grants permission to return information about a labeling job	Read	labeling-job*		
DescribeLineageGroup	Grants permission to describe a lineage group	Read			
DescribeMlflowApp	Grants permission to get information about an MLflow app	Read	mlflow-app*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeMlflowTrackingServer	Grants permission to get information about an MLflow tracking server	Read	mlflow-tracking-server*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DescribeModel	Grants permission to describe a model that you created using the CreateModel API	Read	model*		
DescribeModelBiasJobDefinition	Grants permission to return information about a model bias job definition	Read	model-bias-job-definition*		
DescribeModelCard	Grants permission to get information about a model card	Read	model-card*		
DescribeModelCardExportJob	Grants permission to get information about a model card export job	Read	model-card-export-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeModelExplainabilityJobDefinition	Grants permission to return information about a model explainability job definition	Read	model-explainability-job-definition*		
DescribeModelPackage	Grants permission to describe a ModelPackage	Read	model-package*	sagemaker:CurrentModelLifeCycleStageStatus sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	
DescribeModelPackageGroup	Grants permission to describe a ModelPackageGroup	Read	model-package-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeModelQualityJobDefinition	Grants permission to return information about a model quality job definition	Read	model-quality-job-definition*		
DescribeMonitoringSchedule	Grants permission to return information about a monitoring schedule	Read	monitoring-schedule*		
DescribeNotebookInstance	Grants permission to return information about a notebook instance	Read	notebook-instance*		
DescribeNotebookInstanceLifecycleConfig	Grants permission to describe a notebook instance lifecycle configuration that was created via the CreateNotebookInstanceLifecycleConfig API	Read	notebook-instance-lifecycle-config*		
DescribeOptimizationJob	Grants permission to return information about an optimization job	Read	optimization-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribePartnerApp	Grants permission to describe an Amazon SageMaker Partner AI App	Read	partner-app*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DescribePipeline	Grants permission to get information about a pipeline	Read	pipeline*		
				sagemaker:PipelineVersionId	
DescribePipelineDefinitionForExecution	Grants permission to get the pipeline definition for a pipeline execution	Read	pipeline-execution*		
DescribePipelineExecution	Grants permission to get information about a pipeline execution	Read	pipeline-execution*		
DescribeProcessingJob	Grants permission to return information about a processing job	Read	processing-job*		
DescribeProject	Grants permission to describe a project	Read	project*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeReservedCapacity	Grants permission to return information about a specified Reserved Capacity	Read	reserved-capacity*		
DescribeSharedModel [permission only]	Grants permission to describe a shared model in a SageMaker Studio application	Read	shared-model*		
DescribeSpace	Grants permission to describe a Space	Read	space*		
DescribeStudioLifecycleConfig	Grants permission to describe a Studio Lifecycle Configuration	Read	studio-lifecycle-config*		
DescribeSubscribedWorkteam	Grants permission to return information about a subscribed workteam	Read	workteam*		
DescribeTrainingJob	Grants permission to return information about a training job	Read	training-job*		
DescribeTrainingPlan	Grants permission to return information about a specified training plan	Read	training-plan*		
DescribeTransformJob	Grants permission to return information about a transform job	Read	transform-job*		
DescribeTrial	Grants permission to return information about a trial	Read	experiment-trial*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTrialComponent	Grants permission to return information about a trial component	Read	experiment-trial-component*		
DescribeUserProfile	Grants permission to describe a UserProfile	Read	user-profile*		
DescribeWorkforce	Grants permission to return information about a workforce	Read	workforce*		
DescribeWorkteam	Grants permission to return information about a workteam	Read	workteam*		
DetachClusterNodeVolume	Grants permission to detach an Amazon EBS volume from a SageMaker HyperPod cluster node	Write	cluster*		ec2:DescribeVolumes ec2:DetachVolume eks:DescribeCluster
DisableSagemakerServicecatalogPortfolio	Grants permission to disable a SageMaker Service Catalog Portfolio	Write			
DisassociateTrialComponent	Grants permission to disassociate a trial component from a trial	Write	experiment-trial*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			experiment-trial-component*		
			processing-job*		
EnableSagemakerServicecatalogPortfolio	Grants permission to enable a SageMaker Service Catalog Portfolio	Write			
GetDeployments	Grants permission to get deployment plan for device	Read	device*		
GetDeviceFleetReport	Grants permission to access a summary of the devices in a device fleet	Read	device-fleet*		
GetDeviceRegistration	Grants permission to get device registration. After you deploy a model onto edge devices this api is used to get current device registration	Read	device*		
GetLineageGroupPolicy	Grants permission to retreive a lineage group policy	Read			
GetModelPackageGroupPolicy	Grants permission to get a ModelPackageGroup policy	Read	model-package-group*		
GetRecord	Grants permission to get a record from a feature group	Read	feature-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResourcePolicy [permission only]	Grants AWS Resource Access Manager permission to retrieve a resource policy on a SageMaker resource that supports cross-account sharing	Read			
GetSagemakerServicecatalogPortfolioStatus	Grants permission to get a SageMaker Service Catalog Portfolio	Read			
GetScalingConfigurationRecommendation	Grants permission to get a scaling policy configuration recommendation	Read	inference-recommendations-job*		
GetSearchSuggestions	Grants permission to get search suggestions when provided with a keyword	Read			
ImportHubContent	Grants permission to import hub content	Write	hub*		sagemaker:AddTags
			hub-content*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
InvokeEndpoint	Grants permission to invoke an endpoint. After you deploy a model into production using Amazon SageMaker hosting services, your client applications use this API to get inferences from the model hosted at the specified endpoint	Read	endpoint*		
			inference-component		
				sagemaker:TargetModel	
InvokeEndpointAsync	Grants permission to get inferences from the hosted model at the specified endpoint in an asynchronous manner	Read	endpoint*		
InvokeEndpointWithResponseStream	Grants permission to get the inference response as a stream from the specified endpoint	Read	endpoint*		
			inference-component		
ListActions	Grants permission to list actions	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAlgorithms	Grants permission to list Algorithms	List			
ListAliases	Grants permission to list Aliases that belong to a SageMaker Image or Sagemaker ImageVersion	List	image*		
			image-version*		
ListAppImageConfigs	Grants permission to list the AppImageConfigs in your account	List			
ListApps	Grants permission to list the Apps in your account	List			
ListArtifacts	Grants permission to list artifacts	List			
ListAssociations	Grants permission to list associations	List			
ListAutoMLJobs	Grants permission to list AutoML jobs	List			
ListCandidatesForAutoMLJob	Grants permission to lists candidates for an AutoML job	List			
ListClusterEvents	Grants permission to list events within a SageMaker HyperPod cluster	List	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListClusterNodes	Grants permission to list nodes within a SageMaker HyperPod cluster	List	cluster*		
ListClusterSchedulerConfigs	Grants permission to list cluster scheduler configs	List			
ListClusters	Grants permission to list SageMaker HyperPod clusters	List			
ListCodeRepositories	Grants permission to list code repositories	List			
ListCompilationJobs	Grants permission to list compilation jobs	List			
ListComputeQuotas	Grants permission to list compute quotas	List			
ListContexts	Grants permission to list contexts	List			
ListDataQualityJobDefinitions	Grants permission to list data quality job definitions	List			
ListDeviceFleets	Grants permission to list device fleets	List			
ListDevices	Grants permission to list devices	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDomains	Grants permission to list the Domains in your account	List			
ListEdgeDeploymentPlans	Grants permission to list edge deployment plans	List			
ListEdgePackagingJobs	Grants permission to list edge packaging jobs	List			
ListEndpointConfigs	Grants permission to list endpoint configurations	List			
ListEndpoints	Grants permission to list endpoints	List			
ListExperiments	Grants permission to list experiments	List			
ListFeatureGroups	Grants permission to list feature groups	List			
ListFlowDefinitions	Grants permission to return summary information about flow definitions, given the specified parameters	List			
ListHubContentVersions	Grants permission to list all versions of hub content	List	hub* hub-content*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListHubContents	Grants permission to list newest versions of hub content	List	hub*		
ListHubs	Grants permission to list hubs	List			
ListHumanLoops	Grants permission to return summary information about human loops, given the specified parameters	List			
ListHumanTaskUis	Grants permission to return summary information about human review workflow user interfaces, given the specified parameters	List			
ListHyperParameterTuningJobs	Grants permission to list hyper parameter tuning jobs	List			
ListImageVersions	Grants permission to list ImageVersions that belong to a SageMaker Image	List	image*		
ListImages	Grants permission to list SageMaker Images in your account	List			
ListInferenceComponents	Grants permission to list inference components	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListInferenceExperiments	Grants permission to list inference experiments	List			
ListInferenceRecommendationsJobSteps	Grants permission to list inference recommendations job steps	List			
ListInferenceRecommendationsJobs	Grants permission to list inference recommendations jobs	List			
ListLabelingJobs	Grants permission to list labeling jobs	List			
ListLabelingJobsForWorkteam	Grants permission to list labeling jobs for workteam	List	workteam*		
ListLineageGroups	Grants permission to list lineage groups	List			
ListMlflowApps	Grants permission to list SageMaker MLflow Apps in your account	List			
ListMlflowTrackingServers	Grants permission to list MLflow tracking servers	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListModelBiasJobDefinitions	Grants permission to list model bias job definitions	List			
ListModelCardExportJobs	Grants permission to list export jobs for a model card	List	model-card*		
ListModelCardVersions	Grants permission to list versions of a model card	List	model-card*		
ListModelCards	Grants permission to list model cards	List			
ListModelExplainabilityJobDefinitions	Grants permission to list model explainability job definitions	List			
ListModelMetadata	Grants permission to list model metadata for inference recommendations jobs	List			
ListModelPackageGroups	Grants permission to list ModelPackageGroups	List			
ListModelPackages	Grants permission to list ModelPackages	List	model-package		
ListModelQualityJobDefinitions	Grants permission to list model quality job definitions	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListModels	Grants permission to list the models created with the CreateModel API	List			
ListMonitoringAlertHistory	Grants permission to list the history of a monitoring alert	List			
ListMonitoringAlerts	Grants permission to list monitoring alerts	List			
ListMonitoringExecutions	Grants permission to list monitoring executions	List			
ListMonitoringSchedules	Grants permission to list monitoring schedules	List			
ListNotebookInstanceLifecycleConfigs	Grants permission to list the notebook instance lifecycle configurations that can be deployed using Amazon SageMaker	List			
ListNotebookInstances	Grants permission to list the Amazon SageMaker notebook instances in the requester's account in an AWS Region	List			
ListOptimizationJobs	Grants permission to list optimization jobs	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPartnerApps	Grants permission to list the Amazon SageMaker Partner AI Apps in your account	List			
ListPipelineExecutionSteps	Grants permission to list steps for a pipeline execution	List	pipeline-execution*		
ListPipelineExecutions	Grants permission to list executions for a pipeline	List	pipeline*		
ListPipelineParametersForExecution	Grants permission to list parameters for a pipeline execution	List	pipeline-execution*		
ListPipelineVersions	Grants permission to list versions of a pipeline	List	pipeline*		
ListPipelines	Grants permission to list pipelines	List			
ListProcessingJobs	Grants permission to list processing jobs	List			
ListProjects	Grants permission to list Projects	List			
ListResourceCatalogs	Grants permission to list resource catalogs	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSharedModelEvents [permission only]	Grants permission to list shared model events	List			
ListSharedModelVersions [permission only]	Grants permission to list shared model versions	List	shared-model*		
ListSharedModels [permission only]	Grants permission to list shared models	List			
ListSpaces	Grants permission to list the Spaces in your account	List			
ListStageDevices	Grants permission to list stage devices	List			
ListStudioLifecycleConfigs	Grants permission to list the Studio Lifecycle Configurations that can be deployed using Amazon SageMaker	List			
ListSubscribedWorkteams	Grants permission to list subscribed workteams	List			
ListTags	Grants permission to list the tag set associated with the specified resource	List	action		
			algorithm		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			app		
			app-image-config		
			artifact		
			automl-job		
			cluster		
			cluster-scheduler-config		
			code-repository		
			compilation-job		
			compute-quota		
			context		
			data-quality-job-definition		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			device		
			device-fleet		
			domain		
			edge-deployment-plan		
			edge-packaging-job		
			endpoint		
			endpoint-config		
			experiment		
			experiment-trial		
			experiment-trial-component		
			feature-group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			flow-definition		
			hub		
			hub-content		
			human-task-ui		
			hyper-parameter-tuning-job		
			image		
			inference-component		
			inference-recommendations-job		
			labeling-job		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			mlflow-tracking-server		
			model		
			model-bias-job-definition		
			model-card		
			model-explainability-job-definition		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-package	sagemaker:CurrentModelLifeCycleStageStatus sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	
			model-package-group		
			model-quality-job-definition		
			monitoring-schedule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			notebook-instance		
			notebook-instance-lifecycle-config		
			optimization-job		
			partner-app		
			pipeline		
			pipeline-execution		
			processing-job		
			project		
			reserved-capacity		
			space		
			studio-lifecycle-config		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			training-job		
			training-plan		
			transform-job		
			user-profile		
			workteam		
ListTrainingJobs	Grants permission to list training jobs	List			
ListTrainingJobsForHyperParameterTuningJob	Grants permission to list training jobs for a hyper parameter tuning job	List	hyper-parameter-tuning-job*		
ListTrainingPlans	Grants permission to list all the training plans that have been created in a specified account	List			
ListTransformJobs	Grants permission to list transform jobs	List			
ListTrialComponents	Grants permission to list trial components	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTrials	Grants permission to list trials	List			
ListUltraServersByReservedCapacity	Grants permission to list all UltraServers in a specified Reserved Capacity	List	reserved-capacity*		
ListUserProfiles	Grants permission to list the UserProfiles in your account	List			
ListWorkforces	Grants permission to list workforces	List			
ListWorkteams	Grants permission to list workteams	List			
PutLineageGroupPolicy	Grants permission to put a lineage group policy	Write			
PutModelPackageGroupPolicy	Grants permission to put a ModelPackageGroup policy	Write	model-package-group*		
PutRecord	Grants permission to put a record to a feature group	Write	feature-group*		
PutResourcePolicy [permission only]	Grants AWS Resource Access Manager permission to create a resource policy on a SageMaker resource that supports cross-account sharing	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
QueryLineage	Grants permission to explore the lineage graph	List			
RegisterDevices	Grants permission to register a set of devices	Write	device*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RenderUiTemplate	Grants permission to render a UI template used for a human annotation task	Read			iam:PassRole
RetryPipelineExecution	Grants permission to retry a pipeline execution	Write	pipeline-execution*		
Search	Grants permission to search for SageMaker objects	Read		sagemaker:SearchVisibilityCondition/${FilterKey}	
SearchTrainingPlanOfferings	Grants permissions to search for the available training plan offerings that best match specified capacity requirements	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendHeartbeat	Grants permission to publish heartbeat data from devices. After you deploy a model onto edge devices this api is used to report device status	Write	device*		
SendPipelineExecutionStepFailure	Grants permission to fail a pending callback step	Write	pipeline-execution*		
SendPipelineExecutionStepSuccess	Grants permission to succeed a pending callback step	Write	pipeline-execution*		
SendSharedModelEvent [permission only]	Grants permission to send a shared model event	Write	shared-model-event*		
StartEdgeDeploymentStage	Grants permission to start an edge deployment stage	Write	edge-deployment-plan*		
StartHumanLoop	Grants permission to start a human loop	Write	flow-definition*		
StartInferenceExperiment	Grants permission to start an inference experiment	Write	inference-experiment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartMlflowTrackingServer	Grants permission to start an MLfLow tracking server	Write	mlflow-tracking-server*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
StartMonitoringSchedule	Grants permission to start a monitoring schedule	Write	monitoring-schedule*		
StartNotebookInstance	Grants permission to start a notebook instance. This launches an EC2 instance with the latest version of the libraries and attaches your EBS volume	Write	notebook-instance*		
StartPipelineExecution	Grants permission to start a pipeline execution	Write	pipeline*		
				sagemaker:PipelineVersionId	
StartSession	Grants permission to start a remote session for a SageMaker space	Write	space*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopAutoMLJob	Grants permission to stop a running AutoML job	Write	automl-job*		
StopCompilationJob	Grants permission to stop a compilation job	Write	compilation-job*		
StopEdgeDeploymentStage	Grants permission to stop an edge deployment stage	Write	edge-deployment-plan*		
StopEdgePackagingJob	Grants permission to stop an edge packaging job	Write	edge-packaging-job*		
StopHumanLoop	Grants permission to stop a specified human loop	Write	human-loop*		
StopHyperParameterTuningJob	Grants permission to stop a running hyper parameter tuning job create via the CreateHyperParameterTuningJob	Write	hyper-parameter-tuning-job*		
StopInferenceExperiment	Grants permission to stop an inference experiment	Write	inference-experiment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopInferenceRecommendationsJob	Grants permission to stop an inference recommendations job	Write	inference-recommendations-job*		
StopLabelingJob	Grants permission to stop a labeling job. Any labels already generated will be exported before stopping	Write	labeling-job*		
StopMlflowTrackingServer	Grants permission to stop an MLflow tracking server	Write	mlflow-tracking-server*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
StopMonitoringSchedule	Grants permission to stop a monitoring schedule	Write	monitoring-schedule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopNotebookInstance	Grants permission to stop a notebook instance. This terminates the EC2 instance. Before terminating the instance, Amazon SageMaker disconnects the EBS volume from it. Amazon SageMaker preserves the EBS volume	Write	notebook-instance*		
StopOptimizationJob	Grants permission to stop an optimization job	Write	optimization-job*		
StopPipelineExecution	Grants permission to stop a pipeline execution	Write	pipeline-execution*		
StopProcessingJob	Grants permission to stop a processing job. To stop a job, Amazon SageMaker sends the algorithm the SIGTERM signal, which delays job termination for 120 seconds	Write	processing-job*		
StopTrainingJob	Grants permission to stop a training job. To stop a job, Amazon SageMaker sends the algorithm the SIGTERM signal, which delays job termination for 120 seconds	Write	training-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopTransformJob	Grants permission to stop a transform job. When Amazon SageMaker receives a StopTransformJob request, the status of the job changes to Stopping. After Amazon SageMaker stops the job, the status is set to Stopped	Write	transform-job*		
TrainHubModel	Grants permission to train a model in hub	Write	hub*		
			hub-content*		
UpdateAction	Grants permission to update an action	Write	action*		
UpdateAppImageConfig	Grants permission to update an AppImageConfig	Write	app-image-config*		
UpdateArtifact	Grants permission to update an artifact	Write	artifact*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCluster	Grants permission to update a SageMaker HyperPod cluster	Write	cluster*		ec2:DescribeImages ec2:DescribeSnapshots ec2:ModifyImageAttribute ec2:ModifySnapshotAttribute eks:AssociateAccessPolicy eks:CreateAccessEntry eks:DeleteAccessEntry eks:DescribeAccessEntry eks:DescribeCluster

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:PassRole sagemaker:BatchAddClusterNodes sagemaker:BatchDeleteClusterNodes
			reserved-capacity		
			training-plan		
				sagemaker:InstanceTypes sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateClusterInference [permission only]	Grants permission to update the inference operator for a SageMaker HyperPod cluster	Write	cluster*		eks:AssociateAccessPolicy eks:DescribeCluster eks:ListAssociatedAccessPolicies iam:PassRole sagemaker:DescribeCluster
UpdateClusterSchedulerConfig	Grants permission to update a cluster scheduler config	Write	cluster-scheduler-config*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateClusterSoftware	Grants permission to update platform software for a SageMaker HyperPod cluster	Write	cluster*		ec2:DescribeImages ec2:DescribeSnapshots ec2:ModifyImageAttribute ec2:ModifySnapshotAttribute eks:DescribeCluster
UpdateCodeRepository	Grants permission to update a CodeRepository	Write	code-repository*		
UpdateComputeQuota	Grants permission to update a compute quota	Write	compute-quota*		
UpdateContext	Grants permission to update a context	Write	context*		
UpdateDeviceFleet	Grants permission to update a device fleet	Write	device-fleet*		
UpdateDevices	Grants permission to update a set of devices	Write	device*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDomain	Grants permission to update a Domain	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:VpcSecurityGroupIds sagemaker:InstanceTypes sagemaker:DomainSharingOutputKmsKey sagemaker:ImageArns sagemaker:ImageVersionArns sagemaker:AppNetworkAccessType sagemaker:VpcSubnets sagemaker:StudioLi	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				fecycleConfigArns	
UpdateEndpoint	Grants permission to update an endpoint to use the endpoint configuration specified in the request	Write	endpoint*		
			endpoint-config*		
UpdateEndpointWeightsAndCapacities	Grants permission to update variant weight, capacity, or both of one or more variants associated with an endpoint	Write	endpoint*		
UpdateExperiment	Grants permission to update an experiment	Write	experiment*		
UpdateFeatureGroup	Grants permission to update a feature group	Write	feature-group*		
UpdateFeatureMetadata	Grants permission to update a feature metadata	Write	feature-group*		
UpdateHub	Grants permission to update hubs	Write	hub*		
UpdateHubContent	Grants permission to update hub content	Write	hub*		
			hub-content*		
UpdateHubContentReference	Grants permission to update hub content reference	Write	hub*		
			hub-content*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateImage	Grants permission to update the properties of a SageMaker Image	Write	image*		iam:PassRole
UpdateImageVersion	Grants permission to update the properties of a SageMaker ImageVersion	Write	image-version*		
UpdateInferenceComponent	Grants permission to update an inference component to use the specification and configurations specified in the request	Write	inference-component*		
UpdateInferenceComponentRuntimeConfig	Grants permission to update the runtime config of a given inference component	Write	inference-component*		
UpdateInferenceExperiment	Grants permission to update an inference experiment	Write	inference-experiment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateMlflowApp	Grants permission to update an MLflow app	Write	mlflow-app*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
UpdateMlflowTrackingServer	Grants permission to update an MLflow tracking server	Write	mlflow-tracking-server*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
UpdateModelCard	Grants permission to update a model card	Write	model-card*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateModelPackage	Grants permission to update a ModelPackage	Write	model-package*	sagemaker:CurrentModelLifeCycleStageStatus sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:ModelApprovalStatus sagemaker:CustomerMetadataProperties/${MetadataKey} sagemaker:CustomerMetadataPropertiesToRemove sagemaker:ModelLifeCycle:Stage sagemaker:ModelLifeCycle:StageStatus	
UpdateMonitoringAlert	Grants permission to update a monitoring alert	Write	monitoring-schedule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			monitoring-schedule-alert*		
UpdateMonitoringSchedule	Grants permission to update a monitoring schedule	Write	monitoring-schedule*		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:InstanceTypes sagemaker:MaxRuntimeInSeconds sagemaker:NetworkIsolation sagemaker:OutputKmsKey sagemaker:VolumeKmsKey sagemaker:VpcSecurityGroupIds	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:VpcSubnets sagemaker:InterContainerTrafficEncryption	
UpdateNotebookInstance	Grants permission to update a notebook instance. Notebook instance updates include upgrading or downgrading the EC2 instance used for your notebook instance to accommodate changes in your workload requirements	Write	notebook-instance*	sagemaker:AcceleratorTypes sagemaker:InstanceTypes sagemaker:MinimumInstanceMetadataServiceVersion sagemaker:RootAccess	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateNotebookInstanceLifecycleConfig	Grants permission to updates a notebook instance lifecycle configuration created with the CreateNotebookInstanceLifecycleConfig API	Write	notebook-instance-lifecycle-config*		
UpdatePartnerApp	Grants permission to update an Amazon SageMaker Partner AI App	Write	partner-app*	sagemaker:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
UpdatePipeline	Grants permission to update a pipeline	Write	pipeline*		iam:PassRole
UpdatePipelineExecution	Grants permission to update a pipeline execution	Write	pipeline-execution*		
UpdatePipelineVersion	Grants permission to update a pipeline version	Write	pipeline*		
				sagemaker:PipelineVersionId	
UpdateProject	Grants permission to update a Project	Write	project*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateSharedModel [permission only]	Grants permission to update a shared model	Write	shared-model*		
UpdateSpace	Grants permission to update a Space	Write	space*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:InstanceTypes sagemaker:ImageArns sagemaker:ImageVersionArns sagemaker:OwnerUserProfileArn sagemaker:RemoteAccess sagemaker:SpaceSharingType sagemaker:StudioLifecycleConfigArns	
UpdateTrainingJob	Grants permission to update a training job	Write	training-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:InstanceTypes sagemaker:KeepAlivePeriod sagemaker:EnableRemoteDebu	
UpdateTrial	Grants permission to update a trial	Write	experiment-trial*		
UpdateTrialComponent	Grants permission to update a trial component	Write	experiment-trial-component*		
UpdateUserProfile	Grants permission to update a UserProfile	Write	user-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:InstanceTypes sagemaker:VpcSecurityGroupIds sagemaker:InstanceTypes sagemaker:DomainSharingOutputKmsKey sagemaker:ImageArns sagemaker:ImageVersionArns sagemaker:StudioLifecycleConfigArns	
UpdateWorkforce	Grants permission to update a workforce	Write	workforce*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateWorkteam	Grants permission to update a workteam	Write	workteam*		

Resource types defined by Amazon SageMaker

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
device	`arn:${Partition}:sagemaker:${Region}:${Account}:device-fleet/${DeviceFleetName}/device/${DeviceName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
device-fleet	`arn:${Partition}:sagemaker:${Region}:${Account}:device-fleet/${DeviceFleetName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
edge-packaging-job	`arn:${Partition}:sagemaker:${Region}:${Account}:edge-packaging-job/${EdgePackagingJobName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
edge-deployment-plan	arn:${Partition}:sagemaker:${Region}:${Account}:edge-deployment/${EdgeDeploymentPlanName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
human-loop	arn:${Partition}:sagemaker:${Region}:${Account}:human-loop/${HumanLoopName}	
flow-definition	arn:${Partition}:sagemaker:${Region}:${Account}:flow-definition/${FlowDefinitionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
human-task-ui	arn:${Partition}:sagemaker:${Region}:${Account}:human-task-ui/${HumanTaskUiName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
hub	arn:${Partition}:sagemaker:${Region}:${Account}:hub/${HubName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
hub-content	arn:${Partition}:sagemaker:${Region}:${Account}:hub-content/${HubName}/${HubContentType}/${HubContentName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
inference-recommendations-job	arn:${Partition}:sagemaker:${Region}:${Account}:inference-recommendations-job/${InferenceRecommendationsJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
inference-experiment	arn:${Partition}:sagemaker:${Region}:${Account}:inference-experiment/${InferenceExperimentName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
labeling-job	arn:${Partition}:sagemaker:${Region}:${Account}:labeling-job/${LabelingJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
workteam	arn:${Partition}:sagemaker:${Region}:${Account}:workteam/${WorkteamName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
workforce	arn:${Partition}:sagemaker:${Region}:${Account}:workforce/${WorkforceName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
domain	arn:${Partition}:sagemaker:${Region}:${Account}:domain/${DomainId}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
user-profile	arn:${Partition}:sagemaker:${Region}:${Account}:user-profile/${DomainId}/${UserProfileName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
space	arn:${Partition}:sagemaker:${Region}:${Account}:space/${DomainId}/${SpaceName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
app	arn:${Partition}:sagemaker:${Region}:${Account}:app/${DomainId}/${UserProfileName}/${AppType}/${AppName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
app-image-config	arn:${Partition}:sagemaker:${Region}:${Account}:app-image-config/${AppImageConfigName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
studio-lifecycle-config	arn:${Partition}:sagemaker:${Region}:${Account}:studio-lifecycle-config/${StudioLifecycleConfigName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
notebook-instance	arn:${Partition}:sagemaker:${Region}:${Account}:notebook-instance/${NotebookInstanceName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
notebook-instance-lifecycle-config	arn:${Partition}:sagemaker:${Region}:${Account}:notebook-instance-lifecycle-config/${NotebookInstanceLifecycleConfigName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
code-repository	arn:${Partition}:sagemaker:${Region}:${Account}:code-repository/${CodeRepositoryName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
image	arn:${Partition}:sagemaker:${Region}:${Account}:image/${ImageName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
image-version	arn:${Partition}:sagemaker:${Region}:${Account}:image-version/${ImageName}/${Version}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
algorithm	arn:${Partition}:sagemaker:${Region}:${Account}:algorithm/${AlgorithmName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
cluster	arn:${Partition}:sagemaker:${Region}:${Account}:cluster/${ClusterId}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
training-job	arn:${Partition}:sagemaker:${Region}:${Account}:training-job/${TrainingJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
processing-job	arn:${Partition}:sagemaker:${Region}:${Account}:processing-job/${ProcessingJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
hyper-parameter-tuning-job	arn:${Partition}:sagemaker:${Region}:${Account}:hyper-parameter-tuning-job/${HyperParameterTuningJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
training-plan	arn:${Partition}:sagemaker:${Region}:${Account}:training-plan/${TrainingPlanName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
reserved-capacity	arn:${Partition}:sagemaker:${Region}:${Account}:reserved-capacity/${RandomString}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
project	arn:${Partition}:sagemaker:${Region}:${Account}:project/${ProjectName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
model-package	arn:${Partition}:sagemaker:${Region}:${Account}:model-package/${ModelPackageName}	aws:ResourceTag/${TagKey} sagemaker:CurrentCustomerMetadataProperties/${MetadataKey} sagemaker:CurrentModelLifeCycleStage sagemaker:CurrentModelLifeCycleStageStatus sagemaker:ResourceTag/${TagKey}
model-package-group	arn:${Partition}:sagemaker:${Region}:${Account}:model-package-group/${ModelPackageGroupName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model	arn:${Partition}:sagemaker:${Region}:${Account}:model/${ModelName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
endpoint-config	arn:${Partition}:sagemaker:${Region}:${Account}:endpoint-config/${EndpointConfigName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
endpoint	arn:${Partition}:sagemaker:${Region}:${Account}:endpoint/${EndpointName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
inference-component	arn:${Partition}:sagemaker:${Region}:${Account}:inference-component/${InferenceComponentName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
transform-job	arn:${Partition}:sagemaker:${Region}:${Account}:transform-job/${TransformJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
compilation-job	arn:${Partition}:sagemaker:${Region}:${Account}:compilation-job/${CompilationJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
optimization-job	arn:${Partition}:sagemaker:${Region}:${Account}:optimization-job/${OptimizationJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
automl-job	arn:${Partition}:sagemaker:${Region}:${Account}:automl-job/${AutoMLJobJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
monitoring-schedule	arn:${Partition}:sagemaker:${Region}:${Account}:monitoring-schedule/${MonitoringScheduleName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
monitoring-schedule-alert	arn:${Partition}:sagemaker:${Region}:${Account}:monitoring-schedule/${MonitoringScheduleName}/alert/${MonitoringScheduleAlertName}	
data-quality-job-definition	arn:${Partition}:sagemaker:${Region}:${Account}:data-quality-job-definition/${DataQualityJobDefinitionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-quality-job-definition	arn:${Partition}:sagemaker:${Region}:${Account}:model-quality-job-definition/${ModelQualityJobDefinitionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-bias-job-definition	arn:${Partition}:sagemaker:${Region}:${Account}:model-bias-job-definition/${ModelBiasJobDefinitionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-explainability-job-definition	arn:${Partition}:sagemaker:${Region}:${Account}:model-explainability-job-definition/${ModelExplainabilityJobDefinitionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
experiment	arn:${Partition}:sagemaker:${Region}:${Account}:experiment/${ExperimentName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
experiment-trial	arn:${Partition}:sagemaker:${Region}:${Account}:experiment-trial/${TrialName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
experiment-trial-component	arn:${Partition}:sagemaker:${Region}:${Account}:experiment-trial-component/${TrialComponentName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
feature-group	arn:${Partition}:sagemaker:${Region}:${Account}:feature-group/${FeatureGroupName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
pipeline	arn:${Partition}:sagemaker:${Region}:${Account}:pipeline/${PipelineName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
pipeline-execution	arn:${Partition}:sagemaker:${Region}:${Account}:pipeline/${PipelineName}/execution/${RandomString}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
artifact	arn:${Partition}:sagemaker:${Region}:${Account}:artifact/${HashOfArtifactSource}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
context	arn:${Partition}:sagemaker:${Region}:${Account}:context/${ContextName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
action	arn:${Partition}:sagemaker:${Region}:${Account}:action/${ActionName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
lineage-group	arn:${Partition}:sagemaker:${Region}:${Account}:lineage-group/${LineageGroupName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-card	arn:${Partition}:sagemaker:${Region}:${Account}:model-card/${ModelCardName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-card-export-job	arn:${Partition}:sagemaker:${Region}:${Account}:model-card/${ModelCardName}/export-job/${ExportJobName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
shared-model	arn:${Partition}:sagemaker:${Region}:${Account}:shared-model/${SharedModelId}	
shared-model-event	arn:${Partition}:sagemaker:${Region}:${Account}:shared-model-event/${EventId}	
sagemaker-catalog	arn:${Partition}:sagemaker:${Region}:${Account}:sagemaker-catalog/${ResourceCatalogName}	
mlflow-tracking-server	arn:${Partition}:sagemaker:${Region}:${Account}:mlflow-tracking-server/${MlflowTrackingServerName}	
mlflow-app	arn:${Partition}:sagemaker:${Region}:${Account}:mlflow-app/${MLflowAppId}	
compute-quota	arn:${Partition}:sagemaker:${Region}:${Account}:compute-quota/${ComputeQuotaId}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
cluster-scheduler-config	arn:${Partition}:sagemaker:${Region}:${Account}:cluster-scheduler-config/${ClusterSchedulerConfigId}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
partner-app	arn:${Partition}:sagemaker:${Region}:${Account}:partner-app/${AppId}	

Condition keys for Amazon SageMaker

Amazon SageMaker defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a key that is present in the request the user makes to the SageMaker service	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair	String
aws:TagKeys	Filters access by the list of all the tag key names associated with the resource in the request	ArrayOfString
sagemaker:AcceleratorTypes	Filters access by the list of all accelerator types associated with the resource in the request	ArrayOfString
sagemaker:AppNetworkAccessType	Filters access by the app network access type associated with the resource in the request	String
sagemaker:CurrentCustomerMetadataProperties/${MetadataKey}	Filters access by a current metadata key and value pair associated with the model-package resource	String

Condition keys	Description	Type
sagemaker:CurrentModelLifeCycleStage	Filters access by the current value of the Stage field in the model life cycle object associated with the model-package resource	String
sagemaker:CurrentModelLifeCycleStageStatus	Filters access by the current value of the StageStatus field in the model life cycle object associated with the model-package resource	String
sagemaker:CustomerMetadataProperties/${MetadataKey}	Filters access by a metadata key and value pair	String
sagemaker:CustomerMetadataPropertiesToRemove	Filters access by the list of metadata properties associated with the model-package resource in the request	ArrayOfString
sagemaker:DirectGatedModelAccess	Used to deny direct access to SageMaker gated ModelReferences	String
sagemaker:DirectInternetAccess	Filters access by the direct internet access associated with the resource in the request	String
sagemaker:DomainId	You can use the domainId as a policy variable to filter requests from specific SageMaker Domains	String

Condition keys	Description	Type
sagemaker:DomainSharingOutputKmsKey	Filters access by the Domain sharing output KMS key associated with the resource in the request	ARN
sagemaker:EnableRemoteDebug	Filters access by the remote debug config in the request	Bool
sagemaker:FeatureGroupDisableGlueTableCreation	Filters access by the DisableGlueTableCreation flag associated with the feature group resource in the request	Bool
sagemaker:FeatureGroupEnableOnlineStore	Filters access by the EnableOnlineStore flag associated with feature group in the request	Bool
sagemaker:FeatureGroupOfflineStoreConfig	Filters access by the presence of an OfflineStoreConfig in the feature group resource in the request. This access filter only supports the null-conditional operator	Bool
sagemaker:FeatureGroupOfflineStoreKmsKey	Filters access by the offline store kms key associated with the feature group resource in the request	ARN
sagemaker:FeatureGroupOfflineStoreS3Uri	Filters access by the offline store s3 uri associated with the feature group resource in the request	String

Condition keys	Description	Type
sagemaker:FeatureGroupOnlineStoreKmsKey	Filters access by the online store kms key associated with the feature group resource in the request	ARN
sagemaker:FileSystemAccessMode	Filters access by a file system access mode associated with the resource in the request	String
sagemaker:FileSystemDirectoryPath	Filters access by a file system directory path associated with the resource in the request	String
sagemaker:FileSystemId	Filters access by a file system ID associated with the resource in the request	String
sagemaker:FileSystemType	Filters access by a file system type associated with the resource in the request	String
sagemaker:HomeEfsFileSystemKmsKey	Filters access by a key that is present in the request the user makes to the SageMaker service. This key is deprecated. It has been replaced by sagemaker:VolumeKmsKey	ARN
sagemaker:ImageArns	Filters access by the list of all image arns associated with the resource in the request	ArrayOfARN
sagemaker:ImageVersionArns	Filters access by the list of all image version arns associated with the resource in the request	ArrayOfARN
sagemaker:InstanceTypes	Filters access by the list of all instance types associated with the resource in the request	ArrayOfString

Condition keys	Description	Type
sagemaker:InterContainerTrafficEncryption	Filters access by the inter container traffic encryption associated with the resource in the request	Bool
sagemaker:KeepAlivePeriod	Filters access by the keep-alive period associated with the resource in the request	Numeric
sagemaker:MaxRuntimeInSeconds	Filters access by the max runtime in seconds associated with the resource in the request	Numeric
sagemaker:MinimumInstanceMetadataServiceVersion	Filters access by the minimum instance metadata service version used by the resource in the request	String
sagemaker:ModelApprovalStatus	Filters access by the model approval status with the model-package in the request	String
sagemaker:ModelArn	Filters access by the model arn associated with the resource in the request	ARN
sagemaker:ModelLifeCycle:Stage	Filters access by stage field in the model life cycle object associated with the model-package resource in the request	String
sagemaker:ModelLifeCycle:StageStatus	Filters access by stageStatus field in the model life cycle object associated with the model-package resource in the request	String
sagemaker:NetworkIsolation	Filters access by the network isolation associated with the resource in the request	Bool

Condition keys	Description	Type
sagemaker:OutputKmsKey	Filters access by the output kms key associated with the resource in the request	ARN
sagemaker:OwnerUserProfileArn	Filters access by the OwnerUserProfile arn associated with the space in the request	ARN
sagemaker:PipelineVersionId	Filters access to specific version IDs of a Sagemaker pipeline	String
sagemaker:RemoteAccess	Filters access by the remote access flag associated with the space in the request	String
sagemaker:ResourceTag/	Filters access by the preface string for a tag key and value pair attached to a resource	String
sagemaker:ResourceTag/${TagKey}	Filters access by a tag key and value pair	String
sagemaker:RootAccess	Filters access by the root access associated with the resource in the request	String
sagemaker:SearchVisibilityCondition/${FilterKey}	Limits the results of your search request to the resources that you can access. ${FilterKey} is a key that the VisibilityConditions configuration presents in the Search request	String
sagemaker:ServerlessMaxConcurrency	Filters access by limiting maximum concurrency used for Serverless inference in the request	Numeric

Condition keys	Description	Type
sagemaker:ServerlessMemorySize	Filters access by limiting memory size used for Serverless inference in the request	Numeric
sagemaker:SpaceSharingType	Filters access by the sharing type associated with the space in the request	String
sagemaker:StudioLifecycleConfigArns	Filters access by the list of lifecycle configuration ARNs associated with the resource in the request	ArrayOfARN
sagemaker:TaggingAction	Filters access by the API actions to which a user can apply tags. Uses the name of the API operation that creates a taggable resource to filter access	String
sagemaker:TargetModel	Filters access by the target model associated with the Multi-Model Endpoint in the request	String
sagemaker:UserProfileName	You can use the UserProfileName as a policy variable to filter requests from specific user profiles within a SageMaker Domain. This context key is not applicable to user profiles within shared spaces	String
sagemaker:VolumeKmsKey	Filters access by the volume kms key associated with the resource in the request	ARN
sagemaker:VpcSecurityGroupIds	Filters access by the list of all VPC security group ids associated with the resource in the request	ArrayOfString
sagemaker:VpcSubnets	Filters access by the list of all VPC subnets associated with the resource in the request	ArrayOfString
sagemaker:WorkteamArn	Filters access by the workteam arn associated to the request	ARN

Condition keys	Description	Type
sagemaker:WorkteamType	Filters access by the workteam type associated to the request. This can be public-crowd, private-crowd or vendor-crowd	String

Actions, resources, and condition keys for AWS Savings Plans

AWS Savings Plans (service prefix: `savingsplans`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Savings Plans
- Resource types defined by AWS Savings Plans
- Condition keys for AWS Savings Plans

Actions defined by AWS Savings Plans

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSavingsPlan	Grants permission to create a savings plan	Write		aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
DeleteQueuedSavingsPlan	Grants permission to delete the queued savings plan associated with customers account	Write	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlanRates	Grants permission to describe the rates associated with customers savings plan	Read	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlans	Grants permission to describe the savings plans associated with customers account	Read	savingsplan*		
				aws:ResourceTag/${TagKey}	
DescribeSavingsPlansOfferingRates	Grants permission to describe the rates associated with savings plans offerings	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSavingsPlansOfferings	Grants permission to describe the savings plans offerings that customer is eligible to purchase	Read			
ListTagsForResource	Grants permission to list tags for a savings plan	List	savingsplan*		
ReturnSavingsPlan	Grants permission to return a savings plan	Write	savingsplan*		
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to tag a savings plan	Tagging	savingsplan*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag a savings plan	Tagging	savingsplan*		
				aws:TagKeys	

Resource types defined by AWS Savings Plans

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
savingsplan	`arn:${Partition}:savingsplans::${Account}:savingsplan/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS Savings Plans

AWS Savings Plans defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tags in the request	ArrayOfString

Actions, resources, and condition keys for AWS Secrets Manager

AWS Secrets Manager (service prefix: `secretsmanager`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Secrets Manager
- Resource types defined by AWS Secrets Manager
- Condition keys for AWS Secrets Manager

Actions defined by AWS Secrets Manager

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetSecretValue	Grants permission to retrieve and decrypt a list of secrets	List			
CancelRotateSecret	Grants permission to cancel an in-progress secret rotation	Write	Secret*		
				secretsmanager:SecretId secretsmanager:res	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
CreateSecret	Grants permission to create a secret that stores encrypted data that can be queried and rotated	Write	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:Name secretsmanager:Description secretsmanager:KmsKeyArn secretsmanager:KmsKeyId aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:AddReplicaRegions secretsmanager:ForceOverwriteReplicaSecret secretsmanager:Type	
DeleteResourcePolicy	Grants permission to delete the resource policy attached to a secret	Permissions management	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
DeleteSecret	Grants permission to delete a secret	Write	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:RecoveryWindowInDays secretsmanager:ForceDeleteWithoutRecovery secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
DescribeSecret	Grants permission to retrieve the metadata about a secret, but not the encrypted data	Read	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRandomPassword	Grants permission to generate a random string for use in password creation	Read			
GetResourcePolicy	Grants permission to get the resource policy attached to a secret	Read	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
GetSecretValue		Read	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to retrieve and decrypt the encrypted data				

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:VersionId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:resource/Type	
ListSecretVersionIds	Grants permission to list the available versions of a secret	Read	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
ListSecrets	Grants permission to list the available secrets	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutResourcePolicy	Grants permission to attach a resource policy to a secret	Permissions management	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:BlockPublicPolicy secretsmanager:SecretPrimaryRegion secretsmanager:res	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ource/ Type	
PutSecret Value	Grants permission to create a new version of the secret with new encrypted data	Write	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
	Grants permission to remove regions from replication	Write	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveRegionsFromReplication				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReplicateSecretToRegions	Grants permission to convert an existing secret to a multi-Region secret and begin replicating the secret to a list of new regions	Write	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:AddReplicaRegions	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:ForceOverwriteReplicaSecret secretsmanager:resource/Type	
RestoreSecret	Grants permission to cancel deletion of a secret	Write	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	
RotateSecret	Grants permission to start rotation of a secret	Write	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:RotationLambdaARN secretsmanager:resource/AllowRotationLambdaAr n secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:Mod	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ifyRotationRules secretsmanager:RotateImmediately secretsmanager:resource/Type secretsmanager:ExternalSecretRotationRoleArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopReplicationToReplica	Grants permission to remove the secret from replication and promote the secret to a regional secret in the replica Region	Write	Secret*	secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to add tags to a secret	Tagging	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId aws:RequestTag/${TagKey} aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:resource/Type	
UntagResource	Grants permission to remove tags from a secret	Tagging	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId aws:TagKeys secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSecret	Grants permission to update a secret with new metadata or with a new version of the encrypted data	Write	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:Description secretsmanager:KmsKeyArn secretsmanager:KmsKeyId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretPrimaryRegion secretsmanager:Type secretsmanager:resource/Type	
UpdateSecretVersionStage	Grants permission to move a stage from one secret to another	Write	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:VersionStage secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:res	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ource/ Type	
ValidateResourcePolicy	Grants permission to validate a resource policy before attaching policy	Permissions management	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion secretsmanager:resource/Type	

Resource types defined by AWS Secrets Manager

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
Secret	`arn:${Partition}:secretsmanager:${Region}:${Account}:secret:${SecretId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys secretsmanager:ResourceTag/tag-key secretsmanager:resource/AllowRotationLambdaArn secretsmanager:resource/Type

Condition keys for AWS Secrets Manager

AWS Secrets Manager defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a key that is present in the request the user makes to the Secrets Manager service	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the list of all the tag key names present in the request the user makes to the Secrets Manager service	ArrayOfString
secretsmanager:AddReplicaRegions	Filters access by the list of Regions in which to replicate the secret	ArrayOfString
secretsmanager:BlockPublicPolicy	Filters access by whether the resource policy blocks broad AWS account access	Bool
secretsmanager:Description	Filters access by the description text in the request	String
secretsmanager:ExternalSecretRotationRoleArn	Filters access by the managed external secret rotation role ARN in the request	ARN
secretsmanager:ForceDeleteWithoutRecovery	Filters access by whether the secret is to be deleted immediately without any recovery window	Bool
secretsmanager:For	Filters access by whether to overwrite a secret with the same name in the destination Region	Bool

Condition keys	Description	Type
ceOverwriteReplicaSecret		
secretsmanager:KmsKeyArn	Filters access by the key ARN of the KMS key in the request	ARN
secretsmanager:KmsKeyId	Filters access by the key identifier of the KMS key in the request. Deprecated: Use secretsmanager:KmsKeyArn	String
secretsmanager:ModifyRotationRules	Filters access by whether the rotation rules of the secret are to be modified	Bool
secretsmanager:Name	Filters access by the friendly name of the secret in the request	String
secretsmanager:RecoveryWindowInDays	Filters access by the number of days that Secrets Manager waits before it can delete the secret	Numeric
secretsmanager:ResourceTag/tag-key	Filters access by a tag key and value pair	String
secretsmanager:RotateImmediately	Filters access by whether the secret is to be rotated immediately	Bool
secretsmanager:RotationLambdaARN	Filters access by the ARN of the rotation Lambda function in the request	ARN

Condition keys	Description	Type
secretsmanager:SecretId	Filters access by the SecretID value in the request	ARN
secretsmanager:SecretPrimaryRegion	Filters access by primary region in which the secret is created if the secret is a multi-Region secret	String
secretsmanager:Type	Filters access by the managed external secret type in the request	String
secretsmanager:VersionId	Filters access by the unique identifier of the version of the secret in the request	String
secretsmanager:VersionStage	Filters access by the list of version stages in the request	String
secretsmanager:resource/AllowRotationLambdaArn	Filters access by the ARN of the rotation Lambda function associated with the secret	ARN
secretsmanager:resource/Type	Filters access by the managed external secret type associated with the secret	String

Actions, resources, and condition keys for AWS Security Hub

AWS Security Hub (service prefix: `securityhub`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.

- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Security Hub
- Resource types defined by AWS Security Hub
- Condition keys for AWS Security Hub

Actions defined by AWS Security Hub

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the

permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AcceptAdministratorInvitation	Grants permission to accept Security Hub invitations to become a member account	Write	hub		
AcceptInvitation	Grants permission to accept Security Hub invitations to become a member account	Write	hub		
BatchDeleteAutomationRules	Grants permission to delete one or more automation rules in Security Hub	Write	automation-rule*		
BatchDisableStandards	Grants permission to disable standards in Security Hub	Write	hub		
BatchEnableStandards	Grants permission to enable standards in Security Hub	Write	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetAutomationRules	Grants permission to retrieve a list of details for automation rules from Security Hub based on rule Amazon Resource Names (ARNs)	Read	automation-rule*		
BatchGetConfigurationPolicyAssociations	Grants permission to retrieve information about configuration policies associated with a specific list of member accounts and organizational units of the calling account's organization	Read			
BatchGetControlEvaluations [permission only]	Grants permission to get the enablement and compliance status of controls, the findings count for controls, and the overall security score for controls on the Security Hub console	Read	hub		
BatchGetSecurityControls	Grants permission to get details about specific security controls identified by ID or ARN	Read			securityhub:DescribeStandardsControls

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetStandardsControlAssociations	Grants permission to get the enablement status of a batch of security controls in standards	Read			securityhub:DescribeStandardsControls
BatchImportFindings	Grants permission to import findings into Security Hub from an integrated product	Write	product*		
				securityhub:TargetAccount	
BatchUpdateAutomationRules	Grants permission to update one or more automation rules from Security Hub based on rule Amazon Resource Names (ARNs) and input parameters	Write	automation-rule*		
BatchUpdateFindings	Grants permission to update customer-controlled fields for a selected set of Security Hub findings	Write	hub		
			hubv2		
				securityhub:ASFFSyntaxPath/${ASFFSyntaxPath} securityhub:OCSFSyntaxPath/${OCSFSyntaxPath}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchUpdateStandardsControlAssociations	Grants permission to update the enablement status of a batch of security controls in standards	Write			securityhub:UpdateStandardsControl
ConnectorRegistrationsV2	Grants permission to complete the OAuth 2.0 authorization code flow based on input parameters	Write			
CreateActionTarget	Grants permission to create custom actions in Security Hub	Write	hub		
CreateAggregatorV2	Grants permission to create an aggregatorV2, which configures data aggregation across Regions	Write			
CreateAutomationRule	Grants permission to create an automation rule based on input parameters	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAutomationRuleV2	Grants permission to create an automation rule V2 based on input parameters	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationPolicy	Grants permission to create a configuration policy to manage organization member settings in Security Hub	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectorV2	Grants permission to create a connector V2 based on input parameters	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingAggregator	Grants permission to create a finding aggregator, which contains the cross-Region finding aggregation configuration	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInsight	Grants permission to create insights in Security Hub. Insights are collections of related findings	Write	hub		
CreateMembers	Grants permission to create member accounts in Security Hub	Write	hub		
CreateTicketV2	Grants permission to create ticket for a selected OCSF finding	Write	connectorv2		
DeclineInvitations	Grants permission to decline Security Hub invitations to become a member account	Write	hub		
DeleteActionTarget	Grants permission to delete custom actions in Security Hub	Write	hub		
DeleteAggregatorV2	Grants permission to delete an aggregatorV2, which configures data aggregation across Regions	Write	aggregatorv2*		
DeleteAutomationRuleV2	Grants permission to delete an automation rule V2 in Security Hub	Write	automation-rulev2*		
DeleteConfigurationPolicy	Grants permission to delete an existing configuration policy	Write	configuration-policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteConnectorV2	Grants permission to delete a connector V2 in Security Hub	Write	connectorv2*		
DeleteFindingAggregator	Grants permission to delete a finding aggregator, which disables finding aggregation across Regions	Write	finding-aggregator*		
DeleteInsight	Grants permission to delete insights from Security Hub	Write	hub		
DeleteInvitations	Grants permission to delete Security Hub invitations to become a member account	Write	hub		
DeleteMembers	Grants permission to delete Security Hub member accounts	Write	hub		
DescribeActionTargets	Grants permission to retrieve a list of custom actions using the API	Read	hub		
DescribeHub	Grants permission to retrieve information about the hub resource in your account	Read	hub		
DescribeOrganizationConfiguration	Grants permission to describe the organization configuration for Security Hub	Read	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeProducts	Grants permission to retrieve information about the available Security Hub product integrations	Read	hub		
DescribeProductsV2	Grants permission to retrieve information about the available Security Hub V2 product integrations	Read	hubv2		
DescribeSecurityHubV2	Grants permission to retrieve information about the hub V2 resource in your account	Read			
DescribeStandards	Grants permission to retrieve information about Security Hub standards	Read	hub		
DescribeStandardsControls	Grants permission to retrieve information about Security Hub standards controls	Read	hub		
DisableImportFindingsForProduct	Grants permission to disable the findings importing for a Security Hub integrated product	Write	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableOrganizationAdminAccount	Grants permission to remove the Security Hub administrator account for your organization	Write	hub		organizations:DeregisterDelegatedAdministrator organizations:DescribeOrganization organizations:ListDelegatedAdministrators
DisableSecurityHub	Grants permission to disable Security Hub	Write	hub		
DisableSecurityHubV2	Grants permission to disable Security Hub V2	Write			
DisassociateFromAdministratorAccount	Grants permission to a Security Hub member account to disassociate from the associated administrator account	Write	hub		
DisassociateFromMasterAccount	Grants permission to a Security Hub member account to disassociate from the associated master account	Write	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateMembers	Grants permission to disassociate Security Hub member accounts from the associated administrator account	Write	hub		
EnableImportFindingsForProduct	Grants permission to enable the findings importing for a Security Hub integrated product	Write	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableOrganizationAdminAccount	Grants permission to designate a Security Hub administrator account for your organization	Write	hub		organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:ListAWSServiceAccessForOrganization organizations:ListDelegatedAdministrators organizations:RegisterDelegatedAdministrator
EnableSecurityHub	Grants permission to enable Security Hub	Write	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
EnableSecurityHubV2	Grants permission to enable Security Hub V2	Write		aws:RequestTag/${TagKey} aws:TagKeys	
GetAdhocInsightResults [permission only]	Grants permission to retrieve aggregated statistical data about the findings	Read	hub		
			hubv2		
GetAdministratorAccount	Grants permission to retrieve details about the Security Hub administrator account	Read	hub		
GetAggregatorV2	Grants permission to retrieve details for an aggregatorV2, which configures data aggregation across Regions	Read	aggregatorv2*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAutomationRuleV2	Grants permission to retrieve details for an automation rule V2 from Security Hub based on rule Amazon Resource Name (ARN)	Read	automation-rulev2*		
GetConfigurationPolicy	Grants permission to get a complete overview of one configuration policy created by the calling account	Read	configuration-policy*		
GetConfigurationPolicyAssociation	Grants permission to retrieve information about a configuration policy associated with a member account or organizational unit of the calling account's organization	Read			
GetConnectorV2	Grants permission to retrieve details for a connector V2 from Security Hub based on connector id	Read	connectorv2*		
GetControlFindingSummary [permission only]	Grants permission to retrieve a security score and counts of finding and control statuses for a security standard	Read	hub		
GetEnabledStandards	Grants permission to retrieve a list of the standards that are enabled in Security Hub	List	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFindingAggregator	Grants permission to retrieve details for a finding aggregator, which configures finding aggregation across Regions	Read	finding-aggregator*		
GetFindingHistory	Grants permission to retrieve a list of finding history from Security Hub	Read	hub		
GetFindings	Grants permission to retrieve a list of findings from Security Hub	Read	hub		
			hubv2		
GetFindingsTrendsV2	Grants permission to retrieve findings trends	Read	hubv2		
GetFreeTrialEndDate [permission only]	Grants permission to retrieve the end date for an account's free trial of Security Hub	Read	hub		
GetFreeTrialUsage [permission only]	Grants permission to retrieve information about Security Hub usage during the free trial period	Read	hub		
GetInsightFindingTrend [permission only]	Grants permission to retrieve an insight finding trend from Security Hub in order to generate a graph	Read	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInsightResults	Grants permission to retrieve insight results from Security Hub	Read	hub		
GetInsights	Grants permission to retrieve Security Hub insights	List	hub		
GetInvitationsCount	Grants permission to retrieve the count of Security Hub membership invitations sent to the account	Read	hub		
GetMasterAccount	Grants permission to retrieve details about the Security Hub master account	Read	hub		
GetMembers	Grants permission to retrieve the details of Security Hub member accounts	Read	hub		
GetResourcesStatisticsV2	Grants permission to retrieve aggregate statistics about resources	Read	hubv2		
GetResourcesTrendsV2	Grants permission to retrieve resources trends	Read	hubv2		
GetResourcesV2	Grants permission to retrieve a list of resources	Read	hubv2		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSecurityControlDefinition	Grants permission to get the definition details of a specific security control identified by ID	Read			securityhub:DescribeStandardsControls
GetUsage [permission only]	Grants permission to retrieve information about Security Hub usage by accounts	Read	hub		
InviteMembers	Grants permission to invite other AWS accounts to become Security Hub member accounts	Write	hub		
ListAggregatorsV2	Grants permission to retrieve a list of aggregatorsV2, which configures data aggregation across Regions	List			
ListAutomationRules	Grants permission to retrieve a list of automation rules and their metadata for the calling account from Security Hub	List			
ListAutomationRulesV2	Grants permission to retrieve a list of automation rules V2 and their metadata for the calling account from Security Hub	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListConfigurationPolicies	Grants permission to list the summaries of all configuration policies created by the calling account	List			
ListConfigurationPolicyAssociations	Grants permission to retrieve information about all configuration policies associationed with all member accounts and organizational units of the calling account's organization	List			
ListConnectorsV2	Grants permission to retrieve a list of connectors V2 and their metadata for the calling account from Security Hub	List			
ListControlEvaluationSummaries [permission only]	Grants permission to retrieve a list of controls for a standard, including the control IDs, statuses and finding counts	Read	hub		
ListEnabledProductsForImport	Grants permission to retrieve the Security Hub integrated products that are currently enabled	List	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListFindingAggregators	Grants permission to retrieve a list of finding aggregators, which contain the cross-Region finding aggregation configuration	List			
ListInvitations	Grants permission to retrieve the Security Hub invitations sent to the account	List	hub		
ListMembers	Grants permission to retrieve details about Security Hub member accounts associated with the administrator account	List	hub		
ListOrganizationAdminAccounts	Grants permission to list the Security Hub administrator accounts for your organization	List	hub		organizations:DescribeOrganization organizations:ListDelegatedAdministrators
ListSecurityControlDefinitions	Grants permission to retrieve a list of security control definitions, which contain details for security controls in the current region	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListStandardsControlAssociations	Grants permission to list the enablement status of a security control in standards	List			securityhub:DescribeStandardsControls
ListTagsForResource	Grants permission to list of tags associated with a resource	Read	automation-rule		
			configuration-policy		
			hub		
SendFindingsEvents [permission only]	Grants permission to use a custom action to send Security Hub findings to Amazon EventBridge	Read	hub		
SendInsightEvents [permission only]	Grants permission to use a custom action to send Security Hub insights to Amazon EventBridge	Read	hub		
StartConfigurationPolicyAssociation	Grants permission to associate a configuration policy with a member account or organizational unit in the calling account's organization	Write	configuration-policy		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartConfiguration PolicyDisassociation	Grants permission to remove a configuration policy association from a member account or organizational unit in the calling account's organization	Write	configuration-policy		
TagResource	Grants permission to add tags to a Security Hub resource	Tagging	aggregatorv2		
			automation-rule		
			automation-rulev2		
			configuration-policy		
			connectorv2		
			hub		
			hubv2		
UntagResource	Grants permission to remove tags from a Security Hub resource	Tagging	aggregatorv2		
			automation-rule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			automation-rulev2		
			configuration-policy		
			connectorv2		
			hub		
			hubv2		
UpdateActionTarget	Grants permission to update custom actions in Security Hub	Write	hub		
UpdateAggregatorV2	Grants permission to update an aggregatorV2, which configures data aggregation across Regions	Write	aggregatorv2*		
UpdateAutomationRuleV2	Grants permission to update an automation rule V2 in Security Hub based on rule Amazon Resource Name (ARN) and input parameters	Write	automation-rulev2*		
UpdateConfigurationPolicy	Grants permission to update an existing configuration policy	Write	configuration-policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateConnectorV2	Grants permission to update a connector V2 in Security Hub based on connector id and input parameters	Write	connectorv2*		
UpdateFindingAggregator	Grants permission to update a finding aggregator, which contains the cross-Region finding aggregation configuration	Write	finding-aggregator*		
UpdateFindings	Grants permission to update Security Hub findings	Write	hub		
UpdateInsight	Grants permission to update insights in Security Hub	Write	hub		
UpdateOrganizationConfiguration	Grants permission to update the organization configuration for Security Hub	Write	hub		
UpdateSecurityControl	Grants permission to update properties of a specific security control identified by ID or ARN	Write			securityhub:UpdateStandardsControl
UpdateSecurityHubConfiguration	Grants permission to update Security Hub configuration	Write	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateStandardsControl	Grants permission to update Security Hub standards controls	Write	hub		

Resource types defined by AWS Security Hub

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
hub	`arn:${Partition}:securityhub:${Region}:${Account}:hub/default`	aws:ResourceTag/${TagKey}
hubv2	`arn:${Partition}:securityhub:${Region}:${Account}:hubv2/${HubV2Id}`	aws:ResourceTag/${TagKey}
product	`arn:${Partition}:securityhub:${Region}:${Account}:product/${Company}/${ProductId}`	
finding-aggregator	`arn:${Partition}:securityhub:${Region}:${Account}:finding-aggregator/${FindingAggregatorId}`	
aggregatorv2	`arn:${Partition}:securityhub:${Region}:${Account}:aggregatorv2/${AggregatorV2Id}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
automation-rule	arn:${Partition}:securityhub:${Region}:${Account}:automation-rule/${AutomationRuleId}	aws:ResourceTag/${TagKey}
automation-rulev2	arn:${Partition}:securityhub:${Region}:${Account}:automation-rulev2/${AutomationRuleV2Id}	aws:ResourceTag/${TagKey}
configuration-policy	arn:${Partition}:securityhub:${Region}:${Account}:configuration-policy/${ConfigurationPolicyId}	aws:ResourceTag/${TagKey}
connectorv2	arn:${Partition}:securityhub:${Region}:${Account}:connectorv2/${ConnectorV2Id}	aws:ResourceTag/${TagKey}

Condition keys for AWS Security Hub

AWS Security Hub defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by actions based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by actions based on tag key-value pairs attached to the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by actions based on the presence of tag keys in the request	ArrayOfString
securityhub:ASFFSyntaxPath/${ASFFSyntaxPath}	Filters access by the specified fields and values in the request	String
securityhub:OCSFSyntaxPath/${OCSFSyntaxPath}	Filters access by the specified fields and values in the request	String
securityhub:TargetAccount	Filters access by the AwsAccountId field that is specified in the request	String

Actions, resources, and condition keys for AWS Security Token Service

AWS Security Token Service (service prefix: `sts`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Security Token Service
- Resource types defined by AWS Security Token Service
- Condition keys for AWS Security Token Service

Actions defined by AWS Security Token Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssumeRole	Grants permission to obtain a set of temporary security credentials that you can use to access AWS resources that you might not normally have access to	Write	role*	aws:TagKeys aws:RequestTag/${TagKey} sts:TransitiveTagKeys sts:ExternalId sts:RoleSessionName iam:ResourceTag/${TagKey} sts:SourceIdentity	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				cognito-identity.amazonaws.com:amr cognito-identity.amazonaws.com:aud cognito-identity.amazonaws.com:sub www.amazn.com:app_id www.amazn.com:user_id graph.facebook.com:app_id graph.facebook.com:id accounts.google.com:aud	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				accounts.google.com:sub saml:namequalifier saml:sub saml:sub_type	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssumeRoleWithSAML	Grants permission to obtain a set of temporary security credentials for users who have been authenticated via a SAML authentication response	Write	role*		
				saml:namequalifier saml:sub saml:sub_type saml:aud saml:iss saml:doc saml:cn saml:commonName saml:eduorghomepageuri saml:eduorgidentityauthnpolicyuri saml:eduorglegalname	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				saml:eduorgsuperioruri saml:eduorgwhitepagesuri saml:edupersonaffiliation saml:edupersonassurance saml:edupersonentitlement saml:edupersonnickname saml:edupersonorgdn saml:edupersonorgunitdn saml:edupersonprim	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aryaffiliation saml:edupersonprimaryorgunitdn saml:edupersonprincipalname saml:edupersonscopedaffiliation saml:edupersontargetedid saml:givenName saml:mail saml:name saml:organizationStatus saml:primaryGroupSID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				saml:surname saml:uid saml:x500UniqueIdentifier aws:TagKeys aws:RequestTag/${TagKey} sts:TransitiveTagKeys sts:SourceIdentity sts:RoleSessionName	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssumeRoleWithWebIdentity	Grants permission to obtain a set of temporary security credentials for users who have been authenticated in a mobile or web application with a web identity provider	Write	role*		
				cognito-identity.amazonaws.com:amr cognito-identity.amazonaws.com:aud cognito-identity.amazonaws.com:sub www.amazon.com:app_id www.amazon.com:user_id graph.facebook.com:app_id graph.facebook.com:id	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				accounts.google.com:aud accounts.google.com:oaud accounts.google.com:sub aws:TagKeys aws:RequestTag/${TagKey} sts:TransitiveTagKeys sts:SourceIdentity sts:RoleSessionName	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssumeRoot	Grants permission to obtain a set of temporary security credentials that you can use to perform privileged tasks in member accounts in your organization	Write	root-user *		
				sts:TaskPolicyArn	
DecodeAuthorizationMessage	Grants permission to decode additional information about the authorization status of a request from an encoded message returned in response to an AWS request	Write			
GetAccessKeyInfo	Grants permission to obtain details about the access key id passed as a parameter to the request	Read			
GetCallerIdentity	Grants permission to obtain details about the IAM identity whose credentials are used to call the API	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDelegatedAccessToken	Returns temporary security credentials for accessing an AWS account after temporary delegation request approval. This API requires the tradeInToken provided upon request delegation approval and is intended to be used only by Amazon or AWS Partners	Write			
GetFederationToken	Grants permission to obtain a set of temporary security credentials (consisting of an access key ID, a secret access key, and a security token) for a federated user	Read	federated-user		
			user		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	
GetServiceBearerToken [permission only]	Grants permission to obtain a STS bearer token for an AWS root user, IAM role, or an IAM user	Read		sts:AWSServiceName	
				sts:DurationSeconds	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSessionToken	Grants permission to obtain a set of temporary security credentials (consisting of an access key ID, a secret access key, and a security token) for an AWS account or IAM user	Read			
GetWebIdentityToken	Grants permission to obtain a short-lived, publicly verifiable JSON Web Token (JWT) that represents the calling IAM principal's identity	Write		sts:DurationSeconds sts:IdentityTokenAudience sts:SigningAlgorithm aws:TagKeys aws:RequestTag/${TagKey}	
SetContext [permission only]	Grants permission to set context keys on a STS session	Write	role self-session		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sts:RequestContext/${ContextKey} sts:RequestContextProviders	
SetSourceIdentity [permission only]	Grants permission to set a source identity on a STS session	Write	role		
			user		
				sts:SourceIdentity	
TagGetWebIdentityToken [permission only]	Grants permission to add tags to the JSON Web Token (JWT) generated by the GetWebIdentityToken API	Tagging		aws:TagKeys aws:RequestTag/${TagKey}	
TagSession [permission only]	Grants permission to add tags to a STS session	Tagging	role		
			user		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} sts:TransitiveTagKeys saml:aud	

Resource types defined by AWS Security Token Service

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
role	`arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}`	aws:ResourceTag/${TagKey} iam:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
user	arn:${Partition}:iam::${Account}:user/${UserNameWithPath}	
root-user	arn:${Partition}:iam::${Account}:root	
self-session	arn:${Partition}:sts::${Account}:self	
context-provider	arn:${Partition}:iam::aws:contextProvider/${ContextProviderName}	
federated-user	arn:${Partition}:sts::${Account}:federated-user/${FederatedUserName}	

Condition keys for AWS Security Token Service

AWS Security Token Service defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
accounts.google.com:aud	Filters access by the Google application ID	String
accounts.google.com:oaud	Filters access by the Google audience	String
accounts.google.com:sub	Filters access by the subject of the claim (the Google user ID)	String

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
cognito-identity.amazonaws.com:amr	Filters access by the login information for Amazon Cognito	String
cognito-identity.amazonaws.com:aud	Filters access by the Amazon Cognito identity pool ID	String
cognito-identity.amazonaws.com:sub	Filters access by the subject of the claim (the Amazon Cognito user ID)	String
graph.facebook.com:app_id	Filters access by the Facebook application ID	String
graph.facebook.com:id	Filters access by the Facebook user ID	String
iam:ResourceTag/${TagKey}	Filters access by the tags that are attached to the role that is being assumed	String

Condition keys	Description	Type
saml:aud	Filters access by the endpoint URL to which SAML assertions are presented	String
saml:cn	Filters access by the eduOrg attribute	ArrayOfString
saml:commonName	Filters access by the commonName attribute	String
saml:doc	Filters access by on the principal that was used to assume the role	String
saml:eduorghomepageuri	Filters access by the eduOrg attribute	ArrayOfString
saml:eduorgidentityauthnpolicyuri	Filters access by the eduOrg attribute	ArrayOfString
saml:eduorglegalname	Filters access by the eduOrg attribute	ArrayOfString
saml:eduorgsuperioruri	Filters access by the eduOrg attribute	ArrayOfString
saml:eduorgwhitepagesuri	Filters access by the eduOrg attribute	ArrayOfString
saml:edupersonaffiliation	Filters access by the eduPerson attribute	ArrayOfString
saml:edupersonassurance	Filters access by the eduPerson attribute	ArrayOfString
saml:edupersonentitlement	Filters access by the eduPerson attribute	ArrayOfString

Condition keys	Description	Type
saml:edupersonnickname	Filters access by the eduPerson attribute	ArrayOfString
saml:edupersonorgdn	Filters access by the eduPerson attribute	String
saml:edupersonorgunitdn	Filters access by the eduPerson attribute	ArrayOfString
saml:edupersonprimaryaffiliation	Filters access by the eduPerson attribute	String
saml:edupersonprimaryorgunitdn	Filters access by the eduPerson attribute	String
saml:edupersonprincipalname	Filters access by the eduPerson attribute	String
saml:edupersonscopedaffiliation	Filters access by the eduPerson attribute	ArrayOfString
saml:edupersontargetedid	Filters access by the eduPerson attribute	ArrayOfString
saml:givenName	Filters access by the givenName attribute	String
saml:iss	Filters access by on the issuer, which is represented by a URN	String
saml:mail	Filters access by the mail attribute	String
saml:name	Filters access by the name attribute	String

Condition keys	Description	Type
saml:name qualifier	Filters access by the hash value of the issuer, account ID, and friendly name	String
saml:orga nizationStatus	Filters access by the organizationStatus attribute	String
saml:prim aryGroupSID	Filters access by the primaryGroupSID attribute	String
saml:sub	Filters access by the subject of the claim (the SAML user ID)	String
saml:sub_type	Filters access by the value persistent, transient, or the full Format URI	String
saml:surname	Filters access by the surname attribute	String
saml:uid	Filters access by the uid attribute	String
saml:x500 UniqueIdentifier	Filters access by the uid attribute	String
sts:AWSSe rviceName	Filters access by the service that is obtaining a bearer token	String
sts:Durat ionSeconds	Filters access by the duration in seconds when getting a bearer token	String
sts:ExternalId	Filters access by the unique identifier required when you assume a role in another account	String
sts:Ident ityTokenA udience	Filters access by the audience that is passed in the request	String
sts:Reque stContext/ ${ContextKey}	Filters access by the session context key-value pairs embedded in the signed context assertion retrieved from a trusted context provider	String

Condition keys	Description	Type
sts:RequestContextProviders	Filters access by the context provider ARNs	ArrayOfARN
sts:RoleSessionName	Filters access by the role session name required when you assume a role	String
sts:SigningAlgorithm	Filters access by the signing algorithm that is passed in the request	String
sts:SourceIdentity	Filters access by the source identity that is passed in the request	String
sts:TaskPolicyArn	Filters access by TaskPolicyARN	String
sts:TransitiveTagKeys	Filters access by the transitive tag keys that are passed in the request	ArrayOfString
www.amazon.com:app_id	Filters access by the Login with Amazon application ID	String
www.amazon.com:user_id	Filters access by the Login with Amazon user ID	String

Actions, resources, and condition keys for Amazon SES

Amazon SES (service prefix: `ses`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon SES
- Resource types defined by Amazon SES
- Condition keys for Amazon SES

Actions defined by Amazon SES

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CloneReceiptRuleSet	Grants permission to create a receipt rule set by cloning an existing one	Write		ses:ApiVersion	
CreateConfigurationSet	Grants permission to create a new configuration set	Write		ses:ApiVersion	
CreateConfigurationSetEventDestination	Grants permission to create a configuration set event destination	Write		ses:ApiVersion	
CreateConfigurationSetTrackingOptions	Grants permission to creates an association between a configuration set and a custom domain for open and click event tracking	Write		ses:ApiVersion	
CreateCustomVerificationEmailTemplate	Grants permission to create a new custom verification email template	Write		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateReceiptFilter	Grants permission to create a new IP address filter	Write		ses:ApiVersion	
CreateReceiptRule	Grants permission to create a receipt rule	Write		ses:ApiVersion	
CreateReceiptRuleSet	Grants permission to create an empty receipt rule set	Write		ses:ApiVersion	
CreateTemplate	Grants permission to creates an email template	Write		ses:ApiVersion	
DeleteConfigurationSet	Grants permission to delete an existing configuration set	Write		ses:ApiVersion	
DeleteConfigurationSetEventDestination	Grants permission to delete an event destination	Write		ses:ApiVersion	
DeleteConfigurationSetTrackingOptions	Grants permission to delete an association between a configuration set and a custom domain for open and click event tracking	Write		ses:ApiVersion	
DeleteCustomVerificationEmailTemplate	Grants permission to delete an existing custom verification email template	Write		ses:ApiVersion	
DeleteIdentity	Grants permission to delete the specified identity	Write		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteIdentityPolicy	Grants permission to delete the specified sending authorization policy for the given identity (an email address or a domain)	Permissions management		ses:ApiVersion	
DeleteReceiptFilter	Grants permission to delete the specified IP address filter	Write		ses:ApiVersion	
DeleteReceiptRule	Grants permission to delete the specified receipt rule	Write		ses:ApiVersion	
DeleteReceiptRuleSet	Grants permission to delete the specified receipt rule set and all of the receipt rules it contains	Write		ses:ApiVersion	
DeleteTemplate	Grants permission to delete an email template	Write		ses:ApiVersion	
DeleteVerifiedEmailAddress	Grants permission to delete the specified email address from the list of verified addresses	Write		ses:ApiVersion	
DescribeActiveReceiptRuleSet	Grants permission to return the metadata and receipt rules for the receipt rule set that is currently active	Read		ses:ApiVersion	
DescribeConfigurationSet	Grants permission to return the details of the specified configuration set	Read		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeReceiptRule	Grants permission to return the details of the specified receipt rule	Read		ses:ApiVersion	
DescribeReceiptRuleSet	Grants permission to return the details of the specified receipt rule set	Read		ses:ApiVersion	
GetAccountSendingEnabled	Grants permission to return the email sending status of your account	Read		ses:ApiVersion	
GetCustomVerificationEmailTemplate	Grants permission to return the custom email verification template for the template name you specify	Read		ses:ApiVersion	
GetIdentityDkimAttributes	Grants permission to return the current status of Easy DKIM signing for an entity	Read		ses:ApiVersion	
GetIdentityMailFromDomainAttributes	Grants permission to return the custom MAIL FROM attributes for a list of identities (email addresses and/or domains)	Read		ses:ApiVersion	
GetIdentityNotificationAttributes	Grants permission to return a structure describing identity notification attributes for a list of verified identities (email addresses and/or domains),	Read		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIdentityPolicies	Grants permission to return the requested sending authorization policies for the given identity (an email address or a domain)	Read		ses:ApiVersion	
GetIdentityVerificationAttributes	Grants permission to return the verification status and (for domain identities) the verification token for a list of identities	Read		ses:ApiVersion	
GetSendQuota	Grants permission to return the user's current sending limits	Read		ses:ApiVersion	
GetSendStatistics	Grants permission to returns the user's sending statistics	Read		ses:ApiVersion	
GetTemplate	Grants permission to return the template object, which includes the subject line, HTML par, and text part for the template you specify	Read		ses:ApiVersion	
ListConfigurationSets	Grants permission to list all of the configuration sets for your account	List		ses:ApiVersion	
ListCustomVerificationEmailTemplates	Grants permission to list all of the existing custom verification email templates for your account	List		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListIdentities	Grants permission to list the email identities for your account	List		ses:ApiVersion	
ListIdentityPolicies	Grants permission to list all of the email templates for your account	List		ses:ApiVersion	
ListReceiptFilters	Grants permission to list the IP address filters associated with your account	Read		ses:ApiVersion	
ListReceiptRuleSets	Grants permission to list the receipt rule sets that exist under your account	Read		ses:ApiVersion	
ListTemplates	Grants permission to list the email templates present in your account	List		ses:ApiVersion	
ListVerifiedEmailAddresses	Grants permission to list all of the email addresses that have been verified in your account	Read		ses:ApiVersion	
PutConfigurationSetDeliveryOptions	Grants permission to add or update the delivery options for a configuration set	Write		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutIdentityPolicy	Grants permission to add or update a sending authorization policy for the specified identity (an email address or a domain)	Permissions management		ses:ApiVersion	
ReorderReceiptRuleSet	Grants permission to reorder the receipt rules within a receipt rule set	Write		ses:ApiVersion	
SendBounce	Grants permission to generate and send a bounce message to the sender of an email you received through Amazon SES	Write	identity*		
				ses:ApiVersion ses:FromAddress	
SendBulkTemplatedEmail	Grants permission to compose an email message to multiple destinations	Write	identity*		
			template*		
			configuration-set		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendCustomVerificationEmail	Grants permission to add an email address to the list of identities and attempts to verify it for your account	Write	identity*		
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendEmail	Grants permission to send an email message	Write	identity*		
			configuration-set		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendRawEmail	Grants permission to send an email message, with header and content specified by the client	Write	identity* configuration-set		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SendTemplatedEmail	Grants permission to compose an email message using an email template	Write	identity*		
			template*		
			configuration-set		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients	
SetActiveReceiptRuleSet	Grants permission to set the specified receipt rule set as the active receipt rule set	Write		ses:ApiVersion	
SetIdentityDkimEnabled	Grants permission to enable or disable Easy DKIM signing of email sent from an identity	Write		ses:ApiVersion	
SetIdentityFeedbackForwardingEnabled	Grants permission to enable or disable whether Amazon SES forwards bounce and complaint notifications for an identity (an email address or a domain)	Write		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetIdentityHeadersInNotificationsEnabled	Grants permission to set whether Amazon SES includes the original email headers in the Amazon Simple Notification Service (Amazon SNS) notifications of a specified type for a given identity (an email address or a domain)	Write		ses:ApiVersion	
SetIdentityMailFromDomain	Grants permission to enable or disable the custom MAIL FROM domain setup for a verified identity	Write		ses:ApiVersion	
SetIdentityNotificationTopic	Grants permission to set an Amazon Simple Notification Service (Amazon SNS) topic to use when delivering notifications for a verified identity	Write		ses:ApiVersion	
SetReceiptRulePosition	Grants permission to set the position of the specified receipt rule in the receipt rule set	Write		ses:ApiVersion	
TestRenderTemplate	Grants permission to create a preview of the MIME content of an email when provided with a template and a set of replacement data	Write		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAccountSendingEnabled	Grants permission to enable or disable email sending for your account	Write		ses:ApiVersion	
UpdateConfigurationSetEventDestination	Grants permission to update the event destination of a configuration set	Write		ses:ApiVersion	
UpdateConfigurationSetReputationMetricsEnabled	Grants permission to enable or disable the publishing of reputation metrics for emails sent using a specific configuration set	Write		ses:ApiVersion	
UpdateConfigurationSetSendingEnabled	Grants permission to enable or disable email sending for messages sent using a specific configuration set	Write		ses:ApiVersion	
UpdateConfigurationSetTrackingOptions	Grants permission to modify an association between a configuration set and a custom domain for open and click event tracking	Write		ses:ApiVersion	
UpdateCustomVerificationEmailTemplate	Grants permission to update an existing custom verification email template	Write		ses:ApiVersion	
UpdateReceiptRule	Grants permission to update a receipt rule	Write		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateTemplate	Grants permission to update an email template	Write		ses:ApiVersion	
VerifyDomainDkim	Grants permission to return a set of DKIM tokens for a domain	Write		ses:ApiVersion	
VerifyDomainIdentity	Grants permission to verify a domain	Write		ses:ApiVersion	
VerifyEmailAddress	Grants permission to verify an email address	Write		ses:ApiVersion	
VerifyEmailIdentity	Grants permission to verify an email identity	Write		ses:ApiVersion	

Resource types defined by Amazon SES

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
configuration-set	`arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	

Resource types	ARN	Condition keys
custom-verification-email-template	arn:${Partition}:ses:${Region}:${Account}:custom-verification-email-template/${TemplateName}	
identity	arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}	
template	arn:${Partition}:ses:${Region}:${Account}:template/${TemplateName}	

Condition keys for Amazon SES

Amazon SES defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
ses:ApiVersion	Filters actions based on the SES API version	String
ses:FeedbackAddress	Filters actions based on the "Return-Path" address, which specifies where bounces and complaints are sent by email feedback forwarding	String
ses:FromAddress	Filters actions based on the "From" address of a message	String
ses:FromDisplayName	Filters actions based on the "From" address that is used as the display name of a message	String

Condition keys	Description	Type
ses:Recipients	Filters actions based on the recipient addresses of a message, which include the "To", "CC", and "BCC" addresses	ArrayOfString

Actions, resources, and condition keys for Amazon Simple Email Service - Mail Manager

Amazon Simple Email Service - Mail Manager (service prefix: `ses`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Simple Email Service - Mail Manager
- Resource types defined by Amazon Simple Email Service - Mail Manager
- Condition keys for Amazon Simple Email Service - Mail Manager

Actions defined by Amazon Simple Email Service - Mail Manager

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllowVendedLogDeliveryForResource [permission only]	Grants permission to configure vended log delivery for Mail Manager resources	Permissions management	mailmanager-ingress-point		
			mailmanager-rule-set		
CreateAddonInstance	Grants permission to create an addon instance	Write		aws:RequestTag/${TagKey} aws:TagKeys ses:AddonSubscriptionArn	
CreateAddonSubscription	Grants permission to create an addon subscription	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAddressList	Grants permission to create an address list	Write		aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateAddressListImportJob	Grants permission to create an import job on an address list	Write	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
CreateArchive	Grants permission to create an archive	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIngressPoint	Grants permission to create an ingress point	Write		aws:RequestTag/${TagKey} aws:TagKeys ses:MailManagerRuleSetArn ses:MailManagerTrafficPolicyArn	ec2:DescribeVpcEndpoints iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRelay	Grants permission to create a SMTP relay	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleSet	Grants permission to create a rule set	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTrafficPolicy	Grants permission to create a traffic policy	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAddonInstance	Grants permission to delete an addon instance	Write	addon-instance*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAddonSubscription	Grants permission to delete an addon subscription	Write	addon-subscription*		
				aws:RequestTag/${TagKey}	
DeleteAddressList	Grants permission to delete an address list	Write	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
DeleteArchive	Grants permission to delete an archive	Write	mailmanager-archive*		
				aws:RequestTag/${TagKey}	
DeleteIngressPoint	Grants permission to delete an ingress point	Write	mailmanager-ingress-point*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRelay	Grants permission to delete a SMTP relay	Write	mailmanager-smtp-relay*		
				aws:RequestTag/${TagKey}	
DeleteRuleSet	Grants permission to delete a rule set	Write	mailmanager-rule-set*		
				aws:RequestTag/${TagKey}	
DeleteTrafficPolicy	Grants permission to delete a traffic point	Write	mailmanager-traffic-policy*		
				aws:RequestTag/${TagKey}	
DeregisterMemberFromAddressList	Grants permission to remove a member from an address list	Write	mailmanager-address-list*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAddonInstance	Grants permission to get information about an addon instance	Read	addon-instance*		
				aws:RequestTag/${TagKey}	
GetAddonSubscription	Grants permission to get information about an addon subscription	Read	addon-subscription*		
				aws:RequestTag/${TagKey}	
GetAddressList	Grants permission to get information about an address list	Read	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetAddressListImportJob	Grants permission to get information about an import job on an address list	Read	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetArchive	Grants permission to get information about an archive	Read	mailmanager-archive*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey}	
GetArchiveExport	Grants permission to get information about an archive export	Read	mailmanager-archive*		
GetArchiveMessage	Grants permission to retrieve archived message	Read	mailmanager-archive*		
GetArchiveMessageContent	Grants permission to retrieve archived message content	Read	mailmanager-archive*		
GetArchiveSearch	Grants permission to get information about a search	Read	mailmanager-archive*		
GetArchiveSearchResults	Grants permission to get information about search results	Read	mailmanager-archive*		
GetIngressPoint	Grants permission to get information about an ingress point	Read	mailmanager-ingress-point*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMemberOfAddressList	Grants permission to get information about a member in an address list	Read	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
GetRelay	Grants permission to get information about a SMTP relay	Read	mailmanager-smtp-relay*		
				aws:RequestTag/${TagKey}	
GetRuleSet	Grants permission to get information about a rule set	Read	mailmanager-rule-set*		
				aws:RequestTag/${TagKey}	
GetTrafficPolicy	Grants permission to get information about a traffic policy	Read	mailmanager-traffic-policy*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAddonInstances	Grants permission to list all of the addon instances associated with your account	List			
ListAddonSubscriptions	Grants permission to list all of the addon subscriptions associated with your account	List			
ListAddressListImportJobs	Grants permission to list all of the import jobs associated with an address list	List	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
ListAddressLists	Grants permission to list all of the address lists associated with your account	List			
ListArchiveExports	Grants permission to list all of the archive exports associated with your account	List			
ListArchiveSearches	Grants permission to list all of the archive searches associated with your account	List			
ListArchives	Grants permission to list all of the archives associated with your account	List			
ListIngressPoints	Grants permission to list all of the ingress points associated with your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMembersOfAddressList	Grants permission to list all of the members associated with an address list	List	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
ListRelays	Grants permission to list all of the SMTP relays associated with your account	List			
ListRuleSets	Grants permission to list all of the rule sets associated with your account	List			
ListTagsForResource	Grants permission to list all of the tags associated with the resource	Read	addon-instance		
			addon-subscription		
			mailmanager-archive		
			mailmanager-ingress-point		
			mailmanager-rule-set		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
ListTrafficPolicies	Grants permission to list all of the traffic policies associated with your account	List			
RegisterMemberToAddressList	Grants permission to add a member to an address list	Write	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StartAddressListImportJob	Grants permission to start an import job on an address list	Write	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StartArchiveExport	Grants permission to start an archive export	Write	mailmanager-archive*		
StartArchiveSearch	Grants permission to start an archive search	Write	mailmanager-archive*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopAddressListImportJob	Grants permission to stop an ongoing import job on an address list	Write	mailmanager-address-list*	aws:ResourceTag/${TagKey}	
StopArchiveExport	Grants permission to stop archive export	Write	mailmanager-archive*		
StopArchiveSearch	Grants permission to stop archive search	Write	mailmanager-archive*		
TagResource	Grants permission to add one or more tags (keys and values) to a specified resource	Tagging	addon-instance		
			addon-subscription		
			mailmanager-address-list		
			mailmanager-archive		
			mailmanager-ingress-point		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			mailmanager-rule-set		
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove one or more tags (keys and values) from a specified resource	Tagging	addon-instance		
			addon-subscription		
			mailmanager-address-list		
			mailmanager-archive		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			mailmanager-ingress-point		
			mailmanager-rule-set		
			mailmanager-smtp-relay		
			mailmanager-traffic-policy		
				aws:TagKeys	
UpdateArchive	Grants permission to update an archive	Write	mailmanager-archive*		
				aws:RequestTag/${TagKey}	
UpdateIngressPoint	Grants permission to update an ingress point	Write	mailmanager-ingress-point*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} ses:MailManagerTrafficPolicyArn ses:MailManagerRuleSetArn	
UpdateRelay	Grants permission to update a SMTP relay	Write	mailmanager-smtp-relay*		
				aws:RequestTag/${TagKey}	
UpdateRuleSet	Grants permission to update a rule set	Write	mailmanager-rule-set*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateTrafficPolicy	Grants permission to update a traffic policy	Write	mailmanager-traffic-policy*		
				aws:RequestTag/${TagKey}	

Resource types defined by Amazon Simple Email Service - Mail Manager

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
addon-instance	`arn:${Partition}:ses:${Region}:${Account}:addon-instance/${AddonInstanceId}`	aws:ResourceTag/${TagKey}
addon-subscription	`arn:${Partition}:ses:${Region}:${Account}:addon-subscription/${AddonSubscriptionId}`	aws:ResourceTag/${TagKey}
mailmanager-archive	`arn:${Partition}:ses:${Region}:${Account}:mailmanager-archive/${ArchiveId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
mailmanager-ingress-point	arn:${Partition}:ses:${Region}:${Account}:mailmanager-ingress-point/${IngressPointId}	aws:ResourceTag/${TagKey} ses:MailManagerIngressPointType
mailmanager-smtp-relay	arn:${Partition}:ses:${Region}:${Account}:mailmanager-smtp-relay/${RelayId}	aws:ResourceTag/${TagKey}
mailmanager-rule-set	arn:${Partition}:ses:${Region}:${Account}:mailmanager-rule-set/${RuleSetId}	aws:ResourceTag/${TagKey}
mailmanager-traffic-policy	arn:${Partition}:ses:${Region}:${Account}:mailmanager-traffic-policy/${TrafficPolicyId}	aws:ResourceTag/${TagKey}
mailmanager-address-list	arn:${Partition}:ses:${Region}:${Account}:mailmanager-address-list/${AddressListId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Simple Email Service - Mail Manager

Amazon Simple Email Service - Mail Manager defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
ses:AddonSubscriptionArn	Filters access by SES Addon Subscription ARN	ARN
ses:MailManagerIngressPointType	Filters access by SES Mail Manager ingress point type, for example OPEN or AUTH	String
ses:MailManagerRuleSetArn	Filters access by SES Mail Manager rule set ARN	ARN
ses:MailManagerTrafficPolicyArn	Filters access by SES Mail Manager traffic policy ARN	ARN

Actions, resources, and condition keys for Amazon Simple Email Service v2

Amazon Simple Email Service v2 (service prefix: `ses`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Simple Email Service v2
- Resource types defined by Amazon Simple Email Service v2
- Condition keys for Amazon Simple Email Service v2

Actions defined by Amazon Simple Email Service v2

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetMetricData	Grants permission to get metric data on your activity	Read	configuration-set		
			identity		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CancelExportJob	Grants permission to cancel an export job	Write	export-job*		
				ses:ApiVersion ses:ExportSourceType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConfigurationSet	Grants permission to create a new configuration set	Write	configuration-set*		
			dedicated-ip-pool		
			mailmanager-archive		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateConfigurationSetEventDestination	Grants permission to create a configuration set event destination	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateContact	Grants permission to create a contact	Write	contact-list*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
CreateContactList	Grants permission to create a contact list	Write	contact-list*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateCustomVerificationEmailTemplate	Grants permission to create a new custom verification email template	Write	custom-verification-email-template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateDedicatedIpPool	Grants permission to create a new pool of dedicated IP addresses	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateDeliverabilityTestReport	Grants permission to create a new predictive inbox placement test	Write	identity*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentity	Grants permission to start the process of verifying an email identity	Write	identity*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateEmailIdentityPolicy	Grants permission to create the specified sending authorization policy for the given identity	Permissions management	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEmailTemplate	Grants permission to create an email template	Write	template*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateExportJob	Grants permission to create an export job	Write		ses:ApiVersion ses:ExportSourceType	
CreateImportJob	Grants permission to creates an import job for a data destination	Write		ses:ApiVersion	
CreateMultiRegionEndpoint	Grants permission to create a new multi-region endpoint	Write		ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTenant	Grants permission to create a new tenant	Write	tenant*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
CreateTenantResourceAssociation	Grants permission to associate a SES resource to a tenant	Write	configuration-set*		
			identity*		
			template*		
			tenant*		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	
DeleteConfigurationSet	Grants permission to delete an existing configuration set	Write	configuration-set*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteConfigurationSetEventDestination	Grants permission to delete an event destination	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteContact	Grants permission to delete a contact from a contact list	Write	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteContactList	Grants permission to delete a contact list with all of its contacts	Write	contact-list*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteCustomVerificationEmailTemplate	Grants permission to delete an existing custom verification email template	Write	custom-verification-email-template*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteDedicatedIpPool	Grants permission to delete a dedicated IP pool	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEmailIdentity	Grants permission to delete an email identity	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailIdentityPolicy	Grants permission to delete the specified sending authorization policy for the given identity (an email address or a domain)	Permissions management	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteEmailTemplate	Grants permission to delete an email template	Write	template*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteMultiRegionEndpoint	Grants permission to delete a multi-region endpoint	Write	multi-region-endpoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteSuppressedDestination	Grants permission to remove an email address from the suppression list for your account	Write		ses:ApiVersion	
DeleteTenant	Grants permission to delete a tenant	Write	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
DeleteTenantResourceAssociation	Grants permission to remove an associated SES resource from a tenant	Write	configuration-set*		
			identity*		
			template*		
			tenant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetAccount	Grants permission to get information about the email-sending status and capabilities for your account	Read		ses:ApiVersion	
GetBlacklistReports	Grants permission to retrieve a list of the deny lists on which your dedicated IP addresses or tracked domains appear	Read		ses:ApiVersion	
GetConfigurationSet	Grants permission to get information about an existing configuration set	Read	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetConfigurationSetEventDestinations	Grants permission to retrieve a list of event destinations that are associated with a configuration set	Read	configuration-set*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetContact	Grants permission to return a contact from a contact list	Read	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetContactList	Grants permission to return contact list metadata	Read	contact-list*		
				ses:ApiVersion	
GetCustomVerificationEmailTemplate	Grants permission to return the custom email verification template for the template name you specify	Read	custom-verification-email-template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDedicatedIp	Grants permission to get information about a dedicated IP address	Read		ses:ApiVersion	
GetDedicatedIpPool	Grants permission to get information about a dedicated IP pool	Read	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDedicatedIps	Grants permission to list the dedicated IP addresses a dedicated IP pool	Read	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDeliverabilityDashboardOptions	Grants permission to get the status of the Deliverability dashboard	Read		ses:ApiVersion	
GetDeliverabilityTestReport	Grants permission to retrieve the results of a predictive inbox placement test	Read	deliverability-test-report*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetDomainDeliverabilityCampaign	Grants permission to retrieve all the deliverability data for a specific campaign	Read		ses:ApiVersion	
GetDomainStatisticsReport	Grants permission to retrieve inbox placement and engagement rates for the domains that you use to send email	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEmailAddressInsights	Grants permission to get insights about email address	Read		ses:ApiVersion	iam:CreateServiceLinkedRole
GetEmailIdentity	Grants permission to get information about a specific identity	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailIdentityPolicies	Grants permission to return the requested sending authorization policies for the given identity (an email address or a domain)	Read	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetEmailTemplate	Grants permission to return the template object, which includes the subject line, HTML part, and text part for the template you specify	Read	template*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetExportJob	Grants permission to get information about an export job	Read	export-job*		
				ses:ApiVersion ses:ExportSourceType	
GetImportJob	Grants permission to provide information about an import job	Read	import-job*		
				ses:ApiVersion	
GetMessageInsights	Grants permission to provide insights about a message	Read		ses:ApiVersion	
GetMultiRegionEndpoint	Grants permission to get information about a multi-region endpoint	Read	multi-region-endpoint*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
GetReputationEntity		Read	tenant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to retrieve information about a reputation entity's status			ses:ApiVersion aws:ResourceTag/${TagKey}	
GetSuppressedDestination	Grants permission to retrieve information about a specific email address that's on the suppression list for your account	Read		ses:ApiVersion	
GetTenant	Grants permission to get information about a tenant	Read	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListConfigurationSets	Grants permission to list all of the configuration sets for your account	List		ses:ApiVersion	
ListContactLists	Grants permission to list all of the contact lists available for your account	List		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListContacts	Grants permission to list the contacts present in a specific contact list	List	contact-list*		
				ses:ApiVersion	
ListCustomVerificationEmailTemplates	Grants permission to list all of the existing custom verification email templates for your account	List		ses:ApiVersion	
ListDedicatedIpPools	Grants permission to list all of the dedicated IP pools for your account	List		ses:ApiVersion	
ListDeliverabilityTestReports	Grants permission to retrieve the list of the predictive inbox placement tests that you've performed, regardless of their statuses, for your account	List		ses:ApiVersion	
ListDomainDeliverabilityCampaigns	Grants permission to list deliverability data for campaigns that used a specific domain to send email during a specified time range	Read		ses:ApiVersion	
ListEmailIdentities	Grants permission to list the email identities for your account	List		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEmailTemplates	Grants permission to list all of the email templates for your account	List		ses:ApiVersion	
ListExportJobs	Grants permission to list all the exports jobs for your account	List		ses:ApiVersion ses:ExportSourceType	
ListImportJobs	Grants permission to list all of the import jobs for your account	List		ses:ApiVersion	
ListMultiRegionEndpoints	Grants permission to list all of the multi-region endpoints for your account	List		ses:ApiVersion	
ListRecommendations	Grants permission to list recommendations for your account	Read	identity		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListReputationEntities	Grants permission to retrieve a list of reputation entities	List	tenant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListResourceTenants	Grants permission to list all the tenants associated to a SES resource	List	configuration-set*		
			identity*		
			template*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListSuppressedDestinations	Grants permission to list email addresses that are on the suppression list for your account	Read		ses:ApiVersion	
ListTagsForResource	Grants permission to retrieve a list of the tags (keys and values) that are associated with a specific resource for your account	Read	configuration-set		
			contact-list		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			custom-verification-email-template		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
			template		
			tenant		
				ses:ApiVersion	
ListTenantResources	Grants permission to list all the resources associated to a tenant	List	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
ListTenants	Grants permission to list all the tenants for your account	List		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAccountDedicatedIpWarmupAttributes	Grants permission to enable or disable the automatic warm-up feature for dedicated IP addresses	Write		ses:ApiVersion	
PutAccountDetails	Grants permission to update your account details	Write		ses:ApiVersion	
PutAccountSendingAttributes	Grants permission to enable or disable the ability to send email for your account	Write		ses:ApiVersion	
PutAccountSuppressionAttributes	Grants permission to change the settings for the account-level suppression list	Write		ses:ApiVersion	
PutAccountVdmAttributes	Grants permission to change the settings for VDM for your account	Write		ses:ApiVersion	
PutConfigurationSetArchivingOptions	Grants permission to associate a configuration set with a Mail Manager archive	Write	configuration-set*		
			mailmanager-archive		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutConfigurationSetDeliveryOptions	Grants permission to associate a configuration set with a dedicated IP pool	Write	configuration-set*		
			dedicated-ip-pool		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetReputationOptions	Grants permission to enable or disable collection of reputation metrics for emails that you send using a particular configuration set	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetSendingOptions	Grants permission to enable or disable email sending for messages that use a particular configuration set	Write	configuration-set*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetSuppressionOptions	Grants permission to specify the account suppression list preferences for a particular configuration set	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetTrackingOptions	Grants permission to specify a custom domain to use for open and click tracking elements in email that you send for a particular configuration set	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutConfigurationSetVdmOptions	Grants permission to override account-level VDM settings for a particular configuration set	Write	configuration-set*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpInPool	Grants permission to move a dedicated IP address to an existing dedicated IP pool	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpPoolScalingAttributes	Grants permission to transition a dedicated IP pool from Standard to Managed	Write	dedicated-ip-pool*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutDedicatedIpWarmupAttributes	Grants permission to put Dedicated IP warm up attributes	Write		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutDeliverabilityDashboardOption	Grants permission to enable or disable the Deliverability dashboard	Write		ses:ApiVersion	
PutEmailIdentityConfigurationSetAttributes	Grants permission to associate a configuration set with an email identity	Write	identity*		
			configuration-set		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityDkimAttributes	Grants permission to enable or disable DKIM authentication for an email identity	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutEmailIdentityDkimSigningAttributes	Grants permission to configure or change the DKIM authentication settings for an email domain identity	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityFeedbackAttributes	Grants permission to enable or disable feedback forwarding for an email identity	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutEmailIdentityMailFromAttributes	Grants permission to enable or disable the custom MAIL FROM domain configuration for an email identity	Write	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
PutSuppressedDestination	Grants permission to add an email address to the suppression list	Write		ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReplicateEmailIdentityDkimSigningKey [permission only]	Grants permission to replicate email identity DKIM signing key	Permissions management	identity*		
				ses:ReplicaRegion	
SendBulkEmail	Grants permission to compose an email message to multiple destinations	Write	identity*		
			template*		
			configuration-set		
				ses:ApiVersion ses:MultiRegionEndpointId ses:TenantName	
SendCustomVerificationEmail	Grants permission to add an email address to the list of identities and attempts to verify it	Write	custom-verification-email-template*		
				ses:ApiVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendEmail	Grants permission to send an email message	Write	identity*		
			configuration-set		
			template		
				ses:ApiVersion ses:FeedbackAddress ses:FromAddress ses:FromDisplayName ses:Recipients ses:MultiRegionEndpointId ses:TenantName	
TagResource	Grants permission to add one or more tags (keys and values) to a specified resource	Tagging	configuration-set		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			contact-list		
			custom-verification-email-template		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
			template		
			tenant		
				ses:ApiVersion aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TestRenderEmailTemplate	Grants permission to create a preview of the MIME content of an email when provided with a template and a set of replacement data	Write	template*		
				ses:ApiVersion	
UntagResource	Grants permission to remove one or more tags (keys and values) from a specified resource	Tagging	configuration-set		
			contact-list		
			custom-verification-email-template		
			dedicated-ip-pool		
			deliverability-test-report		
			identity		
			template		
			tenant		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:TagKeys	
UpdateConfigurationSetEventDestination	Grants permission to update the configuration of an event destination for a configuration set	Write	configuration-set*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateContact	Grants permission to update a contact's preferences for a list	Write	contact-list*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateContactList	Grants permission to update contact list metadata	Write	contact-list*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateCustomVerificationEmailTemplate	Grants permission to update an existing custom verification email template	Write	custom-verification-email-template*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateEmailIdentityPolicy	Grants permission to update the specified sending authorization policy for the given identity (an email address or a domain)	Permissions management	identity*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateEmailTemplate	Grants permission to update an email template	Write	template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateReputationEntityCustomerManagedStatus	Grants permission to update the customer-managed sending status	Write	tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	
UpdateReputationEntityPolicy	Grants permission to assign a reputation policy	Write	reputation-policy*		
			tenant*		
				ses:ApiVersion aws:ResourceTag/${TagKey}	

Resource types defined by Amazon Simple Email Service v2

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
reputation-policy	`arn:${Partition}:ses:${Region}:aws:reputation-policy/${ReputationPolicyName}`	
configuration-set	`arn:${Partition}:ses:${Region}:${Account}:configuration-set/${ConfigurationSetName}`	aws:ResourceTag/${TagKey}
contact-list	`arn:${Partition}:ses:${Region}:${Account}:contact-list/${ContactListName}`	aws:ResourceTag/${TagKey}
custom-verification-email-template	`arn:${Partition}:ses:${Region}:${Account}:custom-verification-email-template/${TemplateName}`	aws:ResourceTag/${TagKey}
dedicated-ip-pool	`arn:${Partition}:ses:${Region}:${Account}:dedicated-ip-pool/${DedicatedIPPool}`	aws:ResourceTag/${TagKey}
deliverability-test-report	`arn:${Partition}:ses:${Region}:${Account}:deliverability-test-report/${ReportId}`	aws:ResourceTag/${TagKey}
export-job	`arn:${Partition}:ses:${Region}:${Account}:export-job/${ExportJobId}`	

Resource types	ARN	Condition keys
identity	arn:${Partition}:ses:${Region}:${Account}:identity/${IdentityName}	aws:ResourceTag/${TagKey}
import-job	arn:${Partition}:ses:${Region}:${Account}:import-job/${ImportJobId}	
template	arn:${Partition}:ses:${Region}:${Account}:template/${TemplateName}	aws:ResourceTag/${TagKey}
multi-region-endpoint	arn:${Partition}:ses:${Region}:${Account}:multi-region-endpoint/${EndpointName}	
mailmanager-archive	arn:${Partition}:ses:${Region}:${Account}:mailmanager-archive/${ArchiveId}	aws:ResourceTag/${TagKey}
tenant	arn:${Partition}:ses:${Region}:${Account}:tenant/${TenantName}/${TenantId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Simple Email Service v2

Amazon Simple Email Service v2 defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
ses:ApiVersion	Filters access by the SES API version	String
ses:ExportSourceType	Filters access by the export source type	String
ses:FeedbackAddress	Filters access by the "Return-Path" address, which specifies where bounces and complaints are sent by email feedback forwarding	String
ses:FromAddress	Filters access by the "From" address of a message	String
ses:FromDisplayName	Filters access by the "From" address that is used as the display name of a message	String
ses:MultiRegionEndpointId	Filters access by the multi-region endpoint ID that is used to send email	String
ses:Recipients	Filters access by the recipient addresses of a message, which include the "To", "CC", and "BCC" addresses	ArrayOfString
ses:ReplicaRegion	Filters access by the replica regions for Replicating domain DKIM signing key	ArrayOfString
ses:TenantName	Filters access by the tenant name that is used to send email	String

Actions, resources, and condition keys for Amazon Simple Workflow Service

Amazon Simple Workflow Service (service prefix: `swf`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon Simple Workflow Service
- Resource types defined by Amazon Simple Workflow Service
- Condition keys for Amazon Simple Workflow Service

Actions defined by Amazon Simple Workflow Service

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelTimer [permission only]	Grants permission to cancel a previously started timer and record a TimerCanceled event in the history	Write	domain*		
CancelWorkflowExecution	Grants permission to close the workflow execution and record a WorkflowExecutionCanceled event in the history	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
CompleteWorkflowExecution [permission only]	Grants permission to close the workflow execution and record a WorkflowExecutionCompleted event in the history	Write	domain*		
ContinueAsNewWorkflowExecution [permission only]	Grants permission to close the workflow execution and start a new workflow execution of the same type using the same workflow ID and a unique run Id	Write	domain*		
CountClosedWorkflowExecutions	Grants permission to return the number of closed workflow executions within the given domain that meet the specified filtering criteria	Read	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CountOpenWorkflowExecutions	Grants permission to return the number of open workflow executions within the given domain that meet the specified filtering criteria	Read	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
CountPendingActivityTasks	Grants permission to return the estimated number of activity tasks in the specified task list	Read	domain*		
				swf:taskList.name	
CountPendingDecisionTasks	Grants permission to return the estimated number of decision tasks in the specified task list	Read	domain*		
				swf:taskList.name	
DeleteActivityType	Grants permission to delete the specified activity type	Write	domain*		
				swf:activityType.name swf:activityType.version	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteWorkflowType	Grants permission to delete the specified workflow type	Write	domain*		
				swf:workflowType.name swf:workflowType.version	
DeprecateActivityType	Grants permission to deprecate the specified activity type	Write	domain*		
				swf:activityType.name swf:activityType.version	
DeprecateDomain	Grants permission to deprecate the specified domain	Write	domain*		
DeprecateWorkflowType	Grants permission to deprecate the specified workflow type	Write	domain*		
				swf:workflowType.name swf:workflowType.version	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeActivityType	Grants permission to return information about the specified activity type	Read	domain*		
				swf:activityType.name swf:activityType.version	
DescribeDomain	Grants permission to return information about the specified domain, including its description and status	Read	domain*		
DescribeWorkflowExecution	Grants permission to return information about the specified workflow execution including its type and some statistics	Read	domain*		
DescribeWorkflowType	Grants permission to return information about the specified workflow type	Read	domain*		
				swf:workflowType.name swf:workflowType.version	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
FailWorkflowExecution [permission only]	Grants permission to close the workflow execution and record a WorkflowExecutionFailed event in the history	Write	domain*		
GetWorkflowExecutionHistory	Grants permission to return the history of the specified workflow execution	Read	domain*		
ListActivityTypes	Grants permission to return information about all activities registered in the specified domain that match the specified name and registration status	List	domain*		
ListClosedWorkflowExecutions	Grants permission to return a list of closed workflow executions in the specified domain that meet the filtering criteria	List	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
ListDomains	Grants permission to return the list of domains registered in the account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListOpenWorkflowExecutions	Grants permission to return a list of open workflow executions in the specified domain that meet the filtering criteria	List	domain*		
				swf:tagFilter.tag swf:typeFilter.name swf:typeFilter.version	
ListTagsForResource	Grants permission to list tags for an AWS SWF resource	List	domain		
ListWorkflowTypes	Grants permission to return information about workflow types in the specified domain	List	domain*		
PollForActivityTask	Grants permission to workers to get an ActivityTask from the specified activity taskList	Write	domain*		
				swf:taskList.name	
PollForDecisionTask	Grants permission to deciders to get a DecisionTask from the specified decision taskList	Write	domain*		
				swf:taskList.name	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RecordActivityTaskHeartbeat	Grants permission to workers to report to the service that the ActivityTask represented by the specified taskToken is still making progress	Write	domain*		
RecordMarker [permission only]	Grants permission to record a MarkerRecorded event in the history	Write	domain*		
RegisterActivityType	Grants permission to register a new activity type along with its configuration settings in the specified domain	Write	domain*	swf:defaultTaskList.name swf:name swf:version	
RegisterDomain	Grants permission to register a new domain	Write		aws:TagKeys aws:RequestTag/${TagKey}	
RegisterWorkflowType	Grants permission to register a new workflow type and its configuration settings in the specified domain	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				swf:defaultTaskList.name swf:name swf:version	
RequestCancelActivityTask [permission only]	Grants permission to attempt to cancel a previously scheduled activity task	Write	domain*		
RequestCancelExternalWorkflowExecution [permission only]	Grants permission to request that a request be made to cancel the specified external workflow execution	Write	domain*		
RequestCancelWorkflowExecution	Grants permission to record a WorkflowExecutionCancelRequested event in the currently running workflow execution identified by the given domain, workflowId, and runId	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RespondActivityTaskCanceled	Grants permission to workers to tell the service that the ActivityTask identified by the taskToken was successfully canceled	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RespondActivityTaskCompleted	Grants permission to workers to tell the service that the ActivityTask identified by the taskToken completed successfully with a result (if provided)	Write	domain*		
				swf:activityType.name swf:activityType.version swf:tagList.member.0 swf:tagList.member.1 swf:tagList.member.2 swf:tagList.member.3 swf:tagList.member.4 swf:taskList.name	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				swf:workflowType.name swf:workflowType.version	
RespondActivityTaskFailed	Grants permission to workers to tell the service that the ActivityTask identified by the taskToken has failed with reason (if specified)	Write	domain*		
RespondDecisionTaskCompleted	Grants permission to deciders to tell the service that the DecisionTask identified by the taskToken has successfully completed	Write	domain*		
ScheduleActivityTask [permission only]	Grants permission to schedule an activity task	Write	domain*		
SignalExternalWorkflowExecution [permission only]	Grants permission to request a signal to be delivered to the specified external workflow execution and records	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SignalWorkflowExecution	Grants permission to record a WorkflowExecutionSignaled event in the workflow execution history and create a decision task for the workflow execution identified by the given domain, workflowId and runId	Write	domain*		
StartChildWorkflowExecution [permission only]	Grants permission to request that a child workflow execution be started	Write	domain*		
StartTimer [permission only]	Grants permission to start a timer for a workflow execution	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartWorkflowExecution	Grants permission to start an execution of the workflow type in the specified domain using the provided workflowId and input data	Write	domain*	swf:tagList.member.0 swf:tagList.member.1 swf:tagList.member.2 swf:tagList.member.3 swf:tagList.member.4 swf:taskList.name swf:workflowType.name swf:workflowType.version	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag an AWS SWF resource	Tagging	domain		
				aws:TagKeys aws:RequestTag/${TagKey}	
TerminateWorkflowExecution	Grants permission to record a WorkflowExecutionTerminated event and force closure of the workflow execution identified by the given domain, runId, and workflowId	Write	domain*		
UndeprecateActivityType	Grants permission to undeprecate a previously deprecated activity type	Write	domain*		
				swf:activityType.name swf:activityType.version	
UndeprecateDomain	Grants permission to undeprecate a previously deprecated domain	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UndeprecateWorkflowType	Grants permission to undeprecate a previously deprecated workflow type	Write	domain*		
				swf:workflowType.name swf:workflowType.version	
UntagResource	Grants permission to remove a tag from an AWS SWF resource	Tagging	domain		
				aws:TagKeys	

Resource types defined by Amazon Simple Workflow Service

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
domain	`arn:${Partition}:swf::${Account}:/domain/${DomainName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Simple Workflow Service

Amazon Simple Workflow Service defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tag of the request	String
aws:ResourceTag/${TagKey}	Filters access by tag of the resource	String
aws:TagKeys	Filters access by tag of the key	ArrayOfString
swf:activityType.name	Filters access by the name of the activity type	String
swf:activityType.version	Filters access by the version of the activity type	String
swf:defaultTaskList.name	Filters access by the name of the default task list	String
swf:name	Filters access by the name of activities or workflows	String
swf:tagFilter.tag	Filters access by the value of tagFilter.tag	String
swf:tagList.member.0	Filters access by the specified tag	String
swf:tagList.member.1	Filters access by the specified tag	String

Condition keys	Description	Type
swf:tagList.member.2	Filters access by the specified tag	String
swf:tagList.member.3	Filters access by the specified tag	String
swf:tagList.member.4	Filters access by the specified tag	String
swf:taskList.name	Filters access by the name of the tasklist	String
swf:typeFilter.name	Filters access by the name of the type filter	String
swf:typeFilter.version	Filters access by the version of the type filter	String
swf:version	Filters access by the version of activities or workflows	String
swf:workflowType.name	Filters access by the name of the workflow type	String
swf:workflowType.version	Filters access by the version of the workflow type	String

Actions, resources, and condition keys for Amazon SQS

Amazon SQS (service prefix: sqs) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by Amazon SQS
- Resource types defined by Amazon SQS
- Condition keys for Amazon SQS

Actions defined by Amazon SQS

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddPermission	Grants permission to a queue for a specific principal	Permissions management	queue*		
CancelMessageMoveTask	Grants permission to cancel an in progress message move task	Write	queue*		
ChangeMessageVisibility	Grants permission to change the visibility timeout of a specified message in a queue to a new value	Write	queue*		
CreateQueue	Grants permission to create a new queue, or returns the URL of an existing one	Write	queue*	aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteMessage	Grants permission to delete the specified message from the specified queue	Write	queue*		
DeleteQueue	Grants permission to delete the queue specified by the queue URL, regardless of whether the queue is empty	Write	queue*		
GetQueueAttributes	Grants permission to get attributes for the specified queue	Read	queue*		
GetQueueUrl	Grants permission to return the URL of an existing queue	Read	queue*		
ListDeadLetterSourceQueues	Grants permission to return a list of your queues that have the RedrivePolicy queue attribute configured with a dead letter queue	Read	queue*		
ListMessageMoveTasks	Grants permission to list message move tasks	Read	queue*		
ListQueueTags	Grants permission to list tags added to an SQS queue	Read	queue*		
ListQueues	Grants permission to return a list of your queues	Read			
PurgeQueue	Grants permission to delete the messages in a queue specified by the queue URL	Write	queue*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReceiveMessage	Grants permission to retrieve one or more messages, with a maximum limit of 10 messages, from the specified queue	Read	queue*		
RemovePermission	Grants permission to revoke any permissions in the queue policy that matches the specified Label parameter	Permissions management	queue*		
SendMessage	Grants permission to deliver a message to the specified queue	Write	queue*		
SetQueueAttributes	Grants permission to set the value of one or more queue attributes	Write	queue*		
StartMessageMoveTask	Grants permission to start a message move task	Write	queue*		
TagQueue	Grants permission to add tags to the specified SQS queue	Tagging	queue*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagQueue	Grants permission to remove tags from the specified SQS queue	Tagging	queue*		
				aws:TagKeys	

Resource types defined by Amazon SQS

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

> **Note**
>
> The ARN of the queue is used only in IAM permission policies. In API and CLI calls, you use the queue's URL instead.

Resource types	ARN	Condition keys
queue	`arn:${Partition}:sqs:${Region}:${Account}:${QueueName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon SQS

Amazon SQS defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS Step Functions

AWS Step Functions (service prefix: `states`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Step Functions
- Resource types defined by AWS Step Functions
- Condition keys for AWS Step Functions

Actions defined by AWS Step Functions

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name.

However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateActivity	Grants permission to create an activity	Write	activity*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStateMachine	Grants permission to create a state machine	Write	statemachine*		iam:PassRole states:PublishStateMachineVersion
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStateMachineAlias	Grants permission to create a state machine alias	Write	statemachine*		
				states:StateMachineQualifier	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteActivity	Grants permission to delete an activity	Write	activity*		
DeleteStateMachine	Grants permission to delete a state machine	Write	statemachine*		
DeleteStateMachineAlias	Grants permission to delete a state machine alias	Write	statemachine*		
				states:StateMachineQualifier	
DeleteStateMachineVersion	Grants permission to delete a state machine version	Write	statemachine*		
				states:StateMachineQualifier	
DescribeActivity	Grants permission to describe an activity	Read	activity*		
DescribeExecution	Grants permission to describe an execution	Read	execution*		
			express*		
DescribeMapRun	Grants permission to describe a map run	Read	maprun*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStateMachine	Grants permission to describe a state machine	Read	statemachine*		
				states:StateMachineQualifier	
DescribeStateMachineAlias	Grants permission to describe a state machine alias	Read	statemachine*		
				states:StateMachineQualifier	
DescribeStateMachineForExecution	Grants permission to describe the state machine for an execution	Read	execution*		
GetActivityTask	Grants permission to be used by workers to retrieve a task (with the specified activity ARN) which has been scheduled for execution by a running state machine	Write	activity*		
GetExecutionHistory	Grants permission to return the history of the specified execution as a list of events	Read	execution*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
InvokeHTTPEndpoint [permission only]	Grants permission to invoke the HTTP Task state	Write			
ListActivities	Grants permission to list the existing activities	List			
ListExecutions	Grants permission to list the executions of a state machine	List	maprun*		
			statemachine*		
				states:StateMachineQualifier	
ListMapRuns	Grants permission to list the map runs of an execution	List	execution*		
ListStateMachineAliases	Grants permission to list the aliases of a state machine	List	statemachine*		
				states:StateMachineQualifier	
ListStateMachineVersions	Grants permission to list the versions of a state machine	List	statemachine*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListStateMachines	Grants permission to lists the existing state machines	List			
ListTagsForResource	Grants permission to list tags for an AWS Step Functions resource	List	activity statemachine		
PublishStateMachineVersion	Grants permission to publish a state machine version	Write	statemachine*		
RedriveExecution	Grants permission to redrive an execution	Write	execution*		
RevealSecrets [permission only]	Grants permission to reveal sensitive data from an execution	Read			
SendTaskFailure	Grants permission to report that the task identified by the taskToken failed	Write			
SendTaskHeartbeat	Grants permission to report to the service that the task represented by the specified taskToken is still making progress	Write			
SendTaskSuccess	Grants permission to report that the task identified by the taskToken completed successfully	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartExecution	Grants permission to start a state machine execution	Write	statemachine*		
				states:StateMachineQualifier	
StartSyncExecution	Grants permission to start a Synchronous Express state machine execution	Write	statemachine*		
				states:StateMachineQualifier	
StopExecution	Grants permission to stop an execution	Write	execution*		
TagResource	Grants permission to tag an AWS Step Functions resource	Tagging	activity		
			statemachine		
				aws:TagKeys	
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TestState	Grants permission to test a state machine definition	Write			states:RevealSecrets
UntagResource	Grants permission to remove a tag from an AWS Step Functions resource	Tagging	activity		
			statemachine		
				aws:TagKeys	
UpdateMapRun	Grants permission to update a map run	Write	maprun*		
UpdateStateMachine	Grants permission to update a state machine	Write	statemachine*		iam:PassRole states:PublishStateMachineVersion
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateStateMachineAlias	Grants permission to update a state machine alias	Write	statemachine*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				states:StateMachineQualifier	
ValidateStateMachineDefinition	Grants permission to validate a state machine definition	Read			

Resource types defined by AWS Step Functions

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
activity	`arn:${Partition}:states:${Region}:${Account}:activity:${ActivityName}`	aws:ResourceTag/${TagKey}
execution	`arn:${Partition}:states:${Region}:${Account}:execution:${StateMachineName}:${ExecutionId}`	aws:ResourceTag/${TagKey}
express	`arn:${Partition}:states:${Region}:${Account}:express:${StateMachineName}:${ExecutionId}:${ExpressId}`	

Resource types	ARN	Condition keys
statemachine	arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}	aws:ResourceTag/${TagKey}
statemachineversion	arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}:${StateMachineVersionId}	aws:ResourceTag/${TagKey}
statemachinealias	arn:${Partition}:states:${Region}:${Account}:stateMachine:${StateMachineName}:${StateMachineAliasName}	aws:ResourceTag/${TagKey}
maprun	arn:${Partition}:states:${Region}:${Account}:mapRun:${StateMachineName}/${MapRunLabel}:${MapRunId}	
labelledexecution	arn:${Partition}:states:${Region}:${Account}:execution:${StateMachineName}/${MapRunLabel}:${ExecutionId}	
labelledexpress	arn:${Partition}:states:${Region}:${Account}:express:${StateMachineName}/${MapRunLabel}:${ExecutionId}:${ExpressId}	

Condition keys for AWS Step Functions

AWS Step Functions defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key and value pair that is allowed in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair of a resource	String
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString
states:HTTPEndpoint	Filters access by the endpoint that the HTTP Task state allows in the request	String
states:HTTPMethod	Filters access by the method that the HTTP Task state allows in the request	String
states:StateMachineQualifier	Filters access by the qualifier of a state machine ARN	ArrayOfString

Actions, resources, and condition keys for AWS Storage Gateway

AWS Storage Gateway (service prefix: `storagegateway`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Storage Gateway
- Resource types defined by AWS Storage Gateway
- Condition keys for AWS Storage Gateway

Actions defined by AWS Storage Gateway

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the

Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ActivateGateway	Grants permission to activate the gateway you previously deployed on your host	Write		aws:RequestTag/${TagKey} aws:TagKeys	
AddCache	Grants permission to configure one or more gateway local disks as cache for a cached-volume gateway	Write	gateway*		
AddTagsToResource	Grants permission to add one or more tags to the specified resource	Tagging	cache-report		
			fs-association		
			gateway		
			share		
			tape		
			tapepool		
			volume		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
AddUploadBuffer	Grants permission to configure one or more gateway local disks as upload buffer for a specified gateway	Write	gateway*		
AddWorkingStorage	Grants permission to configure one or more gateway local disks as working storage for a gateway	Write	gateway*		
AssignTapePool	Grants permission to move a tape to the target pool specified	Write	tape* tapepool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate FileSystem	Grants permission to associate an Amazon FSx file system with the Amazon FSx file gateway	Write	gateway*		ds:DescribeDirectories ec2:DescribeNetworkInterfaces fsx:DescribeFileSystems iam:CreateServiceLinkedRole logs:CreateLogDelivery logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
AttachVolume	Grants permission to connect a volume to an iSCSI connection and then attaches the volume to the specified gateway	Write	gateway* volume*		
BypassGovernanceRetention	Grants permission to allow the governance retention lock on a pool to be bypassed	Write	tapepool*		
CancelArchival	Grants permission to cancel archiving of a virtual tape to the virtual tape shelf (VTS) after the archiving process is initiated	Write	gateway* tape*		
CancelCacheReport	Grants permission to cancel a cache report	Write	cache-report*		
CancelRetrieval	Grants permission to cancel retrieval of a virtual tape from the virtual tape shelf (VTS) to a gateway after the retrieval process is initiated	Write	gateway* tape*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCachediSCSIVolume	Grants permission to create a cached volume on a specified cached gateway. This operation is supported only for the gateway-cached volume architecture	Write	gateway*		
			volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNFSFileShare	Grants permission to create a NFS file share on an existing file gateway	Write	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSMBFileShare	Grants permission to create a SMB file share on an existing file gateway	Write	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshot	Grants permission to initiate a snapshot of a volume	Write	volume*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotFromVolumeRecoveryPoint	Grants permission to initiate a snapshot of a gateway from a volume recovery point	Write	volume*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorediSCSIVolume	Grants permission to create a volume on a specified gateway	Write	gateway*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTapePool	Grants permission to create a tape pool	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapeWithBarcode	Grants permission to create a virtual tape by using your own barcode	Write	gateway* tapepool*	 aws:RequestTag/${TagKey} aws:TagKeys	
CreateTapes	Grants permission to create one or more virtual tapes. You write data to the virtual tapes and then archive the tapes	Write	gateway* tapepool*	 aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAutomaticTapeCreationPolicy	Grants permission to delete the automatic tape creation policy configured on a gateway-VTL	Write	gateway*		
DeleteBandwidthRateLimit	Grants permission to delete the bandwidth rate limits of a gateway	Write	gateway*		
DeleteCacheReport	Grants permission to delete the metadata associated with a cache report	Write	cache-report*		
DeleteChapCredentials	Grants permission to delete Challenge-Handshake Authentication Protocol (CHAP) credentials for a specified iSCSI target and initiator pair	Write	target*		
DeleteFileShare	Grants permission to delete a file share from a file gateway	Write	share*		
DeleteGateway	Grants permission to delete a gateway	Write	gateway*		
DeleteSnapshotSchedule	Grants permission to delete a snapshot of a volume	Write	volume*		
DeleteTape	Grants permission to delete the specified virtual tape	Write	gateway* tape*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTapeArchive	Grants permission to delete the specified virtual tape from the virtual tape shelf (VTS)	Write			
DeleteTapePool	Grants permission to delete the specified tape pool	Write	tapepool*		
DeleteVolume	Grants permission to delete the specified gateway volume that you previously created using the CreateCachediSCSIVolume or CreateStorediSCSIVolume API	Write	volume*		
DescribeAvailabilityMonitorTest	Grants permission to get the information about the most recent high availability monitoring test that was performed on the gateway	Read	gateway*		
DescribeBandwidthRateLimit	Grants permission to get the bandwidth rate limits of a gateway	Read	gateway*		
DescribeBandwidthRateLimitSchedule	Grants permission to get the bandwidth rate limit schedule of a gateway	Read	gateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCache	Grants permission to get information about the cache of a gateway. This operation is supported only for the gateway-cached volume architecture	Read	gateway*		
DescribeCacheReport	Grants permission to get a description of a cache report	Read	cache-report*		
DescribeCachediSCSIVolumes	Grants permission to get a description of the gateway volumes specified in the request. This operation is supported only for the gateway-cached volume architecture	Read	volume*		
DescribeChapCredentials	Grants permission to get an array of Challenge-Handshake Authentication Protocol (CHAP) credentials information for a specified iSCSI target, one for each target-initiator pair	Read	target*		
DescribeFileSystemAssociations	Grants permission to get a description for one or more file system associations	Read	fs-association*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeGatewayInformation	Grants permission to get metadata about a gateway such as its name, network interfaces, configured time zone, and the state (whether the gateway is running or not)	Read	gateway*		
DescribeMaintenanceStartTime	Grants permission to get your gateway's weekly maintenance start time including the day and time of the week	Read	gateway*		
DescribeNFSFileShares	Grants permission to get a description for one or more file shares from a file gateway	Read	share*		
DescribeSMBFileShares	Grants permission to get a description for one or more file shares from a file gateway	Read	share*		
DescribeSMBSettings	Grants permission to get a description of a Server Message Block (SMB) file share settings from a file gateway	Read	gateway*		
DescribeSnapshotSchedule	Grants permission to describe the snapshot schedule for the specified gateway volume	Read	volume*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStorediSCSIVolumes	Grants permission to get the description of the gateway volumes specified in the request	Read	volume*		
DescribeTapeArchives	Grants permission to get a description of specified virtual tapes in the virtual tape shelf (VTS)	Read			
DescribeTapeRecoveryPoints	Grants permission to get a list of virtual tape recovery points that are available for the specified gateway-VTL	Read	gateway*		
DescribeTapes	Grants permission to get a description of the specified Amazon Resource Name (ARN) of virtual tapes	Read	gateway*		
DescribeUploadBuffer	Grants permission to get information about the upload buffer of a gateway	Read	gateway*		
DescribeVTLDevices	Grants permission to get a description of virtual tape library (VTL) devices for the specified gateway	Read	gateway*		
DescribeWorkingStorage	Grants permission to get information about the working storage of a gateway	Read	gateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetachVolume	Grants permission to disconnect a volume from an iSCSI connection and then detaches the volume from the specified gateway	Write	volume*		
DisableGateway	Grants permission to disable a gateway when the gateway is no longer functioning	Write	gateway*		
DisassociateFileSystem	Grants permission to disassociate an Amazon FSx file system from an Amazon FSx file gateway	Write	fs-association*		
EvictFilesFailingUpload	Grants permission to clean a share's cache of file entries that are failing upload to Amazon S3	Write	share*		
JoinDomain	Grants permission to enable you to join an Active Directory Domain	Write	gateway*		
ListAutomaticTapeCreationPolicies	Grants permission to list the automatic tape creation policies configured on the specified gateway-VTL or all gateway-VTLs owned by your AWS account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCacheReports	Grants permission to get a list of the cache reports owned by your AWS account	List			
ListFileShares	Grants permission to get a list of the file shares for a specific file gateway, or the list of file shares owned by your AWS account	List			
ListFileSystemAssociations	Grants permission to get a list of the file system associations for the specified gateway	List			
ListGateways	Grants permission to list gateways owned by an AWS account in a region specified in the request. The returned list is ordered by gateway Amazon Resource Name (ARN)	List			
ListLocalDisks	Grants permission to get a list of the gateway's local disks	List	gateway*		
ListTagsForResource	Grants permission to get the tags that have been added to the specified resource	List	gateway		
			share		
			tape		
			volume		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTapePools	Grants permission to list tape pools owned by your AWS account	List			
ListTapes	Grants permission to list virtual tapes in your virtual tape library (VTL) and your virtual tape shelf (VTS)	List			
ListVolumeInitiators	Grants permission to list iSCSI initiators that are connected to a volume	List	volume*		
ListVolumeRecoveryPoints	Grants permission to list the recovery points for a specified gateway	List	gateway*		
ListVolumes	Grants permission to list the iSCSI stored volumes of a gateway	List			
NotifyWhenUploaded	Grants permission to send you a notification through CloudWatch Events when all files written to your NFS file share have been uploaded to Amazon S3	Write	share*		
RefreshCache	Grants permission to refresh the cache for the specified file share	Write	share*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveTagsFromResource	Grants permission to remove one or more tags from the specified resource	Tagging	cache-report		
			fs-association		
			gateway		
			share		
			tape		
			tapepool		
			volume		
				aws:TagKeys	
ResetCache	Grants permission to reset all cache disks that have encountered a error and makes the disks available for reconfiguration as cache storage	Write	gateway*		
RetrieveTapeArchive	Grants permission to retrieve an archived virtual tape from the virtual tape shelf (VTS) to a gateway-VTL	Write	gateway*		
			tape*		
RetrieveTapeRecoveryPoint	Grants permission to retrieve the recovery point for the specified virtual tape	Write	gateway*		
			tape*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetLocalConsolePassword	Grants permission to set the password for your VM local console	Write	gateway*		
SetSMBGuestPassword	Grants permission to set the password for SMB Guest user	Write	gateway*		
ShutdownGateway	Grants permission to shut down a gateway	Write	gateway*		
StartAvailabilityMonitorTest	Grants permission to start a test that verifies that the specified gateway is configured for High Availability monitoring in your host environment	Write	gateway*		
StartCacheReport	Grants permission to start a cache report for an existing file share	Write	share*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartGateway	Grants permission to start a gateway that you previously shut down	Write	gateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAutomaticTapeCreationPolicy	Grants permission to update the automatic tape creation policy configured on a gateway-VTL	Write	gateway* tapepool*		
UpdateBandwidthRateLimit	Grants permission to update the bandwidth rate limits of a gateway	Write	gateway*		
UpdateBandwidthRateLimitSchedule	Grants permission to update the bandwidth rate limit schedule of a gateway	Write	gateway*		
UpdateChapCredentials	Grants permission to update the Challenge-Handshake Authentication Protocol (CHAP) credentials for a specified iSCSI target	Write	target*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFileSystemAssociation	Grants permission to update a file system association	Write	fs-association*		logs:CreateLogDelivery logs:DeleteLogDelivery logs:GetLogDelivery logs:ListLogDeliveries logs:UpdateLogDelivery
UpdateGatewayInformation	Grants permission to update a gateway's metadata, which includes the gateway's name and time zone	Write	gateway*		
UpdateGatewaySoftwareNow	Grants permission to update the gateway virtual machine (VM) software	Write	gateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateMaintenanceStartTime	Grants permission to update a gateway's weekly maintenance start time information, including day and time of the week. The maintenance time is the time in your gateway's time zone	Write	gateway*		
UpdateNFSFileShare	Grants permission to update a NFS file share	Write	share*		
UpdateSMBFileShare	Grants permission to update a SMB file share	Write	share*		
UpdateSMBFileShareVisibility	Grants permission to update whether the shares on a gateway are visible in a net view or browse list	Write	gateway*		
UpdateSMBLocalGroups	Grants permission to update the list of Active Directory users and groups that have special permissions for SMB file shares on the gateway	Write	gateway*		
UpdateSMBSecurityStrategy	Grants permission to update the SMB security strategy on a file gateway	Write	gateway*		
UpdateSnapshotSchedule	Grants permission to update a snapshot schedule configured for a gateway volume	Write	volume*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateVTLDeviceType	Grants permission to update the type of medium changer in a gateway-VTL	Write	device*		

Resource types defined by AWS Storage Gateway

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
cache-report	`arn:${Partition}:storagegateway:${Region}:${Account}:share/${ShareId}/cache-report/${CacheReportId}`	aws:ResourceTag/${TagKey}
device	`arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/device/${Vtldevice}`	

Resource types	ARN	Condition keys
fs-association	arn:${Partition}:storagegateway:${Region}:${Account}:fs-association/${FsaId}	aws:ResourceTag/${TagKey}
gateway	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}	aws:ResourceTag/${TagKey}
share	arn:${Partition}:storagegateway:${Region}:${Account}:share/${ShareId}	aws:ResourceTag/${TagKey}
tape	arn:${Partition}:storagegateway:${Region}:${Account}:tape/${TapeBarcode}	aws:ResourceTag/${TagKey}
tapepool	arn:${Partition}:storagegateway:${Region}:${Account}:tapepool/${PoolId}	aws:ResourceTag/${TagKey}
target	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/target/${IscsiTarget}	
volume	arn:${Partition}:storagegateway:${Region}:${Account}:gateway/${GatewayId}/volume/${VolumeId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Storage Gateway

AWS Storage Gateway defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tags in the request	ArrayOfString

Actions, resources, and condition keys for AWS Support

AWS Support (service prefix: `support`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Support
- Resource types defined by AWS Support
- Condition keys for AWS Support

Actions defined by AWS Support

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Note

Support provides the ability to access, modify and resolve cases, as well as use Trusted Advisor actions. When you use the Support API to call Trusted Advisor-related actions, none of the "trustedadvisor:*" actions restrict your access. The "trustedadvisor:*" actions apply only to Trusted Advisor in the AWS Management Console.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddAttachmentsToSet	Grants permission to add one or more attachments to an AWS Support case	Write			
AddCommunicationToCase	Grants permission to add a customer communication to an AWS Support case	Write			
CreateCase	Grants permission to creates a new AWS Support case	Write			
DescribeAttachment	Grants permission to describe attachment detail	Read			
DescribeCaseAttributes	Grants permission to allow secondary services to read AWS Support case attributes.This is an internally managed function	Read			
DescribeCaseOptions	Grants permission to describe the available options for a single AWS Support case.	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	This is an internally managed function				
DescribeCases	Grants permission to list AWS Support cases that matches the given inputs	Read			
DescribeCommunication	Grants permission to get a single communication and attachments for a single AWS Support case	Read			
DescribeCommunications	Grants permission to list the communications and attachments for one or more AWS Support cases	Read			
DescribeCreateCaseOptions	Grants permission to describes the available options for creating a support case	Read			
DescribeIssueTypes	Grants permission to return issue types for AWS Support cases	Read			
DescribeServices	Grants permission to list AWS services and categories that applies to each service	Read			
DescribeSeverityLevels	Grants permission to list severity levels that can be assigned to an AWS Support case	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSupportLevel	Grants permission to return the support level for an AWS Account identifier	Read			
DescribeSupportedLanguages	Grants permission to describes the available support languages for a given category code, service code and issue type	Read			
DescribeTrustedAdvisorCheckRefreshStatuses	Grants permission to get the status of a Trusted Advisor refresh check based on a list of check identifiers	Read			
DescribeTrustedAdvisorCheckResult	Grants permission to get the results of the Trusted Advisor check that has the specified check identifier	Read			
DescribeTrustedAdvisorCheckSummaries	Grants permission to get the summaries of the results of the Trusted Advisor checks that have the specified check identifiers	Read			
DescribeTrustedAdvisorChecks	Grants permission to get a list of all available Trusted Advisor checks, including name, identifier, category and description	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInteraction	Grants permission to retrieve personalized troubleshooting assistance for account and technical issues for a specific interaction	Read			
InitiateCallForCase	Grants permission to initiate a call on AWS Support Center. This is an internally managed function	Write			
InitiateChatForCase	Grants permission to initiate a chat on AWS Support Center.This is an internally managed function	Write			
InitiateLiveContactForCase	Grants permission to initiate a live contact on AWS Support Center. This is an internally managed function	Write			
ListInteractionEntries	Grants permission to retrieve a list of entries within a specific interaction, including messages, status updates, or other relevant data points	Read			
ListInteractions	Grants permission to retrieve a list of interactions, potentially with filters or pagination	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutCaseAttributes	Grants permission to allow secondary services to attach attributes to AWS Support cases. This is an internally managed function	Write			
RateCaseCommunication	Grants permission to rate an AWS Support case communication	Write			
RefreshTrustedAdvisorCheck	Grants permission to requests a refresh of the Trusted Advisor check that has the specified check identifier	Write			
ResolveCase	Grants permission to resolve an AWS Support case	Write			
ResolveInteraction	Grants permission to mark a specific interaction as resolved by its unique identifier, indicating that the issue has been addressed and no further action is needed	Write			
SearchForCases	Grants permission to return a list of AWS Support cases that matches the given inputs	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartInteraction	Grants permission to start a specific interaction to receive personalized troubleshooting assistance for account and technical issues	Write			support:DescribeSupportLevel
UpdateCaseSeverity	Grants permission to update the severity for a single AWS Support case. This is an internally managed function	Write			
UpdateInteraction	Grants permission to update a specific interaction to receive personalized troubleshooting assistance for account and technical issues	Write			

Resource types defined by AWS Support

AWS Support does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Support, specify `"Resource": "*"` in your policy.

Condition keys for AWS Support

Support has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Support Console

AWS Support Console (service prefix: `support-console`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Support Console
- Resource types defined by AWS Support Console
- Condition keys for AWS Support Console

Actions defined by AWS Support Console

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CheckSubscription [permission only]	Grants permission to check whether the account has access to given product	Read			
CreateCaseDraft [permission only]	Grants permission to create or update case draft for the given case type	Write			
CreateContact [permission only]	Grants permission to create an authenticated contact for the given contact type	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCaseDraft [permission only]	Grants permission to delete a case draft for the given case type	Write			
DescribeDynamicHelp [permission only]	Grants permission to get dynamic help resources for given service and category	Read			
GetAccountGovCloudEnabled [permission only]	Grants permission to determines whether the calling account is GovCloud enabled	Read			
GetAccountState [permission only]	Grants permission to get the state of the calling account	Read			
GetBanner [permission only]	Grants permission to get the support banner information	Read			
GetCaseDraft [permission only]	Grants permission to get a case draft for given case type	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIssueClassificationPredictions [permission only]	Grants permission to get classification predictions of an issue	Read			
GetIssueTextSummary [permission only]	Grants permission to get a generated text summary of an issue	Read			
GetQuestionnaire [permission only]	Grants permission to get a feedback questionnaire	Read			
SaveFeedback [permission only]	Grants permission to save questionnaire feedback	Write			

Resource types defined by AWS Support Console

AWS Support Console does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to AWS Support Console, specify `"Resource": "*"` in your policy.

Condition keys for AWS Support Console

Support Console has no service-specific context keys that can be used in the `Condition` element of policy statements. For the list of the global context keys that are available to all services, see AWS global condition context keys.

Actions, resources, and condition keys for AWS Transfer Family

AWS Transfer Family (service prefix: `transfer`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS Transfer Family
- Resource types defined by AWS Transfer Family
- Condition keys for AWS Transfer Family

Actions defined by AWS Transfer Family

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern

for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAccess	Grants permission to add an access associated with a server	Write	server*		iam:PassRole
CreateAgreement	Grants permission to add an agreement associated with a server	Write	server*		iam:PassRole
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateConnector	Grants permission to create a connector	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} transfer:RequestConnectorProtocol	iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateProfile	Grants permission to create a profile	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateServer	Grants permission to create a server	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} transfer:RequestServerEndpointType transfer:RequestServerDomain transfer:RequestServerProtocols	iam:PassRole
CreateUser	Grants permission to add a user associated with a server	Write	server*		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
CreateWebApp	Grants permission to create a webapp	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateWorkflow	Grants permission to create a workflow	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteAccess	Grants permission to delete access	Write	server*		
DeleteAgreement	Grants permission to delete agreement	Write	agreement*		
DeleteCertificate	Grants permission to delete certificate	Write	certificate*		
DeleteConnector	Grants permission to delete connector	Write	connector*		
DeleteHostKey	Grants permission to delete a host key associated with a server	Write	host-key*		
DeleteProfile	Grants permission to delete profile	Write	profile*		
DeleteServer	Grants permission to delete a server	Write	server*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSshPublicKey	Grants permission to delete an SSH public key from a user	Write	user*		
DeleteUser	Grants permission to delete a user associated with a server	Write	user*		
DeleteWebApp	Grants permission to delete webapp	Write	webapp*		
DeleteWebAppCustomization	Grants permission to delete webapp customization	Write	webapp*		
DeleteWorkflow	Grants permission to delete a workflow	Write	workflow*		
DescribeAccess	Grants permission to describe an access assigned to a server	Read	server*		
DescribeAgreement	Grants permission to describe an agreement assigned to a server	Read	agreement*		
DescribeCertificate	Grants permission to describe a certificate	Read	certificate*		
DescribeConnector	Grants permission to describe a connector	Read	connector*		
DescribeExecution	Grants permission to describe an execution associated with a workflow	Read	workflow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeHostKey	Grants permission to describe a host key associated with a server	Read	host-key*		
DescribeProfile	Grants permission to describe a profile	Read	profile*		
DescribeSecurityPolicy	Grants permission to describe a security policy	Read			
DescribeServer	Grants permission to describe a server	Read	server*		
DescribeUser	Grants permission to describe a user associated with a server	Read	user*		
DescribeWebApp	Grants permission to describe a webapp	Read	webapp*		
DescribeWebAppCustomization	Grants permission to describe a webapp customization	Read	webapp*		
DescribeWorkflow	Grants permission to describe a workflow	Read	workflow*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportCertificate	Grants permission to add a certificate	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
ImportHostKey	Grants permission to add a host key to a server	Write	server*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
ImportSshPublicKey	Grants permission to add an SSH public key to a user	Write	user*		
ListAccesses	Grants permission to list accesses	Read	server*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAgreements	Grants permission to list agreements	Read	server*		
ListCertificates	Grants permission to list certificates	Read			
ListConnectors	Grants permission to list connectors	Read			
ListExecutions	Grants permission to list executions associated with a workflow	Read	workflow*		
ListFileTransferResults	Grants permission to list file transfer statuses for connectors	Read	connector*		
ListHostKeys	Grants permission to list host keys associated with a server	Read	server*		
ListProfiles	Grants permission to list profiles	Read			
ListSecurityPolicies	Grants permission to list security policies	List			
ListServers	Grants permission to list servers	List			
ListTagsForResource	Grants permission to list tags for an AWS Transfer Family resource	Read	agreement		
			certificate		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			connector		
			host-key		
			profile		
			server		
			user		
			workflow		
ListUsers	Grants permission to list users associated with a server	List	server*		
ListWebApps	Grants permission to list webapps	List			
ListWorkflows	Grants permission to list workflows	List			
SendWorkflowStepState	Grants permission to send a callback for asynchronous custom steps	Write	workflow*		
StartDirectoryListing	Grants permission to initiate a list operation on a remote server using a connector	Write	connector*		
StartFileTransfer	Grants permission to initiate a connector file transfer	Write	connector*		
StartRemoteDelete	Grants permission to initiate a connector delete operation on remote server	Write	connector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartRemoteMove	Grants permission to initiate a connector move operation on remote server	Write	connector*		
StartServer	Grants permission to start a server	Write	server*		
StopServer	Grants permission to stop a server	Write	server*		
TagResource	Grants permission to tag an AWS Transfer Family resource	Tagging	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			webapp		
			workflow		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
TestConnection	Grants permission to test a connector's connection to remote server	Write	connector*		
TestIdentityProvider	Grants permission to test a server's custom identity provider	Read	user*		
UntagResource	Grants permission to untag an AWS Transfer Family resource	Tagging	agreement		
			certificate		
			connector		
			host-key		
			profile		
			server		
			user		
			webapp		
			workflow		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateAccess	Grants permission to update access	Write			iam:PassRole
UpdateAgreement	Grants permission to update an agreement	Write	agreement*		iam:PassRole
UpdateCertificate	Grants permission to update a certificate	Write	certificate*		
UpdateConnector	Grants permission to update a connector	Write	connector*		iam:PassRole
UpdateHostKey	Grants permission to update a host key	Write	host-key*		
UpdateProfile	Grants permission to update a profile	Write	profile*		
UpdateServer	Grants permission to update the configuration of a server	Write	server*		iam:PassRole
				transfer:RequestServerEndpointType transfer:RequestServerProtocols	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateUser	Grants permission to update the configuration of a user	Write	user*		iam:PassRole
UpdateWebApp	Grants permission to update the configuration of a webapp	Write	webapp*		iam:PassRole
UpdateWebAppCustomization	Grants permission to update the configuration of a webapp cutomization	Write	webapp*		iam:PassRole

Resource types defined by AWS Transfer Family

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
user	`arn:${Partition}:transfer:${Region}:${Account}:user/${ServerId}/${UserName}`	aws:ResourceTag/${TagKey}
server	`arn:${Partition}:transfer:${Region}:${Account}:server/${ServerId}`	aws:ResourceTag/${TagKey}
workflow	`arn:${Partition}:transfer:${Region}:${Account}:workflow/${WorkflowId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
certificate	arn:${Partition}:transfer:${Region}:${Account}:certificate/${CertificateId}	aws:ResourceTag/${TagKey}
connector	arn:${Partition}:transfer:${Region}:${Account}:connector/${ConnectorId}	aws:ResourceTag/${TagKey}
profile	arn:${Partition}:transfer:${Region}:${Account}:profile/${ProfileId}	aws:ResourceTag/${TagKey}
agreement	arn:${Partition}:transfer:${Region}:${Account}:agreement/${ServerId}/${AgreementId}	aws:ResourceTag/${TagKey}
host-key	arn:${Partition}:transfer:${Region}:${Account}:host-key/${ServerId}/${HostKeyId}	aws:ResourceTag/${TagKey}
webapp	arn:${Partition}:transfer:${Region}:${Account}:webapp/${WebAppId}	aws:ResourceTag/${TagKey}

Condition keys for AWS Transfer Family

AWS Transfer Family defines the following condition keys that can be used in the Condition element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
transfer:RequestConnectorProtocol	Filters access by the connector protocol that is passed in the request	String
transfer:RequestServerDomain	Filters access by the storage domain that is passed in the request	String
transfer:RequestServerEndpointType	Filters access by the endpoint type that is passed in the request	String
transfer:RequestServerProtocols	Filters access by the server protocols that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS User Notifications

AWS User Notifications (service prefix: `notifications`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS User Notifications
- Resource types defined by AWS User Notifications
- Condition keys for AWS User Notifications

Actions defined by AWS User Notifications

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateChannel	Grants permission to associate a new Channel with a particular NotificationConfiguration	Write	NotificationConfiguration*		
AssociateManagedNotificationAccountContact	Grants permission to associate an Account contact to a particular Managed Notification Configuration	Write	ManagedNotificationConfiguration*		
AssociateManagedNotificationAdditionalChannel	Grants permission to associate a Channel to a particular Managed Notification Configuration	Write	ManagedNotificationConfiguration*		
AssociateOrganizationalUnit	Grants permission to associate an Organizational Unit to a particular Notification Configuration	Write	NotificationConfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEventRule	Grants permission to create a new EventRule, associating it with a NotificationConfiguration	Write			
CreateNotificationConfiguration	Grants permission to create a NotificationConfiguration	Write		aws:TagKeys aws:RequestTag/${TagKey}	
DeleteEventRule	Grants permission to delete an EventRule	Write	EventRule*		
DeleteNotificationConfiguration	Grants permission to delete a NotificationConfiguration	Write	NotificationConfiguration*		
DeregisterNotificationHub	Grants permission to deregister a NotificationHub	Write			
DisableNotificationsAccessForOrganization	Grants permission to disable Service Trust for AWS User Notifications	Permissions management			organizations:DisableAWSServiceAccess

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateChannel	Grants permission to remove a Channel from a NotificationConfiguration	Write	NotificationConfiguration*		
DisassociateManagedNotificationAccountContact	Grants permission to remove an Account contact from a Managed Notification Configuration	Write	ManagedNotificationConfiguration*		
DisassociateManagedNotificationAdditionalChannel	Grants permission to remove a Channel from a Managed Notification Configuration	Write	ManagedNotificationConfiguration*		
DisassociateOrganizationalUnit	Grants permission to disassociate an Organizational Unit to a particular Notification Configuration	Write	NotificationConfiguration*		
EnableNotificationsAccessForOrganization	Grants permission to enable Service Trust for AWS User Notifications	Permissions management			iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess
GetEventRule	Grants permission to get an EventRule	Read	EventRule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFeatureOptInStatus [permission only]	Grants permission to read the opt-in status of an AWS User Notification Service feature	Read			
GetManagedNotificationChildEvent	Grants permission to get a Managed Notification Child Event	Read	ManagedNotificationChildEvent*		
GetManagedNotificationConfiguration	Grants permission to get a Managed Notification Configuration	Read	ManagedNotificationConfiguration*		
GetManagedNotificationEvent	Grants permission to get a Managed NotificationEvent	Read	ManagedNotificationEvent*		
GetNotificationConfiguration	Grants permission to get a NotificationConfiguration	Read	NotificationConfiguration*		
GetNotificationEvent	Grants permission to get a NotificationEvent	Read	NotificationEvent*		
GetNotificationsAccessForOrganization	Grants permission to read Service Trust for AWS User Notifications	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListChannels	Grants permission to list Channels by NotificationConfiguration	List	NotificationConfiguration*		
ListEventRules	Grants permission to list EventRules	List			
ListManagedNotificationChannelAssociations	Grants permission to list Account contacts and Channels associated with a Managed Notification Configuration	List	ManagedNotificationConfiguration*		
ListManagedNotificationChildEvents	Grants permission to list Managed Notification Child Events	List			
ListManagedNotificationConfigurations	Grants permission to list Managed Notification Configurations	List			
ListManagedNotificationEvents	Grants permission to list Managed Notification Events	List			
ListMemberAccounts	Grants permission to list Member Accounts for a Notification Configuration	List	NotificationConfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListNotificationConfigurations	Grants permission to list NotificationConfigurations	List			
ListNotificationEvents	Grants permission to list NotificationEvents	List			
ListNotificationHubs	Grants permission to list NotificationHubs	List			
ListOrganizationalUnits	Grants permission to list Organizational Units for a Notification Configuration	List	NotificationConfiguration*		
ListTagsForResource	Grants permission to get tags for a resource	List			
PutFeatureOptInStatus [permission only]	Grants permission to update the opt-in status of an AWS User Notification Service feature	Write			
RegisterNotificationHub	Grants permission to register a NotificationHub	Write			
TagResource	Grants permission to tag a resource	Tagging	NotificationConfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from a resource	Tagging	NotificationConfiguration*		
				aws:TagKeys	
UpdateEventRule	Grants permission to update an EventRule	Write	EventRule*		
UpdateNotificationConfiguration	Grants permission to update a NotificationConfiguration	Write	NotificationConfiguration*		

Resource types defined by AWS User Notifications

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
EventRule	arn:${Partition}:notifications::${Account}:configuration/${NotificationConfigurationId}/rule/${EventRuleId}	
NotificationConfiguration	arn:${Partition}:notifications::${Account}:configuration/${NotificationConfigurationId}	aws:ResourceTag/${TagKey}
NotificationEvent	arn:${Partition}:notifications:${Region}:${Account}:configuration/${NotificationConfigurationId}/event/${NotificationEventId}	
ManagedNotificationChildEvent	arn:${Partition}:notifications::${Account}:managed-notification-configuration/category/${Category}/sub-category/${Subcategory}/event/${NotificationEventId}/child-event/${NotificationChildEventId}	
ManagedNotificationConfiguration	arn:${Partition}:notifications::${Account}:managed-notification-configuration/category/${Category}/sub-category/${Subcategory}	
ManagedNotificationEvent	arn:${Partition}:notifications::${Account}:managed-notification-configuration/category/${Category}/sub-category/${Subcategory}/event/${NotificationEventId}	

Condition keys for AWS User Notifications

AWS User Notifications defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS User Notifications Contacts

AWS User Notifications Contacts (service prefix: `notifications-contacts`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS User Notifications Contacts
- Resource types defined by AWS User Notifications Contacts
- Condition keys for AWS User Notifications Contacts

Actions defined by AWS User Notifications Contacts

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ActivateEmailContact	Grants permission to activate the email contact associated with the given ARN if the provided code is valid	Write	EmailContactResource*		
CreateEmailContact	Grants permission to create an email contact	Write		aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteEmailContact	Grants permission to delete an email contact associated with the given ARN	Write	EmailContactResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEmailContact	Grants permission to get an email contact associated with the given ARN	Read	EmailContactResource*		
ListEmailContacts	Grants permission to list email contacts	List			
ListTagsForResource	Grants permission to get tags for a resource	Read			
SendActivationCode	Grants permission to send an activation link to the email associated with the given ARN	Write	EmailContactResource*		
TagResource	Grants permission to tag a resource	Tagging	EmailContactResource*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from a resource	Tagging	EmailContactResource*		
				aws:TagKeys	

Resource types defined by AWS User Notifications Contacts

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
EmailContactResource	`arn:${Partition}:notifications-contacts::${Account}:emailcontact/${EmailContactId}`	aws:ResourceTag/${TagKey}

Condition keys for AWS User Notifications Contacts

AWS User Notifications Contacts defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for AWS WAF V2

AWS WAF V2 (service prefix: `wafv2`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS WAF V2
- Resource types defined by AWS WAF V2
- Condition keys for AWS WAF V2

Actions defined by AWS WAF V2

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type

is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

> **Note**
>
> Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate WebACL	Grants permission to associate a WebACL with a resource	Write	webacl*		amplify:AssociateWebACL apigateway:SetWebACL apprunner:AssociateWebAcl

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					appsync:SetWebACL cognito-idp:AssociateWebACL ec2:AssociateVerifiedAccessInstanceWebAcl elasticloadbalancing:SetWebAcl wafv2:GetPermissionPolicy wafv2:PutPermissionPolicy
			amplify-app		
			apigateway		
			apprunner		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			appsync		
			loadbalancer/app/		
			userpool		
			verified-access-instance		
CheckCapacity	Grants permission to calculate web ACL capacity unit (WCU) requirements for a specified scope and set of rules	Read			
CreateAPIKey	Grants permission to create an API key for use in the integration of the CAPTCHA API in your JavaScript client applications	Write			
CreateIPSet	Grants permission to create an IPSet	Write	ipset*		wafv2:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRegexPatternSet	Grants permission to create a RegexPatternSet	Write	regexpatternset*		wafv2:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Grants permission to create a RuleGroup	Write	rulegroup*		wafv2:TagResource
			ipset		
			regexpatternset		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACL	Grants permission to create a WebACL	Write	webacl*		wafv2:TagResource
			ipset		
			managedruleset		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			regexpatternset		
			rulegroup		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAPIKey	Grants permission to delete an API key	Write			
DeleteFirewallManagerRuleGroups	Grants permission to delete FirewallManagedRulesGroups from a WebACL if not managed by Firewall Manager anymore	Write	webacl*		
DeleteIPSet	Grants permission to delete an IPSet	Write	ipset*		
DeleteLoggingConfiguration	Grants permission to delete the LoggingConfiguration from a WebACL	Write	webacl*		
				wafv2:LogScope	
DeletePermissionPolicy	Grants permission to delete the PermissionPolicy on a RuleGroup	Permissions management	rulegroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRegexPatternSet	Grants permission to delete a RegexPatternSet	Write	regexpatternset*		
DeleteRuleGroup	Grants permission to delete a RuleGroup	Write	rulegroup*		
DeleteWebACL	Grants permission to delete a WebACL	Write	webacl*		
DescribeAllManagedProducts	Grants permission to retrieve product information for a managed rule group	Read			
DescribeManagedProductsByVendor	Grants permission to retrieve product information for a managed rule group by a given vendor	Read			
DescribeManagedRuleGroup	Grants permission to retrieve high-level information for a managed rule group	Read			
DisassociateFirewallManager [permission only]	Grants permission to disassociate Firewall Manager from a WebACL	Write	webacl*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateWebACL	Grants permission to disassociate a WebACL from an application resource	Write	amplify-app		amplify:DisassociateWebACL apigateway:SetWebACL apprunner:DisassociateWebAcl appsync:SetWebACL cognito-idp:DisassociateWebACL ec2:DisassociateVerifiedAccessInstanceWebAcl elasticloadbalancing:SetWebAcl

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					wafv2:PutPermissionPolicy
			apigateway		
			apprunner		
			appsync		
			loadbalancer/app/		
			userpool		
			verified-access-instance		
GenerateMobileSdkReleaseUrl	Grants permission to generate a presigned download URL for the specified release of the mobile SDK	Read			
GetDecryptedAPIKey	Grants permission to return your API key in decrypted form. Use this to check the token domains that you have defined for the key	Read			
GetIPSet	Grants permission to retrieve details about an IPSet	Read	ipset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetLoggingConfiguration	Grants permission to retrieve LoggingConfiguration for a WebACL	Read	webacl*		
				aws:ResourceTag/${TagKey} wafv2:LogScope	
GetManagedRuleSet	Grants permission to retrieve details about a ManagedRuleSet	Read	managedruleset*		
GetMobileSdkRelease	Grants permission to retrieve information for the specified mobile SDK release, including release notes and tags	Read			
GetPermissionPolicy	Grants permission to retrieve a PermissionPolicy for a RuleGroup	Read	rulegroup*		
GetRateBasedStatementManagedKeys	Grants permission to retrieve the keys that are currently blocked by a rate-based rule	Read	webacl*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRegexPatternSet	Grants permission to retrieve details about a RegexPatternSet	Read	regexpatternset*		
				aws:ResourceTag/${TagKey}	
GetRuleGroup	Grants permission to retrieve details about a RuleGroup	Read	rulegroup*		
				aws:ResourceTag/${TagKey}	
GetSampledRequests	Grants permission to retrieve detailed information about a sampling of web requests	Read	webacl*		
GetWebACL	Grants permission to retrieve details about a WebACL	Read	webacl*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetWebACLForResource	Grants permission to retrieve the WebACL that's associated with a resource	Read	webacl*		amplify:GetWebACLForResource apprunner:DescribeWebAclForService cognito-idp:GetWebACLForResource ec2:GetVerifiedAccessInstanceWebAcl wafv2:GetWebACL
			amplify-app		
			apigateway		
			apprunner		
			appsync		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			loadbalancer/app/		
			userpool		
			verified-access-instance		
ListAPIKeys	Grants permission to retrieve a list of the API keys that you've defined for the specified scope	List			
ListAvailableManagedRuleGroupVersions	Grants permission to retrieve an array of managed rule group versions that are available for you to use	List			
ListAvailableManagedRuleGroups	Grants permission to retrieve an array of managed rule groups that are available for you to use	List			
ListIPSets	Grants permission to retrieve an array of IPSetSummary objects for the IP sets that you manage	List			
ListLoggingConfigurations	Grants permission to retrieve an array of your LoggingConfiguration objects	List		wafv2:LogScope	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListManagedRuleSets	Grants permission to retrieve an array of your ManagedRuleSet objects	List			
ListMobileSdkReleases	Grants permission to retrieve a list of the available releases for the mobile SDK and the specified device platform	List			
ListRegexPatternSets	Grants permission to retrieve an array of RegexPatternSetSummary objects for the regex pattern sets that you manage	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResourcesForWebACL	Grants permission to retrieve an array of the Amazon Resource Names (ARNs) for the resources that are associated with a web ACL	List	webacl*		amplify:ListResourcesForWebACL apprunner:ListAssociatedServicesForWebAcl cognito-idp:ListResourcesForWebACL ec2:DescribeVerifiedAccessInstanceWebAclAssociations
			amplify-app		
			apprunner		
			userpool		
			verified-access-instance		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRuleGroups	Grants permission to retrieve an array of RuleGroup Summary objects for the rule groups that you manage	List			
ListTagsForResource	Grants permission to list tags for a resource	Read	ipset		
			regexpatternset		
			rulegroup		
			webacl		
				aws:ResourceTag/${TagKey}	
ListWebACLs	Grants permission to retrieve an array of WebACLSummary objects for the web ACLs that you manage	List			
PutFirewallManagerRuleGroups [permission only]	Grants permission to create FirewallManagedRulesGroups in a WebACL	Write	webacl*		
PutLoggingConfiguration	Grants permission to enable a LoggingConfiguration, to start logging for a web ACL	Write	webacl*		iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				wafv2:LogScope wafv2:LogDestinationResource	
PutManagedRuleSetVersions	Grants permission to enable create a new or update an existing version of a ManagedRuleSet	Write	managedruleset*		
			rulegroup*		
PutPermissionPolicy	Grants permission to attach an IAM policy to a resource, used to share rule groups between accounts	Permissions management	rulegroup*		
TagResource	Grants permission to associate tags with a AWS resource	Tagging	ipset		
			regexpatternset		
			rulegroup		
			webacl		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to disassociate tags from an AWS resource	Tagging	ipset		
			regexpatternset		
			rulegroup		
			webacl		
				aws:TagKeys	
UpdateIPSet	Grants permission to update an IPSet	Write	ipset*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateManagedRuleSetVersionExpiryDate	Grants permission to update the expiry date of a version in ManagedRuleSet	Write	managedruleset*		
UpdateRegexPatternSet	Grants permission to update a RegexPatternSet	Write	regexpatternset*		
				aws:ResourceTag/${TagKey}	
UpdateRuleGroup	Grants permission to update a RuleGroup	Write	rulegroup*		
			ipset		
			regexpatternset		
				aws:ResourceTag/${TagKey}	
UpdateWebACL	Grants permission to update a WebACL	Write	webacl*		
			ipset		
			managedruleset		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			regexpatternset		
			rulegroup		
				aws:ResourceTag/${TagKey}	

Resource types defined by AWS WAF V2

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
webacl	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/webacl/${Name}/${Id}`	aws:ResourceTag/${TagKey}
ipset	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/ipset/${Name}/${Id}`	aws:ResourceTag/${TagKey}
managedruleset	`arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/managedruleset/${Name}/${Id}`	

Resource types	ARN	Condition keys
rulegroup	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/rulegroup/${Name}/${Id}	aws:ResourceTag/${TagKey}
regexpatternset	arn:${Partition}:wafv2:${Region}:${Account}:${Scope}/regexpatternset/${Name}/${Id}	aws:ResourceTag/${TagKey}
loadbalancer/app/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}	
apigateway	arn:${Partition}:apigateway:${Region}::/restapis/${ApiId}/stages/${StageName}	
appsync	arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}	
userpool	arn:${Partition}:cognito-idp:${Region}:${Account}:userpool/${UserPoolId}	
apprunner	arn:${Partition}:apprunner:${Region}:${Account}:service/${ServiceName}/${ServiceId}	
verified-access-instance	arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}	
amplify-app	arn:${Partition}:amplify:${Region}:${Account}:apps/${AppId}	

Condition keys for AWS WAF V2

AWS WAF V2 defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tags in the request	ArrayOfString
wafv2:LogDestinationResource	Filters access by log destination ARN for PutLoggingConfiguration API	ARN
wafv2:LogScope	Filters access by log scope for Logging Configuration API	String

Actions, resources, and condition keys for AWS X-Ray

AWS X-Ray (service prefix: `xray`) provides the following service-specific resources, actions, and condition context keys for use in IAM permission policies.

References:

- Learn how to configure this service.
- View a list of the API operations available for this service.
- Learn how to secure this service and its resources by using IAM permission policies.

Topics

- Actions defined by AWS X-Ray
- Resource types defined by AWS X-Ray
- Condition keys for AWS X-Ray

Actions defined by AWS X-Ray

You can specify the following actions in the `Action` element of an IAM policy statement. Use policies to grant permissions to perform an operation in AWS. When you use an action in a policy, you usually allow or deny access to the API operation or CLI command with the same name. However, in some cases, a single action controls access to more than one operation. Alternatively, some operations require several different actions.

The **Access level** column of the Actions table describes how the action is classified (List, Read, Permissions management, or Tagging). This classification can help you understand the level of access that an action grants when you use it in a policy. For more information about access levels, see Access levels in policy summaries.

The **Resource types** column of the Actions table indicates whether each action supports resource-level permissions. If there is no value for this column, you must specify all resources ("*") to which the policy applies in the `Resource` element of your policy statement. If the column includes a resource type, then you can specify an ARN of that type in a statement with that action. If the action has one or more required resources, the caller must have permission to use the action with those resources. Required resources are indicated in the table with an asterisk (*). If you limit resource access with the `Resource` element in an IAM policy, you must include an ARN or pattern for each required resource type. Some actions support multiple resource types. If the resource type is optional (not indicated as required), then you can choose to use one of the optional resource types.

The **Condition keys** column of the Actions table includes keys that you can specify in a policy statement's `Condition` element. For more information on the condition keys that are associated with resources for the service, see the **Condition keys** column of the Resource types table.

The **Dependent actions** column of the Actions table shows additional permissions that may be required to successfully call an action. These permissions may be needed in addition to the permission for the action itself. When an action specifies dependent actions, those dependencies may apply to additional resources defined for that action, not only the first resource listed in the table.

Note

Resource condition keys are listed in the Resource types table. You can find a link to the resource type that applies to an action in the **Resource types (*required)** column of the Actions table. The resource type in the Resource types table includes the **Condition keys** column, which are the resource condition keys that apply to an action in the Actions table.

For details about the columns in the following table, see Actions table.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetTraceSummaryById [permission only]	Grants permission to retrieve metadata for a list of traces specified by ID	Read			
BatchGetTraces	Grants permission to retrieve a list of traces specified by ID. Each trace is a collection of segment documents that originates from a single request. Use GetTraceSummaries to get a list of trace IDs	List			
CancelTraceRetrieval	Grants permission to cancel an ongoing trace retrieval job initiated by StartTraceRetrieval using the provided RetrievalToken. A successful cancellation will return an HTTP 200 response	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGroup	Grants permission to create a group resource with a name and a filter expression	Write	group*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSamplingRule	Grants permission to create a rule to control sampling behavior for instrumented applications	Write	sampling-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGroup	Grants permission to delete a group resource	Write	group*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy	Grants permission to delete resource policies	Write		xray:ResourcePolicyName	
DeleteSamplingRule	Grants permission to delete a sampling rule	Write	sampling-rule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetDistinctTraceGraphs [permission only]	Grants permission to retrieve distinct service graphs for one or more specific trace IDs	Read			
GetEncryptionConfig	Grants permission to retrieve the current encryption configuration for X-Ray data	Read			
GetGroup	Grants permission to retrieve group resource details	Read	group*		
				aws:ResourceTag/${TagKey}	
GetGroups	Grants permission to retrieve all active group details	Read			
GetIndexingRules	Grants permission to retrieve all indexing rules. Indexing rules are used to determine the server-side sampling rate for spans ingested through the CloudWatchLogs destination and indexed by X-Ray	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInsight	Grants permission to retrieve the details of a specific insight	Read			
GetInsightEvents	Grants permission to retrieve the events of a specific insight	Read			
GetInsightImpactGraph	Grants permission to retrieve the part of the service graph which is impacted for a specific insight	Read			
GetInsightSummaries	Grants permission to retrieve the summary of all insights for a group and time range with optional filters	Read			
GetRetrievedTracesGraph	Grants permission to retrieve a service graph for traces based on the specified RetrievalToken from the Transaction Search CloudWatch log group	Read			
GetSamplingRules	Grants permission to retrieve all sampling rules	Read			
GetSamplingStatisticSummaries	Grants permission to retrieve information about recent sampling results for all sampling rules	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSamplingTargets	Grants permission to request a sampling quota for rules that the service is using to sample requests	Read			
GetServiceGraph	Grants permission to retrieve a document that describes services that process incoming requests, and downstream services that they call as a result	Read			
GetTimeSeriesServiceStatistics	Grants permission to retrieve an aggregation of service statistics defined by a specific time range bucketed into time intervals	Read			
GetTraceGraph	Grants permission to retrieve a service graph for one or more specific trace IDs	Read			
GetTraceSegmentDestination	Grants permission to retrieve the current destination of data sent to PutTraceSegments and OpenTelemetry API	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTraceSummaries	Grants permission to retrieve IDs and metadata for traces available for a specified time frame using an optional filter. To get the full traces, pass the trace IDs to BatchGetTraces	Read			
Link [permission only]	Grants permission to share X-Ray resources with a monitoring account	Write			
ListResourcePolicies	Grants permission to list resource policies	List			
ListRetrievedTraces	Grants permission to retrieve a list of traces for a given RetrievalToken from the Transaction Search CloudWatch log group	List			
ListTagsForResource	Grants permission to list tags for an X-Ray resource	List	group sampling-rule		
PutEncryptionConfig	Grants permission to update the encryption configuration for X-Ray data	Permissions management			
PutResourcePolicy	Grants permission to create or update resource policies	Write		xray:ResourcePolicyName	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutSpans	Grants permission to upload OpenTelemetry spans to AWS X-Ray	Write		logs:LogGenerating ResourceArns	
PutSpansForIndexing [permission only]	Grants permission to upload spans to AWS X-Ray to be indexed	Write			
PutTelemetryRecords	Grants permission to send AWS X-Ray daemon telemetry to the service	Write			
PutTraceSegments	Grants permission to upload segment documents to AWS X-Ray. The X-Ray SDK generates segment documents and sends them to the X-Ray daemon, which uploads them in batches	Write		logs:LogGenerating ResourceArns	
StartTraceRetrieval	Grants permission to initiate a trace retrieval process using the specified time range and for the given trace IDs on the Transaction Search CloudWatch log group	Read			
TagResource	Grants permission to add tags to an X-Ray resource	Tagging	group sampling-rule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from an X-Ray resource	Tagging	group		
			sampling-rule		
				aws:TagKeys	
UpdateGroup	Grants permission to update a group resource	Write	group*		
				aws:ResourceTag/${TagKey}	
UpdateIndexingRule	Grants permission to modify an indexing rule's configuration	Write			
UpdateSamplingRule	Grants permission to modify a sampling rule's configuration	Write	sampling-rule*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateTraceSegmentDestination	Grants permission to modify the destination of data sent to PutTraceSegments and OpenTelemetry API	Write		xray:TraceSegmentDestination	

Resource types defined by AWS X-Ray

The following resource types are defined by this service and can be used in the `Resource` element of IAM permission policy statements. Each action in the Actions table identifies the resource types that can be specified with that action. A resource type can also define which condition keys you can include in a policy. These keys are displayed in the last column of the Resource types table. For details about the columns in the following table, see Resource types table.

Resource types	ARN	Condition keys
group	`arn:${Partition}:xray:${Region}:${Account}:group/${GroupName}/${Id}`	aws:ResourceTag/${TagKey}
sampling-rule	`arn:${Partition}:xray:${Region}:${Account}:sampling-rule/${SamplingRuleName}`	aws:ResourceTag/${TagKey}

Condition keys for AWS X-Ray

AWS X-Ray defines the following condition keys that can be used in the `Condition` element of an IAM policy. You can use these keys to further refine the conditions under which the policy statement applies. For details about the columns in the following table, see Condition keys table.

To view the global condition keys that are available to all services, see AWS global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters access by the tags associated with the resource	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
logs:LogGeneratingResourceArns	Filters access by LogGeneratingResourceArn in the request	ArrayOfARN
xray:ResourcePolicyName	Filters access by PolicyName in the request	String
xray:TraceSegmentDestination	Filters access by TraceSegmentDestination type in the request	String

Related resources

For related information found in the *IAM User Guide*, see the following resources:

- Tutorial: Create and attach your first customer managed policy
- AWS services that work with IAM
- Policy evaluation logic

Simplified AWS service information for programmatic access

AWS provides service reference information in JSON format to streamline the automation of policy management workflows. With the service reference information, you can access available operations, actions, resources, and condition keys across AWS services from machine-readable files. Service reference information includes metadata beyond authorization details, including IAM action last accessed information and IAM Access Analyzer policy generation data.

Security administrators can establish guardrails and developers can ensure appropriate access to applications by identifying the available actions, resources, and condition keys for each AWS service. AWS provides service reference information for AWS services to allow you to incorporate the metadata into your policy management workflows.

- For an inventory of actions, resources, and condition keys for use in IAM policies, see the Service Authorization Reference page for the AWS service. Actions, resources, and condition keys for services that share a service prefix may be split across multiple pages in the Service Authorization Reference.
- For a list of AWS services and actions for which IAM action last accessed information is displayed, see IAM action last accessed information services and actions in the IAM User Guide.
- For a list of AWS services and actions for which IAM Access Analyzer generates policies with action-level information, see IAM Access Analyzer policy generation services in the IAM User Guide.

The content presented in the Service Authorization Reference may be presented differently or contain different metadata. For more information, see Additional field definitions.

The service reference information also offers metadata on operations, including information on authorized actions and the method names in SDKs.

Additional context of the value of condition keys may be available to assist in scoping permissions. For example, the value of `iam:PassedToService` may appear when the action `iam:PassRole` is authorized by an operation.

This operation to action mapping is not supported for all services. Services that don't yet support this mapping will omit the AuthorizedAction property. Additionally, authorized action information

for operations does not include permissions that might be required for operations called on your behalf with Forward Access Sessions.

> **Note**
>
> Changes to the service reference information may take up to 24 hours to be reflected in the list of metadata for the service.

Accessing AWS service reference information

1. Navigate to the service reference information to access the list of AWS services for which reference information is available.

   There are two main entry points:

   http://servicereference.us-east-1.amazonaws.com/ displays a list of AWS services for which reference information is available.

   The following example shows a partial list of services and URLs for their respective reference information:

   ```
   [
       {
           "service": "s3",
           "url": "https://servicereference.us-east-1.amazonaws.com/v1/s3/s3.json"
       },
       {
           "service": "dynamodb",
           "url": "https://servicereference.us-east-1.amazonaws.com/v1/dynamodb/
   dynamodb.json"
       },
       …
   ]
   ```

   https://servicereference.us-east-1.amazonaws.com/v1/mapping.json displays a mapping from SDK services to the location in the service reference that information can be found under.

   The following example shows a partial list of mappings:

   ```
   {
   ```

```
  "SDK" : {
    "Python" : {
      "Boto3" : {
        "accessanalyzer" : {
          "service" : "access-analyzer",
          "url" : "https://servicereference.us-east-1.amazonaws.com/v1/access-
analyzer/access-analyzer.json"
        },
        "account" : {
          "service" : "account",
          "url" : "https://servicereference.us-east-1.amazonaws.com/v1/account/
account.json"
        },
        "amp" : {
          "service" : "aps",
          "url" : "https://servicereference.us-east-1.amazonaws.com/v1/aps/
aps.json"
        },
        ...
      }
    }
  }
}
```

2. Choose a service and navigate to the service information page in the `url` field for the service to view a list of actions, resources, and condition keys for the service.

   The following example shows a partial list of service reference information for Amazon S3:

```
{
    "Name": "s3",
    "Actions": [
        {
            "Name": "GetObject",
            "ActionConditionKeys": [
                "s3:AccessGrantsInstanceArn",
                "s3:AccessPointNetworkOrigin",
                "s3:DataAccessPointAccount",
                "s3:DataAccessPointArn",
                "s3:ExistingObjectTag/key",
                "s3:ResourceAccount",
                "s3:TlsVersion",
                "s3:authType",
```

```
                "s3:if-match",
                "s3:if-none-match",
                "s3:signatureAge",
                "s3:signatureversion",
                "s3:x-amz-content-sha256"
            ],
            "Annotations" : {
            "Properties" : {
                    "IsList" : false,
                    "IsPermissionManagement" : false,
                    "IsTaggingOnly" : false,
                    "IsWrite" : false
                }
            },
            "Resources": [
                {
                    "Name": "object"
                }
            ],
            "SupportedBy" : {
                "IAM Access Analyzer Policy Generation" : false,
                "IAM Action Last Accessed" : false
            }
        },
        {
            "Name": "ListBucket",
            "ActionConditionKeys": [
                "s3:AccessGrantsInstanceArn",
                "s3:AccessPointNetworkOrigin",
                "s3:DataAccessPointAccount",
                "s3:DataAccessPointArn",
                "s3:ResourceAccount",
                "s3:TlsVersion",
                "s3:authType",
                "s3:delimiter",
                "s3:max-keys",
                "s3:prefix",
                "s3:signatureAge",
                "s3:signatureversion",
                "s3:x-amz-content-sha256"
            ],
            "Annotations" : {
                "Properties" : {
                    "IsList" : true,
```

```
                    "IsPermissionManagement" : false,
                    "IsTaggingOnly" : false,
                    "IsWrite" : false
                }
            },
            "Resources": [
                {
                    "Name": "bucket"
                }
            ],
            "SupportedBy" : {
                "IAM Access Analyzer Policy Generation" : false,
                "IAM Action Last Accessed" : false
            }
        },
        ...
    ],
    "ConditionKeys": [
        {
            "Name": "s3:TlsVersion",
            "Types": [
                "Numeric"
            ]
        },
        {
            "Name": "s3:authType",
            "Types": [
                "String"
            ]
        },
        ...
    ],
    "Operations": [
        {
            "Name" : "GetObject",
            "AuthorizedActions" : [
                {
                    "Name" : "GetObject",
                    "Service" : "s3"
                }, {
                    "Name" : "GetObject",
                    "Service" : "s3-object-lambda"
                }, {
                    "Name" : "GetObjectLegalHold",
```

```
                    "Service" : "s3"
                }, {
                    "Name" : "GetObjectRetention",
                    "Service" : "s3"
                }, {
                    "Name" : "GetObjectTagging",
                    "Service" : "s3"
                }, {
                    "Name" : "GetObjectVersion",
                    "Service" : "s3"
                }
            ],
            "SDK" : [
                {
                    "Name" : "s3",
                    "Method" : "get_object",
                    "Package" : "Boto3"
                }
            ]
        },
        ...
    ],
    "Resources": [
        {
            "Name": "accesspoint",
            "ARNFormats": [
                "arn:${Partition}:s3:${Region}:${Account}:accesspoint/
${AccessPointName}"
            ]
        },
        {
            "Name": "bucket",
            "ARNFormats": [
                "arn:${Partition}:s3:::${BucketName}"
            ]
        }
        ...
    ],
    "Version": "v1.4"
}
```

3. Download the JSON file from the service URL to use in your policy authoring workflows.

Glossary

- Operation - An API that can be called, usually through an SDK
- Action - Permission that is authorized when performing an operation

Additional field definitions

Action properties provide additional metadata about service actions to help categorize them based on their permission scope. These properties are found under the `Annotations` field for each action. The metadata consists of four boolean values:

- `IsList` – Provides permissions to discover and list resources, including basic metadata, without accessing resource contents.

  Example – This property is `true` for the Amazon S3 `ListBucket` action, allowing users to view bucket listings without accessing the objects themselves.
- `IsPermissionManagement` – Provides permissions to modify IAM permissions or access credentials.

  Example – This property is `true` for most IAM and AWS Organizations actions, as well as Amazon S3 actions like `PutBucketPolicy` and `DeleteBucketPolicy`.
- `IsTaggingOnly` – Provides permissions only for modifying tags.

  Example – This property is `true` for IAM actions `TagRole` and `UntagRole`, while this property is `false` for `CreateRole` since it provides broader permissions beyond tagging.
- `IsWrite` – Provides permissions to modify resources, which may include tag modifications.

  Example – This property is `true` for Amazon S3 actions `CreateBucket`, `DeleteBucket`, and `PutObject` since they allow resource modification.

> **Note**
>
> These properties are not mutually exclusive. An action may have multiple properties set to `true`.
> It's also possible for all properties to be `false`, as seen with Amazon S3's `GetObject` action. This indicates the action only grants read permissions on an object.

These properties can be used to generate insights for services. The following example shows which permissions with the `s3` prefix allow mutating resources:

```
> curl https://servicereference.us-east-1.amazonaws.com/v1/s3/s3.json | \
    jq '.Actions[] | select(.Annotations.Properties.IsWrite == true) | .Name'

"AssociateAccessGrantsIdentityCenter"
"BypassGovernanceRetention"
"CreateAccessGrant"
"CreateAccessGrantsInstance"
"CreateAccessGrantsLocation"
...
```

The following example shows which action condition keys with the `lambda` prefix you can use to limit access to permission management actions:

```
> curl https://servicereference.us-east-1.amazonaws.com/v1/lambda/lambda.json | \
    jq '.Actions[] | select(.Annotations.Properties.IsPermissionManagement == true) |
 {Name: .Name, ActionConditionKeys: (.ActionConditionKeys // [])}'

{
   "Name": "AddLayerVersionPermission",
    "ActionConditionKeys": []
}
{
    "Name": "AddPermission",
    "ActionConditionKeys": [
        "lambda:FunctionUrlAuthType",
        "lambda:Principal"
    ]
}
{
    "Name": "DisableReplication",
    "ActionConditionKeys": []
}
{
    "Name": "EnableReplication",
    "ActionConditionKeys": []
}
{
    "Name": "RemoveLayerVersionPermission",
    "ActionConditionKeys": []
}
```

```
{
    "Name": "RemovePermission",
    "ActionConditionKeys": [
        "lambda:FunctionUrlAuthType",
        "lambda:Principal"
    ]
}
```